STRIKING A BALANCE BETWEEN THE SECRECY OF ONLINE COMMUNICATION AND ONLINE CRIMINAL INVESTIGATION IN SOUTH AFRICA

by

OLUMUYIWA OLUWOLE POPOOLA

submitted

in accordance with the requirements

for the degree of

DOCTOR OF LAWS

at the

UNIVERSITY OF SOUTH AFRICA

PROMOTER: PROFESSOR V BASDEO

9 MAY, 2020

ABSTRACT

In the Republic of South Africa ('RSA'), there are exponentially increasing and indeterminable consequential risks and breaches involved in the spontaneous and indispensable personal, official and general *anatomic* uses of the quicksilver, complex and delicate *conscriptive*, *interoperable*, *non-compartmentalised* and *non-passworded compartmentalised* online communication devices, technologies, networks, applications, and services. These risks and breaches result in a disequilibrium in the following antithetical legal vector argument. On the one hand, these risks and breaches are attributed to the non-recognition, and inadequate protection of the independent and unique right in online communication, the concept of which originates from the jurisprudence of the broad gamut of the right to privacy. On the other hand, these risks are exacerbated by the increasing, unrestrictive and perpetual techno-legal abuse of online communication by law enforcement agencies or officers ('LEAs' or 'LEOs') of the alternative conduct of the covert online criminal investigation ('OCI') of serious offences, arising from the dearth of and non-compliance with the regulation for the conduct of an OCI.

This dual study clinically examines the irreconcilable conflict between the protection of the right in online communication and the public criminal mandate of the State to conduct an OCI of serious offences. Firstly, this study investigates the existence of the levels of risks involved in the *conscriptive*, *interoperable*, *non-compartmentalised* and *non-passworded compartmentalised* continua of privacy interests in online communication, requiring a corresponding protective and secure regime in the conduct of an OCI. Secondly, it probes into the various substantive and procedural thresholds required in the limitation of the right in online communication when conducting an OCI. Lastly, it examines the mechanisms for institutional and structural independence, competence, due process, separation of powers and checks and balances in the conduct and oversight of the conduct of an OCI in the RSA.

Consequently, the examination of the above issues reveals the absence, inadequacy of, and non-compliance with the substantive and procedural constitutional, legislative and policy framework that caters for the protection of the right in online communication and the conduct of an OCI in the RSA. Accordingly and specifically, this study proposes that the RSA adopts an adequate constitutional and single legislative framework to address the contemporary societal techno-legal tapestry in the conflict between the right in online communication and the conduct of an OCI of serious offences in the RSA as follows.

Firstly, it is imperative to unequivocally, in the legal framework in the RSA, including the Constitution, consider the existence of higher levels of *risks* and the simultaneous or consequential recognition of the higher levels of *protection* of the invaluability in online communication —including the emerging quantum computing— in contrast with non-online communications. This contrast hierarchically compels the unimpeachable protection of the independent right to the secrecy of online communication ('SOC'), which is inadequately and incongruously protected as mere online privacy in section 14 of the Constitution of the RSA.

Secondly, it is equally crucial to consider the application of or compliance with adequate substantive and procedural scientific threshold requirements to conduct an OCI of serious offences in the RSA. These requirements include the application of: online conscription; section 205 of the Criminal Procedure Act; '*no server, but law*' principle as opposed to the U.S. '*no server, no law*' principle; robotic and non-robotic OCI; *ex-parte* and non-*ex-parte* verbal and written quadripartite techno-legal individual and mass online criminal investigation of privileged and non-privileged online communications by ghost and non-ghost applicants; pre and post OCI data management procedure and admissibility of void and voidable evidence. Furthermore, it is of great importance to apply the all-embracing proportionality principle in section 36 of the Constitution in which this study, from a contrarian belief, classifies serious offences into six categories under four criteria and propounds some definite and functional Popoola mathematical and non-mathematical formulae in the standard of proof required to conduct an OCI, the procedure of which should be incorporated in a legislation.

Thirdly and finally, it is of utmost significance to, in the legal framework in the RSA, including the Constitution, consider the application of or compliance with safeguard mechanisms in the conduct of an OCI. These mechanisms are to ensure the inviolability of the principles or requirements of structural and institutional independence, competence, due process, separation of powers and checks and balances in the conduct and oversight of the conduct of an OCI of serious offences by LEAs or LEOs and other stakeholders respectively.

KEYWORDS: Admissibility, conscription, data, interoperability, law enforcement agency or officer, limitation, non-compartmentalisation, non-passworded compartmentalised, online communication, online criminal investigation, privacy, proportionality, protection, risk, robotic online criminal investigation, secrecy of online communication and standard of proof.

DEDICATION

To God Almighty, the creator, author and finisher of my faith who bestowed unto me the inestimable energy and inspiration to weather the storm from the labyrinth in the sea to the shore;

To my loving brother, Omotayo, for the journey of life;

To my late father and mother, Chief J and Madam B Popoola;

To Ire (late) and Abike Olopade;

To kings Adekunmi, Irekunmi and Ifekunmi for their patience while I was studying and for contributing to the debate on the technical issues in this study;

To Adetutu, Adeola, Folasade and Adebimpe;

To the Ojos;

To I Popoola

To Dr A Ribeiro;

To the: victims of climate change; ignored or neglected girl children and women who, regrettably have been, are being and are likely to be raped, and killed; silenced, invisible and trapped boys and men who are victims of rape by men and women; victims of ageism, sexism, homophobia, racism, xenophobia, Afrophobia and religious bigotry.

ACKNOWLEDGMENT

My profound heartfelt gratitude goes to:

My promoter, Prof. V Basdeo, who with invaluable and unflinching guidance, mentorship and support prodigiously rekindled and re-engineered my hopes, aspirations and confidence to conduct an x-ray of this techno-legal study at an excruciating moment when my energy was evaporating. All I can say is, God, bless you abundantly;

The personal assistants to my promoter, V Shale-Moroane and M Teka, for their support in this academic journey;

The authorities at Unisa, for the support provided in achieving this goal, including Ms R Matatiele;

Engr. T Karem and Dr. O Badejogbin, for the genetical support and for being my sounding boards in the invaluable intellectual discourse on the techno-legal issues in this study;

My dear friends, colleagues, well-wishers and ghost models who seemingly do not know their invaluability but somewhat and multi-dimensionally gave me warm oxygen in the course of this long, freezing and stormy oceanic voyage to freedom which propelled my flippers and hand paddles to swim to the shore triumphantly; more importantly, are the following to whom I am immensely indebted for their support in achieving this feat: T Matshego, A Gbemavo, R Akinlolu, D Badmus, M Pitsi, Pastor A Fawole, Dr. A Ogungbire, A Masango, E Mckaiser, Pastor O Oyedapo, K Idowu, Barrister A Ademoyega, late Dr. S Adeyefa, Barrister O Adeleye, Prince A Olugbemiga, Prof. A Olutola, K Mampuru, Dr. G Akinrinmade, O Igandan, O Oladayo Esq., Prof. B Fagbayibo, S Diale, Dr. R Sehapi, Prof. A Okharedia, N Maseko, Prof. A Banjo, O Adamson, A Adenuga, Dr. B Olugbuo, Dr. C Ukattah, Barrister A Sotuminu, Dr. O Akinyeye, Prof. A Diala and Dr. P Kiabilua.

The law firms of E O Idisi & Co and “akinlawon (SAN) & ajomo” for consolidating my desire to acquire and practice the secrets of law.

General quote

While Nelson Mandela in the context of his chequered history says, ‘It’s a long walk to freedom’, my story is worth saying that it’s a long crawl to freedom in this context.

Personal quote

Drawing on the philosophy of Habakkuk 2: 2-3, I state with humility that out of the lavatory is the fertiliser that is reengineered to a techno-legal gold in contemporary society.

Techno-legal quote

No matter the level of secrecy protection we bellow for, we will increasingly, overwhelmingly and conscriptively remain naked in online communication in contemporary society where unjustifiable infringement of new architectural online communications —including quantum computing. These inventions will uncontrollably and unbearably become the norm, get worse and coercively and hopelessly determine how we live our lives like zombies, worthless of our personhood, personality, dignity and humanity; without excluding law enforcement officers and investigators who may also be victims of cyber quake during or after their tenure of service.

Therefore, until individual, corporate, government and international entities sincerely and compulsorily synergise on the management of the conflict between the right to the secrecy of online communication and the conduct of an online criminal investigation, an unpredictable, catastrophic, immeasurable and irreversible cyber warfare would unceasingly erupt between the two divides.

DECLARATION

I declare that **Striking a balance between the secrecy of online communication and online criminal investigation in South Africa** is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

……..

OLUMUYIWA OLUWOLE POPOOLA

TABLE OF CONTENTS

CHAPTER 3: JURISPRUDENCE OF THE TECHNO-LEGAL PROTECTION OF THE RIGHT TO THE SECRECY OF ONLINE COMMUNICATION

CHAPTER 5: LIMITATION OF THE RIGHT TO THE SECRECY OF ONLINE COMMUNICATION

CHAPTER 7: EXECUTION AND POST-EXECUTION OF ONLINE CRIMINAL INVESTIGATION DIRECTION

GLOSSARY OF ACRONYMS AND TERMINOLOGIES

INTRODUCTION

Given the very technical and complex nature and features of this study, this rubric may, in some instances below, deviate from the usual acronym, terminology and meaning generally known to the public. This study describes, and explains the acronym, terminology and meaning in line with the objectives, outcomes, positions and realities of this study.

It is noted that despite the highlight of these acronyms, terminologies, and meanings, some of these acronyms, terminologies and meanings may not be adopted in all instances of the texts in this study in order to reduce the complexities and technicalities involved in reading through this study. Nevertheless, this study still identifies with the need to adopt acronyms, terminologies and meanings for proper uniformity in this areas of philosophy.

ACA: Accreditation Authority

ADM: Alternative Dispute Management

ADR: Alternative Dispute Resolution

AI: Artificial Intelligence

AIDS: Acquired Immune Deficiency Syndrome

ATM: Automated Teller Machine

AUTOMATIC or ARTIFICIAL LEO: An Automatic or Artificial Law Enforcement Officer is an AI driven system that carries out the function of an OCI without the intervention or with minimal intervention of human beings in the performance of the system. An Automatic or Artificial LEO includes robots and drones.

AUCCSPDA: African Union Convention on Cyber Security and Personal Data Protection

CC: Constitutional Court of the Republic of South Africa

CCB: Cybercrime and Cybersecurity Bill of B6-2017 (CCB)

CCTV: Closed Circuit Television

CHANNELS OF COMMUNICATION: Five channels of communication identified in this study are:

a) Broadcasting

b) Human agency

c) Offline electronic communication devices

d) On-demand online communication devices

e) Postal services

CI-SAPS: Crime Intelligence of South African Police Service

CoE CoCC: Council of Europe on the Convention on Cybercrime 2004 - Budapest, 23.XI.2001 (CoE CoCC)

CONTENT DATA: Where this term is used in the context of any communication, it includes an information that relates to the 'substance, purport or meaning of that communication'.[1]

COPA: Consumer Protection Act 68 of 2008

CPA: Criminal Procedure Act 51 of 1977

CSA: Correctional Services Act 11 of 1998

DG: Director General

DP2P: Decentralised Peer To Peer

DI-SANDF: Defence Intelligence of South African National Defence Force

DNA: Deoxyribonucleic acid

DPCI: Directorate for Priority Crime Investigation (also known as HAWKS), which is a specialised crime unit in the South African Police Service

[1] See s 1 of Regulation of Interception of Communications and Provisions of Communication Related Information Act 70 of 2002 (RICA); Berkowitz R 'Packet sniffers and privacy: Why the no-suspicion-required standard in the USA Patriot Act is constitutional' 2002 7 *Computer Law Review and Technology Journal* 2-8 (Berkowitz 2002 7 *Computer Law Review and Technology Journal*)'; Watney M 'Cybercrime and the investigation of crime' in Papadopoulos S & Snail S (eds.) *Cyberlaw @ SA 111 - The law of the Internet in South Africa* (2012) 340 (Watney '*Cybercrime and investigation*').

DSO: Directorate of Special Operations, popularly known as 'Scorpion' which was the investigative arm and under the control of the National Prosecuting Authority ('NPA'), which was disbanded by the court[2] and now succeeded by DPCI.

ECA: Electronic Communications Act 36 of 2005

ECHR: European Commission of Human Right

ECTA: Electronic Communications and Transactions Act 25 of 2002

EFF: Electronic Front Foundation is an international organisation that advocates for online communication right

EFF RSA: Economic Freedom Fighter, which is a political party in the Republic of South Africa

ETSA: European Telecommunications Standard Associations

EUDP DIRECTIVE: European Union Data Protection Directive

FACSIMILE MACHINE: It is one of the six online communication devices identified in this study.

FATF: Financial Action Task Force

FBI: Federal Bureau of Investigation

FFF: First Fact Factor

FIC: Financial Intelligence Centre

FISA: Foreign Intelligence Surveillance Act (of the United States)

FLO: Fixed Line Operator

[2] Berning J and Montesh M 'Countering corruption in South Africa-The rise and fall of the Scorpions and Hawks' 2012 39 *SACQ* 3 at 5-8 (Berning and Montesh 2012 39 *SACQ* 3 at 5-8); Kinnes I and Newham G 'Freeing the Hawks-Why an anti-corruption agency should not be in SAPS' 2012 39 *SACQ* 33 at 33-39 (Kinnes and Newham 2012 39 *SACQ* 33 at 33-39); Mashele P 'Will the Scorpion still sting?-The future of the Directorate of Special Operations' 2006 17 *SACQ* 24 at 24-29 (Mashele 2006 17 *SACQ* 24 at 24-29); Wannenburg G 'Putting Paid to the Untouchables?- The effects of dissolving the Directorate of Special Operations and Specialized Commercial Crime Units' 2008 24 *SACQ* 17 at 17- 20 (Wannenburg 2008 24 *SACQ* 17 at 17- 20); Section 199(1) of the 1996 Constitution and *Glenister v President of the Republic of South Africa and others* 2011 (7) BCLR 651 (CC)(*Glenister v President*).

FOCI: Foreign Online Criminal Investigation

FOCIP: Foreign Online Criminal Investigative Procedure

FTO: Field Training Officers

GILAA: General Intelligence Law Amendment Act No. 11 of 2013

GPS: Global Positioning System

GLT: Geographical Location Technology

GRT: Geo-Restrictive Technology

HAWKS: It is an acronym for DPCI which is the Directorate for Priority Crime Investigation, a unit under the South African Police Service

HC: High Court of the Republic of South Africa

IC: Interception Centre

ICANN: Internet Corporation for Assigned Names and Numbers

ICC: International Criminal Court

ICCS: Intelligence Council on Conditions of Service

ICD: Independent Complaints Directorate

ICT: Information and Communication Technology

ID-NPA: Investigating Directorate of National Prosecuting Authority

ID-SSA: Intelligence Division of State Security Agency

IMSI: International Mobile Subscriber Identity

IoT: Internet of Things

IPID: Independent Police Investigative Directorate is the oversight authority that oversees the misdeeds of officials of South African Police Service

IPIDA: Independent Police Investigative Directorate Act No 1 of 2011

INTEROPERABLE: It is another word for convergence. Interoperability means that though online communication devices, technologies, devices, networks, and

applications are able to maintain their independence when communication occurs, they are now able to simultaneously or dependently operate or converge with each other for better services.

Hitherto, the six online communication devices had limited functional capacities in electronic communications because they operated independently. However, due to the rapid advancement of technologies, networks, applications and services, these devices are now able to engage in various interactive, cooperative and interchangeable operations and functions which create some technical and operational complexities.[3]

INTERPOL: International Criminal Police Organisation

ISP: Internet Service Provider

ISOA: Intelligence Services Act 40 of 1994

ITU: International Telecommunication Union

JSC: Judicial Service Commission

JSCI: Joint Standing Committee on Intelligence is a committee of the Parliament of the Republic of South Africa

JSCD: Joint Standing Committee on Defence is a committee of the Parliament of the Republic of South Africa

LEA: Law Enforcement Agency. Aside from the constitutional and statutory law enforcement officers, LEA includes corporate and private entities commissioned by the State to technically assist or support in law enforcement operation, for example, CCB now provides for Information Technology specialists to join forces with LEO in conducting an OCI.[4] Therefore, it is better to categorise the tasks of corporate and private entities under LEA and not under LEO since the latter as officers may not have the broad mandate

[3] See Chapter 7 of Electronic Communications Act ('ECA') 36 of 2005; See also ss 5(3)(e),(4)(c)(i)-(iv) and 6(a)-(d) of Electronic Communications and Transactions Act ('ECTA') 25 of 2002.
[4] Section 1 of Cybercrime and Cybersecurity Bill (CCB) B6 – 2017, published in Gazette No 40487 of 9 December, 2016 (CCB B6-2017).

to delegate such OCI powers to the corporate and private entities but to restrict the mandate to delegate the power to conduct an OCI to the statutory authority itself for proper control and management.

LEO: Law Enforcement Officer

LOCATION DATA: Another name for location data is meta or traffic data which shows the location of an individual, object or substance.[5]

LOSC: Law of the Sea Convention 1982

ML: Machine learning

MLA: Mutual Legal Agreement

MLAT: Mutual Legal Agreement Treaty

MOU: Memorandum of Understanding

NCC: National Communication Centre

NIA: National Intelligence Authority

NICOC: National Intelligence Coordinating Committee[6]

NON-CONTENT DATA: It consists of meta, status or traffic data[7] in an online communication which can further be divided into four main categories namely, *geographic-traffic data*, *status meta data*, *technical-traffic data* and *socio-economic traffic data*.

[5] ITU 'Interception of communications: Model policy guidelines and legislative text' (2012) 11 (ITU 'Interception Policy & Legislative Text' (2012). Articles 2(b) & (c), 5, 6, 7, 8 & 9 of Directive 2002/58/EC of the European Parliament and of the Council on Privacy an Electronic Communications of 12 July 2002 ('Directive 2002/58/EC'). Article 1(d) of European Council Convention on Cybercrime.

[6] S 4 of the National Strategic Intelligence Act ('NSIA') 39 of 1994 and s 5 of General Intelligence Law Amendment Act (GILAA) 11 of 2013 establish the National Intelligence Co-ordinating Committee (NICOC).

[7] Gratton E *Internet and wireless privacy - A legal guide to global business practices* (2003) 7 -12 (Gratton *Internet and wireless privacy*'); See the latter part of the definition of the term 'communication-related information' in s 1 of RICA. See also Geomans C & Dumortier J 'Enforcement issues - Mandatory Retention of Traffic Data in the EU: Possible impact on privacy and online anonymity' in Nicoll C et al (eds) *Digital anonymity and the law: Tensions and dimensions* (2003) 162-172 (Geomans & Dumortier 'Traffic data: Privacy and online anonymity'); Edwards L and Howells G 'Anonymity, consumers and the Internet: Where everyone knows you're a dog' in Nicoll C et al (eds.) *Digital anonymity and the law: Tensions and dimensions* (2003) 216-217 and 222-224; Watney *Cybercrime and the investigation* 340; Berkowitz 2002 7 *Computer Law Review and Technology Journal* 2-8; Larsson C 'Telecom Operator's Incident Investigations' in Wahlgren P (ed.) *Information & Communication Technology – Legal issues* – Scandinavian Studies in Law Vol. 56 (2010) 234 - 235; Currie I and De Waal J *The Bill of Rights Handbook* 6 ed. (2013) 295 (Currie and De Waal *Bill of rights*); Volonino L

i. ***Geographic traffic data*** or ***geo-locus data*** is an information that indicates the physical location, positioning or movement of parties or objects in an online communication network.[8] Examples of geographic traffic data include: a) smart interaction system such as Global Positioning System (GPS)[9] and Google Maps Street View;[10] b) an application in a mobile cellular telephone indicating where a picture was taken or where other transactions took place; and c) vehicular movement tracker on a mobile cellular telephone which gives feedback about the location of a vehicle.

ii. ***Social-economic traffic data***[11] refers to the information that is made available in electronic form which means, purports to mean or indicate the social interactions; marketing, economic and business preferences; and moral and cultural beliefs of users.[12] An example is profiling an individual for social, economic and cultural purposes.[13]

iii. ***Status meta data*** entails the non-content or non-verbal expression of state of affairs, condition, standing or process of things or persons through an online network. The status meta data, which in some respect is similar to geographic traffic data, is synonymous with the o-tag system that is attached to a vehicular o-toll payment system, vehicular and pedestrian o-access card system, household o-monitoring system (or *Internet* of *things*) and similar devices.

'Electronic evidence and computer forensics' 2003 12 *Communications of the Association for Information Systems* 459; Whitcomb C M 'A Historical perspective of the digital evidence: A forensic scientist's view' (2002) 1 *International Journal of Digital Evidence* 1- 4; Basdeo V 'The legal challenges of search and seizure of electronic evidence in South African criminal procedure: A comparative analysis' 2012 2 *SACJ* 198. See generally Protection of Personal Information Act (POPIA) No 4 of 2013; Snail S and Papadopoulos S 'Privacy and data protection' in Van der Merwe D et al *Information Communications and Technology Law* (2008) 275 (Snail and Papadopoulos '*Privacy and data protection*'); Section 1 of ECTA No 25 of 2002; Section 1(t) of ECTA Amendment Bill [B-2012]; Section 1 of ECA No 36 of 2005; Ncube C B 'Watching the Watcher: Recent Developments in Privacy Regulation and Cyber-surveillance in South Africa' (2006) 13 *SCRIPT-ed* 349; Weber R H 'Internet of things-Need for a new legal environment?' 2009 25 *Computer Law & Security Report* 522-527; Weber R H and Weber R *Internet of things – Legal perspectives* (2010) 1; Roos A 'Privacy in the Facebook era: a South African legal perspective' 2012 129 *SALJ* 382-383 (Roos 2012 129 *SALJ*).

[8] ITU 'Interception Policy & Legislative Text' (2012) 11.

. Articles 2(b) & (c), 5, 6, 7, 8 & 9 of Directive 2002/58/EC of the European Parliament and of the Council on Privacy an Electronic Communications of 12 July 2002 ('Directive 2002/58/EC'). Article 1(d) of CoE CoCC.

[9] Gratton E *Internet and wireless privacy* 29-36 and 299 - 305; Roos 2012 129 *SALJ* 390.

[10] Snail and Papadopoulos *Privacy and data protection* 275.

[11] ITU 'Interception Policy & Legislative Text' (2012) 11. Articles 2(b) & (c), 5, 6, 7, 8 & 9 of Directive 2002/58/EC of the European Parliament and of the Council on Privacy an Electronic Communications of 12 July 2002 ('Directive 2002/58/EC'). Article 1(d) of CoE CoCC.

[12] ITU 'Interception Policy & Legislative Text' (2012) 11. Articles 2(b) & (c), 5, 6, 7, 8 & 9 of Directive 2002/58/EC of the European Parliament and of the Council on Privacy an Electronic Communications of 12 July, 2002 ('Directive 2002/58/EC'). Article 1(d) of CoE CoCC.

[13] Gratton *Internet and wireless privacy* 11-12.

Examples of status meta data include: a) tracker or monitoring system of the safety, security and functionality of a vehicle battery or other devices in a vehicle, which a geographic traffic data system does not perform; b) o-medical tag or monitoring system which does the medical check-up of an individual periodically where there is a medical abnormality of any nature programmed into the system.

iv. ***Technical-traffic data*** indicates substances such as switching, dialling and signalling in online communications and interception and monitoring of records. It includes records showing the numbers dialled, origin of calls or communications made, signal, location, destination, route, switch, date, duration, termination or size of the communications, type of service carried out, type of equipment used or other records indicating the activities of a user in an online communications.[14]

NON-online communication devices: Aside from online communications, there are four other agents or channels of communications which do not have the same features like online communications. Non-online communication devices are:

a) Broadcasting communications
b) Human agency as a form of communication
c) Offline or physical seizure of electronic communication contents and devices, which do not involve the use of either wired or wireless online connectivity
d) Postal communication

NON-U.S. person: Is a person who is not a U.S. citizen or is a person who does not have the permanent residence of the U.S.

NPA: National Prosecuting Authority

NQF: National Qualification Framework

NSIA: National Strategic Intelligence Act

MCO: Mobile Cellular Operator

[14] Gratton *Internet and wireless privacy* 11-12.

MOBILE CELLULAR TELEPHONE: It is one of the six online communication devices identified in this study which are: a) land line telephone; b) two-way radio communication; c) facsimile machine; d) Internet; e) mobile cellular telephone and f) o-tag system.[15]

OCI: Online Criminal Investigation[16] is an alternative procedure in conducting criminal investigation in any wired or wireless online network. Another term or phrase for an OCI is 'online surveillance' which is a broad concept comprising interception, monitoring, decryption and data retention or data preservation of online communication.[17] Through a wired or wireless online network[18] including Bluetooth technology,[19] an OCI is conducted to investigate offences committed in offline and online spaces.

OCSP: Online Communication Service Provider. Hitherto, the term 'Online Service Provider' or OSP has been publicly used to describe the function and role of entities that provide the core or primary technical aspect of online communication services. However, given the broad and extensive technical functions in an online communication, the term 'OCSP' may now be used to describe the services rendered in an online communication including pre and post-execution of an OCI such as the authentication service provider, cryptography, cyber inspector, decryption key holder, fixed line operator, interception centre, Internet service provider, mobile cellular operator and telecommunication service provider.

OECD: Organisation for Economic Cooperation and Development

OGA: Office of the Ghost Advocate

OIGI: Office of the Inspector General of Intelligence

OIC: Office of the Interception Centre

O-mail: Is an online communication ('*o-mail*') which is an alternative abbreviation to an electronic communication ('*e-mail*'), which in this study, is seen as an incorrect or inappropriate terminology in contemporary society in which an *o-mail* correctly or appropriately describes the protection for the right to the secrecy of online communication (SOC). Given the compelling distinction made in this study between

[15] ITU 'Interception Policy & Legislative Text' (2012) 12.
[16] Art 18(18) and 24(2)(b) and (4) of TOCC and Art 25(3) of CoE CoCC.
[17] Watney *Cybercrime and investigation* 339 - 342.
[18] Watney *Cybercrime and investigation* 334; Van der Merwe D 'Telecommunication law' in D van der Merwe et al *Information and communications technology law* (2008) 13 - 21.
[19] *State v Terrence Stephan Brown* (1) SACR 206 (WCC) para 6.

an online communication and other channels of communication such as electronic communications which include offline electronic communication (such as a computer without an online network connection) and broadcasting,[20] it is posited that an *o-mail* best describes the nature and features of an online communication that takes place in an electronic signal which is not seen by human eye or with the aid of a device.[21]

Online communication devices: are landline telephone, facsimile machine, two-way radio communication, Internet, mobile cellular phone and o-tag system.[22]

ONLINE TAG SYSTEM: It is a meta or traffic tag system that is attached or imbedded into human body, object or substance which grants access to a holder, silently records an access transaction, records traffic or monitors movement of the tag holder, substance or object, etc.

OPA: Office of the Public Advocate

OPP: Office of the Public Protector

PAA: Public Audit Amendment Act 2018

PDA: Personal Digital Assistant

PFMA: Public Finance Management Act

PIN: Personal Identification Number

POPIA: Protection of Personal Information Act 4 of 2013

POPOOLA QOCI: Popoola Quadripartite Online Criminal Investigation

PRASA: Passenger Rail Agency of South Africa

PSA: Public Service Act 103 of 1994

PSIB: Protection of State Information Bill [B 6D -2010] (or Secrecy Bill)

PSIRAB: Private Security Industry Regulation Amendment Bill No 27D- 2012

[20] Para 2.2 of Chapter 2 and para 3.5.7 of Chapter 3 of this study.
[21] Para 2.2.2.1 of Chapter 2 of this study.
[22] ITU 'Interception Policy & Legislative Text' (2012) 12.

RICA: Regulation of Interception of Communications and Provisions of Communication Related Information Act No 70 of 2002

ROCI: Robotic online criminal investigation

ROCITOR: Robotic online criminal investigator

RSA: Republic of South Africa

TSP: Telecommunication Service Provision

SALRC: South African Law Reform Commission

SANDF: South African National Defence Force

SANEF: South African National Editors Forum

SANRAL: South African National Road Agency Limited

SAPS: South African Police Service

SAPSA: South African Police Service Act 68 of 1995

SAPSAA: South African Police Service Amendment Act 10 of 2012 (SAPSAA)

SAQA: South African Qualification Authority

SARS: South African Revenue Service

SCA: Supreme Court of Appeal of the Republic of South Africa

SCM: Supply Chain Management

SCOPA: Standing Committee on Public Accounts of Parliament

SCORPION: This is another title for the Directorate of Special Operations, popularly known as 'DSO' which was the investigative arm and under the control of the NPA, which was disbanded by the court[23] and now succeeded by DPCI, popularly known as the 'HAWKS'.

[23] Berning and Montesh 2012 39 *SACQ* 3 at 5-8; Kinnes and Newham 2012 39 *SACQ* 33 at 33-39; Mashele 2006 17 *SACQ* 24 at 24-29; Wannenburg 2008 24 *SACQ* 17 at 17- 20; S 199(1) of the 1996 Constitution and *Glenister v President* supra 651.

SIM: Subscriber Identification Module

SIU: Special Investigating Unit

SLA: Service Level Agreement

SMS: Short Message Service

SNS: Social Network Site

SOC: Secrecy of Online Communication

SONA: State Of the Nation Address

SOP: Standard Operating Procedure

SPECIAL LEO: This is a special law enforcement officer whose primary duty may not be related to law enforcement but by necessity or default finds himself or herself conducting an OCI in exceptional circumstances. Special LEOs include *human pilots* or *crew members* in an aircraft or air borne moving object or substance, *human captains* or *crew members* in a ship or water borne moving object or substance, *robot, drone*, amongst others.

SSA: State Security Agency

TFA: Training Fund for Agency

TOCC: United Nations Convention against Transnational Organized Crime 2000.

TSP: Telecommunication Service Provider

UAV: Unmanned Area Vehicle

UN: United Nations

UNCLOS: United Nations Convention on the Law of the Sea

UNECOMIC: United Nations Convention on the Use of Electronic Communications in International Contracts

UNODC: United Nations Office on Drugs and Crime

VoIP: Voice over Internet Protocol

VPN: Virtual Private Network

> As I vanish into thin air on a voyage of chirpation, chatteration or communication discovery, I thought I was free to express my innermost feelings and being in the deepest part of my 'nest' like a bird. But whether or not I am a holy bird, which no one knows about me until God judges me, my dignity, more importantly, my secrecy is violently, perpetually and irredeemably trapped, raped and stolen from afar in the covert, conscriptive, interconnected and unjustifiable web of the eagle spying on me from the redwoods?

CHAPTER 1: INTRODUCTION

1.1 BACKGROUND TO THE STUDY

The gravamen of this study is anchored on one of the first cases of offline conflict witnessed by humankind, recorded in some religious writings by the anthropologists. According to those who electively believe in Christian religion, the conflict was between the protection of the right to the privacy of Adam and Eve and their investigation for disobeying the commandment of God concerning the instruction that the former should not eat from the 'forbidden fruit in the Garden of Eden'.[1] However, upon discovering the defiance of the instruction, God proceeded to conduct an investigation on Adam and Eve, which led to their resistance to submit to the investigation, having realised that they were stark naked in the Garden of Eden.[2]

This religious scenario highlights two key, adverse and controversial concepts in contemporary society. The controversy highlights the disequilibrium between the protection of the neglected or emerging right to the secrecy of online communication ('SOC')[3] and the public criminal

[1] Genesis 2: 16-17 and 25 and 3:4-13 in the Holy Bible and Chapter 20: verse 120 in the Holy Quran.
[2] Supra.
[3] This is one of the most used abbreviations in this study which is listed under the 'key words' at the abstract page, therefore, it may not be written in full in subsequent appearances.

mandate by law enforcement agencies or officers ('LEAs' or 'LEOs')[4] to conduct an online criminal investigation ('OCI')[5] in the Republic of South Africa ('RSA')[6] where there is criminal wrongdoing against a public authority, an individual or entity.

The protection of the right to the SOC is not new in the world and to the twenty-first century too. In fact, the right to the SOC is modelled after the right to the 'secrecy of telecommunications', developed by the European and U.S. twenty-first century jurisprudence,[7] which had hitherto been neglected in the broad privacy jurisprudence in the RSA.[8] The identification of the problem associated with the protection of the right to the SOC in the RSA is not traceable to the twenty-first-century quicksilver technology era alone, but before this time too. As far back as 1978 when the development of information and communication technology was in its infancy, it was then observed that the use of the unrestrictive OCI procedure was inherently intrusive and posed high levels of risks to the protection of the right to privacy in the RSA.[9]

It is therefore not surprising that in the present time where online communication devices[10] have become 'an important part of human anatomy'[11] in modern South African society,[12] the

[4] Supra.
[5] Supra.
[6] Supra.
[7] Ruiz B R *Privacy in telecommunications–A European and American approach* (1997) 1-5, 15, 20-23, 45-46, 59-67, 70, 81-83, 86-87, 143, 151-159, 171-172, 175-177, 179-257, 313-318 and 322-323 (Ruiz *Privacy in telecommunications*).
[8] Section 14(4) of the Constitution which broadly provides for communication of privacy without identifying or classifying it into offline and online privacy communications is inadequate, given the significance of the development of technology in online communication.
[9] McQuoid-Mason D J *The law of privacy in South Africa* (1978) XXXIX, 5-8 and 146-48 (McQuoid-Mason *Privacy I*).
[10] Six online communication devices are identified in this study, which are: a) landline telephone; b) facsimile machine; c) two-way radio communication; d) Internet; e) mobile cellular telephone and f) o-tag system. *Jamieson v Sobingo* 2002 (4) SA 49 (SCA) 5 (*Jamieson v Sobingo*); *Entores Ltd v Miles Far East Corporation* [1955] 2 QB 327(CA) 327 [1955] 2 All ER 493 (*Entores Ltd v Miles*); Eiselen S 'E-Commerce' in Van der Merwe D et. al. *Information and communication technology law* (2008) 148 (Eiselen *E-Commerce*); ITU 'Interception of Communications: Model Policy Guidelines and Legislative Text' (2012) 12.
[11] *David Leon Riley v California* and *United States v Brima Wurie* 573 U.S. 2014 (*Riley v California* and *U.S v Wurie*) 9, 16-17 and 28 of the Opinion and p 6 of the minority decision by Alito J; Swire P P and Ahmad K (eds.) 'Part 5: Locational Tracking' in *Privacy and surveillance with new technologies* (2012) 245 (Swire and Ahmad (eds.) *Part 5: Locational tracking*); Thompson R M II '*United States v Jones*: GPS monitoring, property, and privacy' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 250 (Thompson *GPS monitoring*). In the U.S., cellphone users are more than the population of the U.S., Crump C 'On the Geolocational Privacy and Surveillance Act' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 274 (Crump *Geolocational Privacy and Surveillance Act*).
[12] Moyo A 'Only 3.5% of SA's households don't have phones' https://www.itweb.co.za/content/JOlx4z7kVpv56kmW (Date of use: 26 June 2017); Bawa *ROICA* 331; Affidavit in support of the Notice of Motion in *AmaBhungane v Minister of Justice* at 125-136, more particularly

frequent indiscriminate uses of an OCI by LEAs or LEOs,[13] investigators and non-authorised persons in the society are alarming[14] unreasonable, irrational and unjustifiable[15] in the present time when compared to 1978.

The indiscriminate uses of OCI are expressed in the observation of Bawa on the primary objective of RICA which is misconstrued by society.[16] Bawa states that RICA, whose primary objective is supposed to be that of protecting 'confidential' information[17] from unlawful interception, is now being misconstrued to be available or used as a primary, indispensable and compelling law or tool for crime prevention[18] in all degrees of serious offences or circumstances, whereas, an OCI is meant to investigate serious offences only.[19]

Compounding this problem is the fact that the conduct of an OCI, which is generally not supposed to be a first-instance method of investigation[20] of offences committed offline and

---

paras 126 and 133; Regulations 5.1 and 5.2 of Schedule C of Directive for Internet Service Providers in terms of Section 30(7)(a) read with section 30(2) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002' ('RICA') - No. 28271 Government Gazette, Notice 1325 of 28 November 2005 (Schedule C of RICA); SALRC 'Discussion Paper 109- Project 124 —Privacy and Data Protection' (2005) paras 4.2.38–4.2.39 http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016 (SALRC http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016).

[13] In the U.S., wiretapping is a 'common method used by police to gather information, Swire P P and Ahmad K (eds.) 'Part 4: Backdoor surveillance' in *Privacy and surveillance with new technologies* (2012) 191 (Swire and Ahmad (eds.) *Part 4: Backdoor surveillance*).

[14] Basdeo V 'The legal challenges of search and seizure of electronic evidence in South African criminal procedure: A comparative Analysis' (2012) 2 *SACJ* 196 (Basdeo 2012 2 *SACJ*). In the U.S., 'most LEAs do not obtain warrants to track cell phones, and legal standards used very widely''. The U.S. Attorney-General's office obtained 'geological data under inconsistent standards. According to the U.S. Department of Justice, it says it need not show probable cause before conducting an OCI save where real-time and triangulation data is involved, see generally Crump *Geolocational Privacy and Surveillance Act* 283 - 284.

[15] Swart H 'Secret state: How the government spies on you' https://mg.co.za/article/2011-10-14-secret-state/ (Date of use: 12 December 2016 (Swart https://mg.co.za/article/2011-10-14-secret-state/ (Date of use:12 December 2016).

[16] Bawa N 'Regulation of the Interception of Communications and Provisions of Communication Related Information Act' in Thornton L et. al. (eds.) *Telecommunication law in South Africa* 297, 300, 302 and 303 (Bawa *ROICA*).

[17] In *Protea technology Ltd & another v Wainer & others* (1997) 3 B All SA 594, 603 (*Protea*) the court held that confidential information is such information that is restricted or only disclosed to a person intended and necessary.

[18] *Lenco Holdings Ltd v Eckstein* 1996(2) SA 693 (N) 700 and *S v Kidson* 1999 (1) SACR 338 (W) 344; Bawa *ROICA* 297, 300, 302 and 303; Gereda S L 'Electronic Communications and Transactions Act' in 'Thornton L et al (eds) *Telecommunication law in South Africa* (2006)'282 (Gereda *Electronic Communications and Transactions Act*).

[19] *AmaBhungane v Minister of Justice* supra 29 and 60.

[20] Section 16(2)(d)(ii) and (e) and (5)(b) and (c) of RICA; American Bar Association 'Standards on Prosecutorial Investigations' (2014) para 2.2 (b) https://www.americanbar.org/publications/criminal_justice_section_archive/crimjust_standards_pinvestigate.html (Date of use: 12 July 2017 (American Bar Association https://www.americanbar.org/publications/criminal_justice_section_archive/crimjust_standards_pinvestigate.html (Date of use: 12 July 2017).

online, is more intrusive and poses higher and unquantifiable levels of risks in the protection of the right to the SOC in the present time.[21]

The foregoing *status qua* remain hamstrung by the slow development of law, which does not keep pace with the exponential pace of technological development and the risk of its abuse because nefarious and criminal activities[22] make interception 'much easier than it used to be'.[23]

[21] Swart H 'Your cellphone records and the law: The legal loophole that lets state spying run rampant' https://www.msn.com/en-za/news/techandscience/your-cellphone-records-and-the-law-the-legal-loophole-that-lets-state-spying-run-rampant/ar-AAxyCpM?ocid=spartandhp (Date of use: 20 May 2018 (Swart https://www.msn.com/en-za/news/techandscience/your-cellphone-records-and-the-law-the-legal-loophole-that-lets-state-spying-run-rampant/ar-AAxyCpM?ocid=spartandhp (Date of use: 20 May 2018); Hunter M and Smith T *Spooked: Surveillance of journal* Hunter M and Smith T *Spooked: Surveillance of journalists in South Africa* at 2 and 7 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018) (Hunter and Smith https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use : 27 November 2018).

[22] Basdeo 2012 2 *SACJ* 196 and 210; *AmaBhungane v Minister of Justice* supra 28;Goodman M *Future crimes: A journey to the dark side of technology - and how to survive it* (2015) (Goodman *Future crimes: Dark side of technology*); De Sola Pool I and Baeza M L *Safeguarding the first amendment in the telecommunications era technologies of freedom* (I983) 8 (De Sola Pool and Baeza *Telecommunications era technologies of freedom*) and Van der Merwe D 'Introduction' in Van der Merwe D, Roos A and Pistorius T (eds.) *Information communications and technology law* (2008) 1 and 7 (Van der Merwe *Introduction*) and Watney M 'Cybercrime and the investigation of crime' in Papadopoulos S and Snail S (eds.) *Cyberlaw @ SA 111- The law of the Internet in South Africa* (2012) 333 (Watney *Cybercrime and investigation*); Thompson *GPS monitoring* 258; Carr N 'Tracking is an assault on liberty, with real dangers' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 365 (Carr *Tracking is an assault on liberty*). Gamble J in para 61 of *State v Philip Miller and 8 Others* 2016 (1) *SACR* 251 (WCC) (*State v Miller*) states that the development of nuanced and clear regime regulating the conduct of an OCI by LEAs in the RSA will take long years to come and several cases tested in court, by which time technological development would have further grown exponentially. For similar comments, see also SALRC para 2.4.3 http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016).

[23] The Economist 'Learning to Live with Big Brother' in Swire P P and Ahmad K *Privacy and surveillance with new technologies* (2012) 31 (The Economist *Learning to live with big brother*).

1.2 PROBLEM STATEMENT

In pursuance of the scope of this study, the central problem is twofold. On the one hand, the absence of a constitutional principle,[24] inadequate legislation[25] in and non-compliance[26] with existing law regulating the conduct of an OCI —as an intrusive, alternative and a covert investigative method in the RICA—[27] constitute the interdependent central problem in the

[24] It is noted that aside from the omnibus provision of section 36 of the 1996 Constitution (Act108 of 1966 'Constitution'), which generally caters for the limitation of rights, the significance of making specific provision for the regulation of the conduct of an OCI in the constitution cannot be over-emphasized. This is because the complex and delicate nature and features of the conduct of an OCI are relatively overwhelming than in the nature and features of the conduct of non-OCI procedures, therefore, the inclusion of the protection of the former in the Constitution will ensure adequate regulation in this regard in the RSA. Chapter 11 (more particularly sections 199(5) and (6), 205(3) and 206(5) and (6)) of the Constitution provides for the regulation of security services including the general mandate of the SAPS to investigate crime in the society and the investigation of the inefficiency and misconduct in SAPS. The Chapter also prohibits LEOs from 'obeying a manifestly illegal order'. However, there is no constitutional principle or provision for the conduct of an OCI nor guiding principles regulating the conduct of OCI, being an intrusive method of investigation in online communication. This is unlike the express constitutional provision of some principles in some important areas of governance stipulated in the Constitution. These include the principles of cooperative governance, procurement, public administration, Alternative Dispute Management mechanism (which this study refers to as 'ADM' instead of the misconstrued Alternative dispute Resolution 'ADR') etc., see Chapter 3 (see particularly section 41(1)(h)(i) - (vi), (2)(a) and (b), (3) and (4)) and sections 195 and 217 of the Constitution. In pursuance of the Constitutional provision, ADM principle is also provided in section 57(7) of the Cybercrime and Cybersecurity Bill (CCB) B6–2017, published in Gazette No 40487 of 9 December 2016. Please note that CCB B6-2017 replaces the Cybercrime and Cybersecurity Bill 2015 (CCB-2015). Further, the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 replaces other previous bills. Section 69(1) of ECTA provides for ADR in disputes relating to domain name dispute.

[25] *AmaBhungane v Minister of Justice Centre for Investigative Journalism & Another v Minister of Justice and Correctional Services* Case No: 25978/2017 paras 91, 102 and 103 (*AmaBhungane v Minister of Justice*).

[26] Letsoalo M 'Spooks' cash 'used to spy on Cyril Ramaphosa'' https://mg.co.za/article/2017-09-08-00-secret-funds-used-to-spy-on-cyril (Date of use: 8 September 2017) (Letsoalo https://mg.co.za/article/2017-09-08-00-secret-funds-used-to-spy-on-cyril (Date of use: 8 September 2017); Mashego A and Masondo S 'Secret plot to oust Mbaks' https://www.news24.com/SouthAfrica/News/secret-plot-to-oust-mbaks-20170827-2 (Date of use: 30 August 2017 (Mashego and Masondo https://www.news24.com/SouthAfrica/News/secret-plot-to-oust-mbaks-20170827-2 (Date of use: 30 August 2017); Serrao A 'Senior crime intelligence officials without top secret clearance' https://www.news24.com/SouthAfrica/News/senior-crime-intelligence-officials-without-top-secret-clearance-20171130 (Date of use: 1 December 2017 (Serrao https://www.news24.com/SouthAfrica/News/senior-crime-intelligence-officials-without-top-secret-clearance-20171130 (Date of use: 1 December 2017). In the U.S., some service providers never comply with court orders while some delay in complying with court orders, with considerable effort and expense, Caproni V 'Going dark: Lawful electronic surveillance in the face of new technologies' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 205 and 213 (Caproni *Lawful electronic surveillance*). In the U.S., it has been opined that 'The problem with online law enforcement is not the need for new law or for government to ''do more'' Government should get better at carrying out its existing responsibilities', see The Economist 'Economist debates: online privacy' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 362 (The Economist *Online privacy*); In Italy, monetary motivation —such as bribes and blackmail influenced the massive collection of the online dossiers of politicians, financiers, business people, bankers, journalists and judges, see Landau S 'Going dark: Lawful electronic surveillance in the face of new technologies' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 220 (Landau *Lawful electronic surveillance in the face of new technologies*); Thompson S A and Warzel C 'How to Track President Trump' https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html (Date of use: 12 January 2018).

[27] This is the main legislation referred to in this study, therefore, it may not be written in full in subsequent appearances. Section 16(7) of the RICA; *R v Abelson* 1933 TPD 227 231; Kruger A *Organised crime and*

criminal justice system in the RSA. On the other hand, Van der Merwe states '[that] until specific legislation has been enacted to give effect to the right to privacy of communication, however, it is very difficult to speculate how privacy will be protected in the "open" world of the Internet'.[28]

In this regard, no adequate constitutional and statutory regime exists in the RSA to protect the emerging right to the SOC in the complex, delicate, conscriptive, interoperable, non-compartmentalised and non-pass-worded-compartmentalised online communication devices, technologies, networks, applications and services tapestry in the contemporary society.[29]

The consequences emanating from the above dual problems are demonstrated by the complaints about certain unlawful online communication infringements that were lodged with various authorities in the RSA against local[30] and foreign[31] LEAs, LEOs, investigators and

proceeds of crime law in South Africa (2008) 1 (Kruger *Organised crime and proceeds of crime*); Van der Vyver J D 'State secrecy' in Oosthuizen G C et. al. (eds.) *Professional secrecy in South Africa* (1983) 48 (Van der Vyver *State secrecy*). It is submitted that 'online communication', which can also be referred to as 'cyber communication' or 'on-demand online communication', is one of the five channels of communication of privacy. In online communication, six devices are identified in this study namely: landline telephone, facsimile machine, two-way radio communication, Internet, mobile cellular telephone and o-tag system, see para 2.2.2 of Chapter 2 of this study; ITU 'Interception of Communications: Model Policy Guidelines and Legislative Text' (2012) 12. Other channels of communication of privacy are a) broadcasting; b) human agency; (c) offline electronic communication (for example, a computer which does not have an online connectivity, but which has a memory stick which can be used for communication via copying of data into or from a memory stick); d) postal services. Further, for ease of reference, 'online communication' seems to be simpler term, which will be adopted in this study, to specifically deal with the unique nature, features and issues in this study as opposed to 'offline electronic communication', both of which constitute 'electronic communication'. The latter term is a broad and general term used in the society, which includes 'online communication', 'offline electronic communication', broadcasting communication and other related types of electronic communications.

[28] Van der Merwe D 'Telecommunication law' in Van der Merwe D, A Roos and T Pistorius (eds.) *Information and communications technology law* (2008) 23 (Van der Merwe *Telecommunication law*).

[29] See chapters 2 and 3 of this study for the examination of the techno-legal features and nature of online communication.

[30] AmaBhugane 'Advocacy: amaB challenges Snooping Law' 2 http://AmaBhungane v Minister of Justice.co.za/article/2017-04-20-amab-challenges-snooping-law (Date of use: 20 April 2017) (AmaBhugane http://AmaBhungane v Minister of Justice.co.za/article/2017-04-20-amab-challenges-snooping-law (Date of use: 20 April 2017); eNCA 'Beware: big brother is listening' http://www.msn.com/en-za/news/national/beware-big-brother-is-listening/ar-AAqCyLp?li=BBqg6Q6&ocid=UE07DHP (Date of use: 24 August 2017) (eNCA http://www.msn.com/en-za/news/national/beware-big-brother-is-listening/ar-AAqCyLp?li=BBqg6Q6&ocid=UE07DHP (Date of use: 24 August 2017); Mail and Guardian 'Zuma: SA not immune to security threats' http://mg.co.za/article/2009-12-03-zuma-sa-not-immune-to-security-threats (Date of use: 18 April 2016) (Mail and Guardian http://mg.co.za/article/2009-12-03-zuma-sa-not-immune-to-security-threats (Date of use: 18 April 2016); *Primemedia Broadcasting & Others v Speaker of the National Assembly & Others* Case No 2749/ 2015 at 61 (*Primemedia v Speaker, National Assembly*); Respondents Affidavit in *AmaBhungane v Minister of Justice* paras 28- 131, 136 and 140, 143, 144 and 146.

[31] SAPA-AFP 'NSA is tracking mobile phones all over the world' https://businesstech.co.za/news/general/50542/nsa-is-tracking-mobile-phones-all-over-the-world/ (Date of use: 12 January 2017) (SAPA-AFP https://businesstech.co.za/news/general/50542/nsa-is-tracking-mobile-phones-all-over-the-world/ (Date of use: 12 January 2017); Human Rights Council 'The right to privacy in the digital age'

unauthorised persons. These complaints, amongst others, range from the abuse of power, in-fighting in the LEAs,[32] political interference to conflict of interest[33] by LEOs; leading to the brazen and unauthorised specific and bulk interceptions and monitoring of communications of different categories of people.

The categories of complainants include ordinary citizens, the general public,[34] influential[35] and politically connected people[36] as well as top government officials in the RSA,[37] including the former deputy president of the RSA, who almost immediately after the alleged interception of his online communication became the President of the RSA in 2018.[38]

What is unprecedented is that if the privacy of a former deputy president could allegedly and

https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (Date of use: 13 December 2017; Seetharaman D and Bindley K 'Facebook Controversy: What to Know About Cambridge Analytica and Your Data Facebook Inc.'s crisis centres on the company's most precious asset: the personal data of nearly two billion people' https://www.wsj.com/articles/facebook-scandal-what-to-know-about-cambridge-analytica-and-your-data-1521806400 (Date of use: 2 April 2018 (Seetharaman D and Bindley K https://www.wsj.com/articles/facebook-scandal-what-to-know-about-cambridge-analytica-and-your-data-1521806400 (Date of use: 2 April 2018); The U.S. Foreign Intelligence Surveillance Act (FISA) of 1978 operates under the guise of intercepting foreign online communications which George Bush used in establishing his own secret 'warrantless' eavesdropping programme. Even after the amendment of FISA, it is possible for the U.S. to spy on its ordinary citizens who are outside the U.S. without the need to obtain a warrant. This implies that any citizen of the RSA who communicates with a U.S. citizen in the RSA is being spied on which contravenes the provisions of RICA. Britain allows warrantless interception, which only requires the approval of the Home Secretary, see The Economist *Learning to live with big brother* 31. During the early days of the Cold War, former Soviet Union spied on the U.S. military, Landau *Lawful electronic surveillance in the face of new technologies* 221 and 223.

[32] Hunter and Smith at 2 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use : 27 November 2018).

[33] Bateman B 'SAPS, IPID working to avert conflict of interest in cases' http://ewn.co.za/2018/07/05/saps-ipid-working-to-avert-conflict-of-interest-in-cases (Date of use: 6 July 2018).

[34] *Primemedia v Speaker, National Assembly* supra 3, 4, 44 - 54 of majority decision and paras 55-70, 74 -76 and 80-82 of Savage J; Business Tech 'Phone tapping and signal jamming threat in SA' https://businesstech.co.za/news/general/79800/phone-tapping-and-signal-jamming-threat-in-sa/ (Date of use: 18 November 2017) (Business Tech https://businesstech.co.za/news/general/79800/phone-tapping-and-signal-jamming-threat-in-sa/ (Date of use: 18 November 2017).

[35] NIA 'Office of the Inspector-General of Intelligence, Executive Summary of the Final Report of the Findings of an Investigation into the Legality of the Surveillance Operations carried out by NIA on Mr. S Macozoma – 23 March 2006' 2, 8, 13, 17-19 and 24 (NIA 'Investigations on Mr. Macozoma').

[36] Staff Reporter 'Zille maintains her calls were being monitored' http://mg.co.za/article/2011-03-09-zille-maintains-her-calls-were-being-monitored (Date of use: 18 April 2016) (Staff Reporter http://mg.co.za/article/2011-03-09-zille-maintains-her-calls-were-being-monitored (Date of use: 18 April 2016); Staff Reporter 'NIA says it is not monitoring Zille's calls' http://mg.co.za/article/2011-03-09-nia-says-it-is-not-monitoring-zilles-calls (Date of use: 18 April 2016) (Staff Reporter http://mg.co.za/article/2011-03-09-nia-says-it-is-not-monitoring-zilles-calls (Date of use: 18 April 2016).

[37] Surveillance was carried out on a senior state prosecutor, *AmaBhungane v Minister of Justice* supra19.

[38] Letsoalo https://mg.co.za/article/2017-09-08-00-secret-funds-used-to-spy-on-cyril (Date of use: 8 September 2017); Mashego and Masondo https://www.news24.com/SouthAfrica/News/secret-plot-to-oust-mbaks-20170827-2 (Date of use: 30 August 2017; Serrao https://www.news24.com/SouthAfrica/News/senior-crime-intelligence-officials-without-top-secret-clearance-20171130 (Date of use: 1 December 2017).

unlawfully be invaded without any legal action or consequence against the infringers, then the statement that we all ''have zero privacy''[39] is inconceivable, valid and worrisome. Worse still, we have all been told in some quarters to 'Get over' the constant cry for online protection and infringement,[40] which conversely demonstrates a state of anarchy and hopelessness in protecting the right to the SOC in the RSA.

As much as the intrusion of the online privacy of a politically exposed person is shocking to the powers that be, the invasion of online privacy of ordinary individuals in the RSA is no less worrisome. This is because of the general prevailing and prominent inadequacies and challenges in the regulation of online communication in the RSA, some of which are specifically described below. Emphatically, without necessarily highlighting the specific disequilibrium throughout this study; the issues below and some other issues which are raised in this study directly, and indirect impact on the protection of the right to the SOC and the conduct of an OCI.

Firstly, there is no legal framework on the jurisprudence of the protection of the right to the SOC in section 14(d) of the Constitution of the RSA[41] that adequately addresses or equates the intrusive nature of the conduct of an OCI and its effect on contemporary online communication of privacy. As mentioned above, the right to the SOC is persuasively modelled after the European and U.S. jurisprudence on the 'secrecy of telecommunication', which expressly, adequately and unequivocally recognises and protects the independent right to the SOC.[42] This right emanates from the concept of offline secrecy of telecommunication.[43] The latter right, which originated from the protection of postal services —such as letters, postal cheques and other items sent by post—[44] was recorded in the latter part of the twentieth century in the RSA,[45] about two centuries ago in Europe and lately in the U.S.[46]

---

[39] Carr N '*Tracking is an assault on liberty* 368.
[40] Carr N '*Tracking is an assault on liberty* 368.
[41] See Chapter 3 of this study. Ruiz *Privacy in telecommunications* 1-5, 15, 20-23, 45-46, 59-67, 70, 81-83, 86-87, 143, 151-159, 171-172, 175-177, 179-257, 313-318 and 322-323.
[42] Ruiz *Privacy in telecommunications* 1-5, 15, 20-23, 45-46, 59-67, 70, 81-83, 86-87, 143, 151-159, 171-172, 175-177, 179-257, 313-318 and 322-323.
[43] Ruiz *Privacy in telecommunications* 1-5, 15, 20-23, 45-46, 59-67, 70, 81-83, 86-87, 143, 151-159, 171-172, 175-177, 179-257, 313-318 and 322-323.
[44] Ruiz *Privacy in telecommunications* 61-66.
[45] McQuoid-Mason *Privacy I* 141- 144.
[46] Ruiz *Privacy in telecommunications*1-5, 15, 20-23, 45-46, 59-67, 70, 81-83, 86-87, 143, 151-159, 171-172, 175 -177, 179 - 257, 313 - 318 and 322 – 323; Art 8 of the European Convention on Human Rights; Art 10 of the German Basic Law; *Ex-Parte Jackson*, 96 US 727 (1877); Ruiz *Privacy in telecommunications* 1-5, 15, 19, 20-21, 59-67 and 81-83, 151, 171-172, 173, 177, 179-257; Richard A Posner *The economics of justice* (1981) 272-

In the RSA, there is no Constitutional Court or Supreme Court of Appeal decision concerning the protection of the right to the SOC. However, the High Court in an attempt to proffer a remedy to this lacuna erroneously equates the volume and value of contents as well as the levels of risks and protection of information in a paper or book diary format with the voluminous, complex and sensitive digital data in a cellular phone found at a crime scene.[47] This is because most of the current judges, with due respect, do not have practical understanding in the use and application of information and communication technology and its law, though it does seem promising that future judges would close this gap.[48]

Secondly, the classification by the Constitutional Court of the three levels of the reasonable continuum of offline privacy interests in any channel of privacy communication, namely the: inner,[49] middle[50] and communal[51] sancta, is narrow, inadequate and disproportionate to protect the heterogeneous, complex and dynamic values, interests in and rights of the SOC. Furthermore, the classification is not proportionate in conducting an OCI according to the degree of serious offences identified in this study.

Thirdly, there is a dearth of specific legal framework regulating the protection of the institutional and structural management of the affairs and activities of LEAs, LEOs and the

273, 315 - 323; Solove D J 'Conceptualising privacy' *California Law Review* 2002 Vol. 90 1105 (Solove 2002 Vol. 90 *California Law Review*); *Katz v U.S.* 389 supra 347; *Maryland Penitentiary v Hayden*, 387 U.S 294 (1967); Sections 2510-2520 of Chapter 119 of Title 19 U.S.C; Chapter 36 of Title 50 of U.S.C; *Gloria Bartnicki and Anthony F. Kane, Jr. v Frederick W. Vopper, et al.* Nos. 99-1687, 99-1728 72 and 76; Chapter 18 U.S.C. § 2520(b), (c); Section 1 of the Fourteenth Amendment; Silard J 'A Constitutional Forecast: Demise of the State Action' Limit on the Equal Protection Guarantee' 1966 66 *Col L Rev* 855 (Silard 1966 66 *Col L Rev* 855); Section 2511(4)(a) and 2520 of Chapter 119 of Title 18 of U.S.C.

[47] *State v Terrence Stephan Brown* 2016 (1) SACR 206 (WCC) paras 5 and 29 (*State v Terrence Brown*); Swart https://www.msn.com/en-za/news/techandscience/your-cellphone-records-and-the-law-the-legal-loophole-that-lets-state-spying-run-rampant/ar-AAxyCpM?ocid=spartandhp (Date of use: 20 May 2018). If the digital information contained in a matchbox is printed, a cathedral will hardly contain such printed information. This statement on 'cybernetic revolution' was made with respect to the jurisprudence of privacy in the RSA as far back as 1978, see McQuoid-Mason *Privacy I* 7 - 8.

[48] Van der Merwe *Introduction* 5.

[49] *Bernstein v Bester NO* supra 18, 65, 67, 69, 77, 83 and 85; *NM & Others v Smith & Others* 2007 7 BCLR 751 (CC) 33, 130, 131 and 135 (*NM* v *Smith*) and *Ashok Rama Mistry v The Interim National Medical and Dental Council of South Africa & Others* CCT 13/97 para 27 ('*Mistry v Medical and Dental Council*'); *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributor (Pty) Ltd v Smit NO* 2001 (1) SA 545 (CC) para 15 (*Investigating Directorate v Hyundai and Smit No*); *F & Another v The Minister of Safety & Security* CCT 20/95 91 ('*F v Min of Safety* ').

[50] *NM v Smith* supra 143.

[51] Basdeo V 'The constitutional validity of search and seizure powers in South African criminal procedure' 2009 (12) 4 *PER* 2009 316/360-319/360 and 326/360-328/360 (Basdeo 2009 *PER* (12)4 316/360 - 319/360 and 326/360 - 328/360); *Bernstein v Bester NO* supra 67, 77, 83 and 85 and *NM v Smith* supra 135-136; *National Media Ltd & another v Jooste* 1996 (3) SA 262, 271 (A) (*National Media v Jooste*); *Mholongo v Bailey & another* 1958 (1) SA 370 (W) (*Mholongo v Bailey*); Section s 22 of CPA No. 51 of 1977 and ss 13(6) and 13 (7) and (8) of the SAPSA.

other relevant stakeholders in the conduct of an OCI. It is anticipated that this study will reveal that no matter how adequate the principles, practices and procedures of an OCI might be, if no adequate legal framework exists to regulate the management of the affairs of these stakeholders —including administrators and political office holders— in conducting and overseeing the conduct of an OCI, striking a balance in the conflict between the protection of the right to the SOC and the conduct of an OCI would be an exercise in futility or a mere academic gymnastic.

Fourthly, the classification of offences in the RSA[52]is inadequate, neither has the international law assisted in this regard[53] which makes the application of the proportionality principle in conducting an OCI difficult, thus adversely impacts on the protection of the right to the SOC.

Fifthly, as a corollary to the fourth problem statement, despite the decision by the Constitutional Court which emphasises that there is a need to conduct an earlier investigation into the commission of certain serious offences that are more serious than the others,[54] however, there is no specific, accurate and functional legal framework that examines or simplifies the 'seriousness and stages of crime commission proportionality' principle.[55] This principle relates to the reasonable ground standards required to conduct an OCI according to the seriousness of an offence and the appropriate timing of the investigation based on the effect or the degree of the serious offence commission.

In addition, this inadequate legal framework is exacerbated by the fact that LEOs are not required, by law, to have special knowledge or skill to conduct an OCI. These inadequacies negative the protection of the right to the SOC. Specifically, the Constitutional Court in

[52] See the fifth problem statement in this study on the six categories of serious offences propounded in this study.
[53] Sections 2, 11 and 13-17 of Maintenance Amendment Act No 9 of 2015; *Investigating Directorate v Hyundai and Smit No* supra 4; *National Commissioner of the South African Police Service & Another v Southern African Human Rights Litigation Centre, Zimbabwe Exiles' Forum and John Dugard and three others* CCT 02/14 [2014] ZACC 30 77 ('*SAPS v Zim & Dugard*'); *Powell NO and Others v Van der Merwe and Others* (503/2002) [2004] ZASCA 25; [2005] 1 All SA 149 (SCA) (1 April 2004) para 5 (*Powell v Van der Merwe Powell*); Art 6 of United Nations Office on Drugs and Crime *Model Legislative Provisions against Organised Crime* (2012) at 25 ('UNODC 'Model Legislative Provisions Against Organised Crime' 2012); Koops B-J and Goodwin M 'Cyberspace, the Cloud, and Cross-Border Criminal Investigation' (2014) 5/2016 83 *Tilburg Law School Research Paper* at 26 (Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 5/2016).
[54] *Investigating Directorate v Hyundai and Smit No* supra 1, 2, 4, 6, 7, 8, 13, 14, 27, 28, 30, 31, 33, 34, 44, 45, 46, 47, 48, 51 and 52.
[55] See Chapter Five (paras 5.3.4, 5.3.6 and 5.4) of this study.

Investigating Directorate v Hyundai and Smit No[56] and *Thint* [57] does not provide for the accurate, adequate, specific, and determinable guidance, logic, and mathematical formulae on the constitution of the standard of proof required to investigate certain serious offences at the earliest stages of crime commission. This lacuna, *ab initio*, results in some confusion, uncertainty or ambiguity in the mind or mental imagery of LEOs and other stakeholders when considering the proportionate determination of the standards of proof required not only at the stages of crime commission but also at the various degrees of serious offences commission.

The non-pronouncement or non-recognition on or of the use of some mathematical formulae by the Constitutional Court is neither due to any illegality, unlawfulness or invalidity of the application of mathematical formulae in the decision-making process of the court, nor is it due to any scientific proof or evidence-based principle to reject the merit in the use of mathematical formulae in resolving legal issues.

It is therefore submitted that the non-pronouncement on or non-recognition of the use of some mathematical formulae by the Constitutional Court is, with due respect, simply based on the unnecessarily rigid reluctance, trepidation, and unfounded argument of the court that mathematical formulae would replace the discretion of the court.[58] Respectfully, the High Court in *Intercape v Pro-Haul* innocently expresses its candid, unscientific and unequivocal view by stating that the courts believe that mathematical formulae are nothing but the usurpation of the inherent function of the court.[59] This is because the consideration or application of mathematical formulae prevents the court from applying its mind in the adjudication of cases that require usual daily or ordinary mental effort to resolve.[60]

[56] *Investigating Directorate v Hyundai and Smit No* supra 1, 2, 4, 6, 7, 8, 13, 14, 27, 28, 30, 31, 33, 34, 44, 45, 46, 47, 48, 51 and 52.
[57] *Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others* 2008 (2) SACR 421 (CC) paras 80, 127, 153, 168, 247, 252 and 257 (*Thint*). See also *Estate Agency Affairs Board v Auction Alliance (Pty) Ltd and Others Case* CCT 94/13 33, 37, 40, 41 and 63 (*Estate Board v Auction Alliance*) 63 where the Constitutional Court states that the legislature should be given the 'latitude to formulate the inner and outer reaches of the search power'.
[58] *Intercape Ferreira Mainliner (Pty) Limited v Pro-Haul Transport Africa CC & Another* Case No. 44350/2012 para 15 (*Intercape v Pro-Haul*).
[59] *Intercape v Pro-Haul* supra 15.
[60] *Intercape v Pro-Haul* supra 15.

Sixthly, section 15 of RICA recognises the proviso in section 205(1) of the CPA[61] and vice versa in which the former allows an alternative law —such as the latter— to conduct an OCI. However, the general application of section 205, which the Constitutional Court has declared as being consistent with the Constitution to conduct a preliminary investigation according to section 35 of the Constitution,[62] is defective or inadequate to strike a balance in the conflict between the protection of the right to SOC and to conduct an OCI. This is because section 205(1) does not comply with the significant import of the substantive and procedural requirements in RICA, which is the main and authoritative law that regulates the conduct of an OCI in the RSA.

Chief amongst the requirements in which the provisions of section 205 (1) the CPA do not comply with RICA provisions is section 16(2)(e) and (5)(b) and (c) which require that an OCI be conducted as an alternative method of investigation and not as a method of investigation in the first instance, save where certain exceptions apply thereto. Thus, the provisions of RICA, which are meant to strike a balance between the protection of the right to the SOC and the conduct of an OCI, are rendered ineffective by the application of section 205 of CPA, given that LEOs now resort to section 205 as a short-cut in the procedure in RICA or an unethically preferred way of conducting an OCI.[63]

Interestingly, the seventh point to consider is that some LEAs or LEOs engage in fraudulent misrepresentation in many instances when presenting facts before the court in the conduct of an OCI. This is due to the conduct of LEAs or LEOs who intercept an online communication of an individual without an interception direction[64] or without such interception falling under any of the exceptions in RICA, which do not require an interception order.[65]

---

[61] Criminal Procedure Act ('CPA') No. 51 of 1977 ('CPA'); Basdeo 2012 2 *SACJ* 206; See also the application of ss 81, 82(3) and (4), 83 and Chapter XII of ECTA in relation to the conduct of OCI.

[62] *Nel v Le Roux No & Others* Case No: CCT 30/95 paras 4, 6, 7, 8, 9, 10, 11, 14, 25 and 27 (*Nel*); *Haysom v Additional Magistrate, Cape Town and another* 1979(3) SA 155 (C) (*Haysom*) and *State v Matisonn* 1981(3) SA 302 (A) (*State v Matisonn*).

[63] *State v Naidoo* 1998 1 *SACR* 479 (N) paras 485 A-C, 516D-517D, 521A-J, 531C-J (*State v Naidoo*); *State v Norbert Glenn Agliotti* case No SS 154/2009 paras 135-137 and 146.1 ('*State v Agliotti'*); *State v Miller* supra 15-26, 33, 34; *S v de Vries and others* 2009(1) SACR 613 (C)(*S v de Vries***).** Parliamentary Committee No 164-2016 at 40; Swart https://www.msn.com/en-za/news/techandscience/your-cellphone-records-and-the-law-the-legal-loophole-that-lets-state-spying-run-rampant/ar-AAxyCpM?ocid=spartandhp (Date of use: 20 May 2018); Hunter and Smith at 4 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use : 27 November 2018).

[64] Swart https://mg.co.za/article/2011-10-14-secret-state/ (Date of use: 12 December 2016).

[65] Sections 4 - 11 of RICA.

In practice, some LEAs or LEOs fraudulently apply to court after unlawfully intercepting an online communication and filing the same unconstitutionally obtained information to secure an interception order and make the subsequent interception appear legitimate, whereas it is *de facto* and *de jure* illegitimate.[66] Worse still, in many cases, LEAs do not even bother to apply to the court to obtain a direction to conduct an OCI after fraudulently gathering information from online communication.[67] Thereafter, LEAs resort to a full-scale offline investigation based on the unlawfully gathered information in online communication on the alleged crime commission, thus, the LEOs feign to make the unlawfully obtained offline evidence look lawful; whereas, it is not lawful.

One of the causes of unlawful interception referred to above is the abuse of the current inadequate or non-existing legal framework relating to the technical configuration of the various interception devices.[68] In reality, the authorities, entities and individuals unlawfully intercept online communications[69] due to the absence of configuration of a quadripartite techno-legal interdependent interception device or system for the conduct of an OCI,[70] as proposed in this study. *Popoola QOCI* system prevents an authority, entity or individual in the OCI process from having access to the interception device without a corresponding consent from the other authority in the quadripartite system amongst the LEAs, court, Online Communication Service Provider and Interception Centre.[71]

Generally, the authorities, entities and individuals that abuse the current system include: LEAs or LEOs who in their personal capacity fail or refuse to comply with the constitutional provision that prohibits the unlawful conduct of OCI;[72] LEAs who do not generally understand

[66] Swart https://mg.co.za/article/2011-10-14-secret-state/ (Date of use: 12 December 2016).
[67] Swart https://mg.co.za/article/2011-10-14-secret-state/ (Date of use: 12 December 2016).
[68] Maphumulo S 'Cops in Spy Gadget Probe- Hawks' Damning Investigation Set to open Can of Worms' 2016-08-30 *The Sunday Independent* 1 (Maphumulo 2016-08-30 *The Sunday Independent*)**;** Maphumulo S 'Senior Official helped bring in Grabber-Assistant Director at Centre of Hawks Probe was Rewarded for His Role' 2015-11-03 *The Star* November 2 (Maphumulo 2015-11-03 *The Star* 2).
[69] Swart https://mg.co.za/article/2011-10-14-secret-state/ (Date of use: 12 December, 2016); Business Tech https://businesstech.co.za/news/general/79800/phone-tapping-and-signal-jamming-threat-in-sa/ (Date of use: 18 November 2017); Hunter and Smith at 2 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use : 27 November 2018).
[70] The Respondents Affidavit in *AmaBhungane v Minister of Justice* supra 139 indicates the configuration capacity for LEAs. Although section 41(5) of the CCB provides for online transmission by the court to a member of the LEA in order to execute a preservative order, the provision does not create a quadripartite system nor establish an online hearing application system to conduct an OCI.
[71] Paragraph 6.11 of this study.
[72] Section 51 of RICA.

the technicalities involved in conducting an investigation[73] and LEAs or LEOs who execute general unlawful orders from the authorities.[74] Other abusers of the current system include unauthorised officers of the Interception Centre;[75] the NCC and Telecommunication Service Providers[76] as well as those mischievous individuals in the society who conduct interceptions with their unlawfully acquired interception devices.[77]

The eighth pertinent problem is that, as a corollary to the seventh problem in this study, the irony of the conduct of an OCI is that the legal framework of an OCI, being an online investigative procedure, does not provide for the hearing of an online application system that enables the use or configuration of an online or audio-visual[78] application system to conduct an efficient and effective OCI. The current use of an offline application filing system and the physical hearing of such an application is frustrating,[79] slow and time-consuming in conducting an OCI, which is supposed to be a fast, efficient and effective procedure.

The complaint of the erstwhile RICA judge in the report of the JSCI of Parliament partially corroborates the cumbersome administrative offline application system in the RSA.[80] Although she suggested the use of an electronic filing system in her report as a remedy to the problems stated therein,[81] nevertheless, the suggestion is still not adequate for the effective and efficient conduct of an OCI. Her suggestion is similar to the use of the tele-warrant system in Canada, which provides that a LEA can simply apply for an OCI via telephone communication or other means of online communication.[82]

---

[73] Moster D *Utilisation of the Financial Intelligence Centre as a crime intelligence source* at i (M. Tech Dissertation Unisa 2012)

[74] Section 199 (5) & (6) of the 1996 Constitution.

[75] Maphumulo 2016-08-30 *The Sunday Independent* 1; Maphumulo 2015-11-03 *The Star* 2.

[76] Swart https://mg.co.za/article/2011-10-14-secret-state/ (Date of use: 12 December 2016).

[77] *Okundu v State* CA&R117/16 2016 (ZAECGHC) 131 paras 4 -6, 7, 9, 11 – 13 and 16 – 26 (*Okundu v State*); Swart https://mg.co.za/article/2011-10-14-secret-state/ (Date of use: 12 December 2016).

[78] Articles 18(18) and 24(2)(b) and (4) of United Nations Convention against Transnational Organized Crime (TOCC) 2000 and Art 25(3) of CoE CoCC.

[79] Cassilly J I 'Geolocational Privacy and Surveillance Act' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 270 (Cassilly *Geolocational Privacy and Surveillance Act*).

[80] Parliament of the Republic of South Africa 'Announcements, Tablings and Committee Report' No 164-2016 https://www.parliament.gov.za/storage/app/media/Docs/atc/616458_1.pdf (Date of use: 14 January 2017) 56 (Parliament of the RSA https://www.parliament.gov.za/storage/app/media/Docs/atc/616458_1.pdf (Date of use: 14 January 2017).

[81] Parliament of the RSA https://www.parliament.gov.za/storage/app/media/Docs/atc/616458_1.pdf at 56 (Date of use: 14 January 2017).

[82] Hubbard R W, Brauti P M and Fenton S K *Wiretapping and other electronic surveillance: Law and procedure* – Vol. 1 (2013) 2-16.3 and 3-20.4h. (Hubbard, Brauti and Fenton *Wiretapping*).

It is noted that although the CCMA commissioners now officially use telephonic-audio-communication in conciliation hearing in the ADM[83] mechanism in the RSA,[84] it is still inadequate to address the needs of an OCI as opposed to the proposed *Popoola QOCI* interdependent interception device application and execution process.[85]

The ninth problem is that no legal framework exists in the RSA regarding the application or otherwise of the U.S. principle of '*no server, no law*'[86] when conducting an OCI on the Internet in the RSA. The U.S. principle states that an OCI cannot be conducted on the Internet by LEAs in the RSA without first seeking and obtaining consent from the U.S. authorities.

The U.S. principle does not only undermine the effective and efficient conduct of an OCI and infringe the right to the SOC of the public in the RSA, but from many perspectives, breaches the constitutional cyber sovereign mandate of the RSA to conduct an OCI within its territory. It is not surprising therefore that this principle has been rejected by the courts in other

[83] It is submitted that no conflict or dispute is generally ever resolved, rather a conflict or dispute is only managed because there is still an element of the effect of the conflict or dispute hanging over or re-occurring between the parties, therefore it is erroneous to continue to use the word 'resolution'. Put differently, in a graphical representation, a conflict or dispute does not generally go back to the zero level on the vertical line in the graph but becomes parallel with the horizontal line or even escalate again.

[84] *Pioneer Foods (Pty) Ltd t/a Sasko Milling & Baking (Duens Bakery) v CCMA* (2011) 32 ILJ 1988 (LC) paras 17 and 48 (*Pioneer Foods v CCMA*). Relating the rationale in the case of *Pioneer Foods v CCMA* to the urgency required to conduct an OCI, it is submitted that where a CCMA commissioner placed a telephone call to a party in a Con-Arb proceedings in ADR to inquire about the absence of the representative of the party who explained what transpired for his absence and requested for postponement may amount to the hearing of an application in OCI proceedings; Wiese T Alternative dispute resolution in South Africa- Negotiation, mediation, arbitration and ombudsmen (2016) 123-124 (Wiese *ADR in SA*). Section 68(7)(d)(ii) of ECA. See also Kleve P, De Mulder R V & Van Der Wees J G L 'Re-engineering Dispute in an EDI-environment' Law' 1995 Vol. 4 No 1 *Computers & Artificial Intelligence* at 25- 32. **(**Kleve, De Mulder and Van Der Wees 1995 Vol. 4 No 1 *Computers & Artificial Intelligence* 25).

[85] Para 6.11 of Chapter 6 of this study.

[86] *Yahoo! Inc* [2015] Court of Cassation of Belgium P.13.2082.N. (*Yahoo! Inc* [2015]); e.g. *Yahoo! Inc* [2013] Belgium Court of Appeal of Antwerp, 12th chamber for criminal cases 2012/CO/1054 (*Yahoo! Inc* [2013]); *eBay Canada Ltd v M.N.R.*(2008), 330 D.L.R (4th) 360, 53 B.L.R (4th) 202 (F.C.A) 3, 17, 48 and 51 (*eBay Canada*); *UEJF et Licra* c. *Yahoo! Inc. et Yahoo France* 22 mai 2000 (Tribunal de Grande Instance Paris), 2000 Communication et Commerce Electronique (Comm. Com. Electr. Comm. n°92, note J-Chr. Galloux) (*UEJF et Licra* c. *Yahoo! Inc. et Yahoo France*); *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp*., 13 Mag. 2814 WL 1661004 (S.D.N.Y. 2014) (*Microsoft I*); *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp*., No. 14–2985 (2d Cir. 2016) 2 (*Microsoft II*); Osula A *Remote search and seizure of extraterritorial data* (PhD thesis) (2017) 25 and 31 (Osula *Seizure of extraterritorial data*) 25 and 31; Michaels R 'Some Fundamental Jurisdictional Conceptions as applied in Judgment Conventions' 9-10 https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2281&context=faculty_scholarship (Date of use: 21 March 2016 (Michaels https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2281&context=faculty_scholarship (Date of use: 21 March 2016).

jurisdictions[87] such as Belgium,[88] Canada,[89] France[90] and Ireland,[91] all of which is corroborated by some domestic and international techno-legal arguments canvassed in this study.

In the tenth problem, the offline conscription principle, in terms of the confession and other statements made by an individual, usually regards unconstitutionally obtained evidence as inadmissible,[92] which is generally challenging.[93]

In online communication, there is the absence of a legal framework by the Constitutional Court while there are erroneous decisions by the Supreme Court of Appeal and High Court on the applicability of offline conscription and its admissibility to the conscription of online communication where an OCI is conducted.

The obvious implication is that the outright denial of the existence of conscription in online communication by the courts makes it difficult for the objective consideration of the application of section 35(5) of the Constitution in appropriate cases of admissibility of online conscription and its exception, as one of the final consequences or steps in the conduct of an OCI.

Consequently, this denial adversely influences the effective and efficient conduct of an OCI and subsequently, the fairness or otherwise of the trial or the administration of justice when considering the application of section 35(5) of the Constitution. However, as the High Court in *AmaBhugane v Minister of Justice* quotes the recommendation of the United Nations on the need for the adequate application of proportionality principle,[94] this study attempts to establish the existence of the concept of online conscription and proposes some proportionality principles —all through in this study— to address the inadequacies in the admissibility of unlawfully obtained online evidence in the RSA.

---

[87] Ax J 'U.S. judge orders Microsoft to submit customer's emails from abroad' http://www.reuters.com/article/2014/07/31/usa-tech-warrants-idUSL2N0Q61WN20140731 (Date of use: 18 March 2016 (Ax http://www.reuters.com/article/2014/07/31/usa-tech-warrants-idUSL2N0Q61WN20140731 (Date of use: 18 March 2016).

[88] *Yahoo! Inc* [2015] supra and *Yahoo! Inc* [2013] supra; Osula *Seizure of extraterritorial data* 25 and 31.

[89] *eBay Canada* supra 3,17, 48 and 51.

[90] *UEJF et Licra* c. *Yahoo! Inc. et Yahoo France* supra.

[91] *Microsoft I and Microsoft II*.

[92] Section 35(5) of the Constitution; Van der Merwe S E 'Unconstitutionally obtained evidence' in Schwikkard P J and Van der Merwe S E *Principles of evidence* 4th ed. (2016) 198-201 (Van der Merwe S E *Unconstitutionally obtained evidence*).

[93] Van der Merwe *Unconstitutionally obtained evidence* 257.

[94] *AmaBhungane v Minister of Justice* supra 91, 95 and 96.

1.3 RESEARCH QUESTION

This study seeks to provide an answer to the main hypothesis: what measures are necessary for striking a balance in the conflict in the principle, practice and procedure between the protection of the right to the SOC and the conduct of an OCI in the RSA? More specifically, the following sub-questions are posed to provide an adequate response to this question:

1.3.1 Despite the development of 'quick-silver' information and communication technology; are the broad privacy jurisprudence —particularly section 14(d) of the Constitution and the statutes in the RSA on privacy protection— adequate[95] to protect the activities, values, interests and severe risks in or involved in the use and protection of the conscriptive, interoperable, non-compartmentalised and non-passworded-compartmentalised online communication in the RSA? [96]

1.3.2 How could LEAs, LEOs and the other relevant stakeholders be competent, impartial, independent, transparent and accountable in respectively conducting and overseeing the conduct of an OCI without having specific, comprehensive and adequate legal institutional and structural framework regulating:[97]

1.3.2.1 the respective professionalism in the activities, functions or services involved in the conduct and oversight of the conduct of an OCI as a specialised, autonomous or independent function or activity which is distinct from the general security or intelligence functions or services?

1.3.2.2 the requirements of special knowledge, experience, training or skill in the employment, retention, deployment and execution of the function of LEOs and the other relevant stakeholders in respectively conducting and overseeing the conduct of an OCI?[98]

[95] Basdeo 2012 2 *SACJ* 196.
[96] This question is answered in Chapters 2 and 3 of this study.
[97] The questions below are answered in Chapter 4 and paras 6.7, 6.8, 7.3 and 7.6 of this study.
[98] Applicants Affidavit in *AmaBhungane v Minister of Justice* supra 175.3.

1.3.2.3 the independent operation and funding of an OCI as a specialised system, and unit in the security or intelligence services cluster?

1.3.2.4 the accountability[99] and oversight of and by LEAs, LEOs and other relevant stakeholders in respectively conducting and overseeing the conduct of an OCI?

1.3.3 Given that that there is no absolute protection of any right and that there is a public criminal interest or need to investigate crime, what substantive and procedural measures should be adopted to limit the right to the SOC and specifically? Most importantly, how can the proportionality principle (which is applicable in various ways in this study) be specifically formulated[100] —in terms of some mathematical and non-mathematical formulae— in the determination of the factual matrices standards required to substantively and procedurally conduct an OCI in the various classes and timing of the commission of offences?[101]

1.3.4 How does the existing legal framework on the application for and issuance of an OCI direction and the pre-and post-execution of an OCI direction prohibit the incessant brazen, wilful, and unauthorised specific and bulk interceptions of online communications in the RSA?[102]

1.4 OBJECTIVES OF THE STUDY

The overarching objective of the study is to investigate the measures that are necessary for striking a balance in the conflict in the principle, practice and procedure between the protection of the right to the SOC and the conduct of an OCI in the RSA in the twenty-first-century conscriptive, interoperable, non-compartmentalised and non-passworded-compartmentalised online communication. In ensuring the achievement of the main objective and providing answers to the research questions, the following sub-objectives are considered:

[99] *Primemedia v Speaker, National Assembly* supra 72, 75 and 76.
[100] This question is answered in Chapter 5 of this study.
[101] This question is answered in paras 6.3 - 6.6 of Chapter 6 of this study.
[102] This question is answered in chapters 6 and 7 of this study.

1.4.1 To examine the adequacy of the protection of the right in online communication in the broader privacy jurisprudence in section 14(d) of the Constitution and the statutes on privacy protection in the RSA (including a comparison between online and non-online communications), the duty of care by stakeholders in protecting the right in online communication and the significance of the imposition of sanctions thereof for non-compliance with the duty of care.[103]

1.4.2 To examine the adequacy of professionalism, competence, operations and independence of LEAs, LEOs and other relevant stakeholders in respectively conducting and overseeing the conduct of an OCI in the RSA based on the provision of specific and comprehensive legal, institutional and structural framework regulating, in particular:[104]

1.4.2.1 the professional activities, functions or services involved in the conduct and oversight of the conduct of an OCI as a specialised activity which is different from the general investigative, intelligence or security services.

1.4.2.2 the requirements for special knowledge, training, skill or experience in the employment, retention, deployment and execution of the function of LEOs and other relevant stakeholders in conducting an OCI[105] as a specialised method of investigation.

1.4.2.3 the independent funding[106] and techno-legal operation of an OCI as a specialised method, system, and unit in the investigative, security or intelligence services cluster.

1.4.2.4 the accountability[107] and oversight of and by LEAs, LEOs and the other stakeholders in respectively conducting and overseeing the conduct of an OCI as a specialised method of investigation.

[103] Chapter 3 of this study.
[104] Chapter 4 and paras 7.3, 7.5 and 7.6 of this study.
[105] Applicants' Affidavit in *AmaBhungane v Minister of Justice* supra 175.3.
[106] For example, low budgetary allocation generally incapacitates IPID, see IPID 'Briefing to the Select Committee on Security & Justice on IPID's Budget 2017/18 and Annual Performance Plan (2017/18)' (2017) 32; Mokgosi L 'The Telecommunications Regulators' in 'Thornton L et al (eds) *Telecommunication law in South Africa* (2006)' 103 and 121 (Mokgosi *the telecommunications regulators*).
[107] *Primemedia v Speaker, National Assembly* supra 72, 75 and 76.

1.4.3 To examine the adequacy of the limitation of both the right to the SOC and the duty of LEAs to conduct an OCI of serious offences. The examination includes the adequacy of the formulation of some mathematical and non-mathematical formulae[108] in the proportionality principle —as one of the section 36 constitutional limitation clauses— in determining the factual matrixes standards required to conduct an OCI in the various classes and timing of commission of serious offences.[109]

1.4.4 To explore the substantive and procedural legal framework on the application for and issuance of an OCI direction and the pre-and post-execution of an OCI direction.[110]

1.5 SIGNIFICANCE OF THE STUDY

Given the various inadequacies identified in this study most of which have not been the subjects of litigation at the Constitutional Court to exercise its constitutional muscle, the outcome of this study is significant in the following ways.

First of all, in rebutting the pessimism on the prediction of the court in *State v Miller*[111] that the development of rules required for the search of a seized cellular telephone is not in sight in the nearest future, this study emphatically and timeously highlights the necessity by government and the stakeholders to appreciate or acknowledge the inadequacies in the conduct of an OCI and urgently address the issues raised, as may be required in this study. Such address will set the scene for extensive, productive and effective regulatory and policy debate, and reform by Parliament, court, LEAs, scholars and society, all of whom will be opportune to be abreast of the developments of the framework on the conduct of an OCI in the RSA and other jurisdictions.

---

[108] The mathematical formulae aspect of the limitation of the right to the SOC is addressed in para 6.4 of Chapter 6 of this study.

[109] Chapters 5 -7 of this study.

[110] Chapters 6 and 7 of this study.

[111] Gamble J in *State v Miller* supra 61 observes as follows:

> 'Law enforcement officers need clear rules regarding searches incident to arrest, and *it would take many cases and many years for the courts to develop more nuanced rules.* And during that time, the nature of the electronic devices that ordinary Americans carry on their persons would continue to change'.

This study is also aimed at negotiating and contributing towards the development and enforcement of global uniform best principles, practices and procedures in the jurisprudence of the protection of the right to the SOC and the conduct of an OCI. It has been reported lately that RICA needs urgent review.[112]

In addition, this study, specifically, opens up an opportunity for LEAs (as the main case study in this study) to, pending the consideration for an amendment of the constitution, various laws, regulations and policies to strengthen the values in online communication protection and OCI conduct; positively and immediately respond to the knowledge gap in the field of OCI by reviewing their principles, practices and procedures when conducting an OCI in a way that the review does not constitute a constitutional incongruity.

Accordingly, the conduct of this study at an LL. D degree level will provide an opportunity for debate and reform, as it is designed to contribute to the immediate development and enforcement of global uniform best principles, practices and procedures in the protection of the right to the SOC and the conduct of an OCI in the public interests. In addition, it is believed that the study will be used to disseminate knowledge through several fora.

Furthermore, it is believed that the issues raised in this study will be considered as part of the formulation of curriculum or content development in and contributions to cyber law textbooks and peer-reviewed articles respectively in the areas of online communication protection and investigation.

Finally, this study further creates awareness on and lays the foundation for the discourse on the future role and impact of the deployment of artificial intelligence and machine learning in robotic law, particularly in the use of a robotic LEO in automatically conducting an OCI as described in this study.[113]

[112] Parliament of the Republic of South Africa 'Announcement, Tablings and Committee Reports' No 164 -2016 para 4.7.4 at 21.
[113] Paras 2.11.4, 6.4.9 and 6.11 of this study.

1.6 RESEARCH METHODOLOGY

This study is strictly limited to non-empirical, desk-top research and library-based approach.[114] Given the covert, intrusive, risky and sensitive nature of conducting an OCI by LEAs or LEOs, it would be a Herculean task or even impossible to carry out a quantitative study to collate data with the use of a questionnaire or other methods from LEAs,[115] amongst other stakeholders, who are compelled to comply with the secrecy oath requirements in pursuance of their contracts of employment.

Therefore, the research approach is qualitative[116] which is subject to the dynamics of issues addressed in this study. The research design is analytical, descriptive, prescriptive[117] and more importantly, largely argumentative because of the nature of this study which deals the conflict between the protection of the right to the SOC and the conduct of an OCI, highlighting numerous techno-legal inadequacies.

While this study primarily focuses on the RSA, however, *reference* is *summarily* made to some jurisdictions that have same, similar or even dissimilar provisions, principles, practices and procedures to the RSA to arrive at an informed opinion that will stand the test of time, [118] notwithstanding the expected changes in technology.

---

[114] McConville M and Chui W H (eds) 'Introduction and overview' in *Research methods for law* (2014) 1-4 (McConville and Chui (eds.) *Introduction and overview*); Hutchinson *Doctrinal research* 8; Burton M 'Doing empirical research – Exploring the decision making of magistrates and juries' in Watkins D and Burton M (eds.) *Research Methods in Law* (2018) 66-70 (Burton *Doing empirical research – Exploring the decision making of magistrates and juries*);Westerman P C 'Open or Autonomous? The debate on legal methodology as a reflection of the debate on law' in Van Hoecke M *Methodologies of legal research- What kind of methods for what kind of discipline?* (2013) 108-110 (Westerman *The debate on legal methodology as a reflection of the debate on Law*); Pendleton M 'Non-empirical discovery in legal scholarship- Choosing, researching and writing a traditional scholarly article' in McConville M and Chui W H (eds.) *Research methods for law* (2014) 159- 160 (Pendleton *Non-empirical discovery in legal scholarship- Choosing, researching and writing a traditional scholarly article*). It is however noted that Epstein and King opine that empirical research is 'based on observations of the world' comprising both qualitative and quantitative research, see Dobinson I and Johns F 'Qualitative legal research' in McConville M and Chui W H (eds.) *Research methods for law* (2014) 16-18 (Dobinson and Johns *Qualitative legal research*).

[115] Dobinson and Johns *Qualitative legal research* 16-41; Chui W H 'Quantitative legal research' in McConville M and Chui W H (eds.) *Research methods for law* (2014) 46- 63 (Chui *Quantitative legal research*); CBC Radio 'British student jailed for life in U.A.E. on spy charges 'totally innocent': PhD supervisor' https://www.cbc.ca/radio/asithappens/as-it-happens-thursday-edition-1.4916477/british-student-jailed-for-life-in-u-a-e-on-spy-charges-totally-innocent-phd-supervisor-1.4916485 (Date of use: 24 November 2018).

[116] Dobinson and Johns *Qualitative legal research* 16-41; Chui *Quantitative legal research* 46-63.

[117] Bathia K L and Srivastava S C *Legal method, reasoning and research methodology* (2014) 237-238 (Bathia and Srivastava *Legal method, reasoning and research methodology*); NYU 'What is research design?' https://www.nyu.edu/classes/bkg/methods/005847ch1.pd f (Date of use: 23 October 2018).

[118] Ackermann L W 'Constitutional comparativism in South Africa' (2006) Vol 123 Issue 3 *SALJ* (Ackermann 2006 Vol 123 Issue 3 *SALJ*) 497, 502 -510 and 514 - 515.

It should be noted that reference to such jurisdictions is made with caution[119] *to prevent unintended comparative research with such jurisdictions*, given that a comparative study will deny one the opportunity of making a comprehensive development of the jurisprudence of the important issues identified in this study about the RSA.

This study relies on the analysis of both primary and secondary sources.[120] The primary sources include the Constitution, legislation, case law, regulation, policies and international and regional instruments and agreements, while the secondary sources will include books, published articles and newspaper reports.[121]

1.7 SCOPE AND LIMITATION OF THE STUDY

The overall scope of this study covers the principles of, practices and procedures in the techno-legal aspects of the protection of the right to content and meta or traffic data online communication or the six online communication devices. It also covers the management by LEAs or LEOs of the conduct of an OCI in the RSA (as the case study) of serious offences committed offline and in online instances in or outside the RSA, but which the RSA has the cyber territorial jurisdiction to conduct an OCI, provided the target of an OCI conduct is a user of an online communication service within the territory of the RSA.

Although reference may be made to other methods of investigations in passing,[122] however, the object of reference to other methods of investigation is to determine the higher (or highest) risk and protection levels in the investigation between online communications and non-online communications and in turn, determine the levels of regulation required in the conduct of an OCI in the RSA.

The limitations of this study are as follows:

---

[119] *Primemedia v Speaker, National Assembly* supra 71.

[120] Campbell E, Poh-York L and Tooher J *Legal research materials and methods* (4th ed.) (1996) 2-6 (Campbell, Poh-York and Tooher *Legal research materials and methods*); Hoffman M and Rumsey M *International and foreign legal research: A course book* (2008) 7-12 (Hoffman and Rumsey *International and foreign legal research*).

[121] Campbell, Poh-York and Tooher *Legal research materials and methods* 2-6; Hoffman and Rumsey *International and foreign legal research* 7- 12.

[122] For example, reference may be made to offline electronic investigation which occurs where an electronic device e.g., a cell phone or computer is *physically* seized, searched, intercepted or monitored by LEOs or individuals.

To begin, save in offline privacy protection and investigation cases where the Constitutional Court has made some pronouncements, this study is limited by the dearth of cases and literature in online communication and investigation in the RSA. Therefore, there is the need for the comprehensive building blocks to distinguish between the offline and online forms of privacy. It would not have been necessary to have some building blocks if there was a plethora of cases on the jurisprudence of online communication and investigation in the RSA from which mere reference to such cases would suffice to easily or summarily establish a legal point in the relevant instance.

Moreover, related to the above issue are the astonishingly technical nature and features of information and communication technology, low level of development of jurisprudence on the right in online communication and duty to conduct a covert OCI in contemporary society.[123] All of this requires extensive explanation and distinction when applying the legal aspects of the issues raised, thus, this study is ultimately limited by the number of words approved by the authorities, though this study still adequately conveys the expression of the intention of every point raised in this study.

Therefore, *this study is unable to conduct a comparative study with another country* which would require an in-depth examination of issues in both countries. The inability to conduct a comparative study is to ensure that as many germane issues affecting the RSA as possible are covered in this study to adequately develop the jurisprudence of online communication protection and OCI conduct in the RSA. However, *reference is summarily made to other jurisdictions without further ado to substantiate a position in this study*.[124]

It is strongly noted that this study does not intend to make reference to the jurisprudence of other jurisdictions as a *stare decisis* in the jurisprudence of any issue raised in the RSA. Essentially, it needless to state that reference to the jurisprudence of other jurisdictions is perforce generally persuasive in this study. It is further noted that, given the undeniable global uniform nature and features of online communication devices, technologies, networks, applications and services; not making reference to some foreign jurisprudence is tantamount to

[123] It is submitted that one lunar calendar year is three months in the field of ICT innovation and creativity.
[124] Ackermann 2006 Vol 123 Issue 3 *SALJ* 497, 502 - 510 and 514 - 515.

placing the RSA on a cyber jurisprudential island, which will be fallacious and counter-productive to the objective of this study.

Third and finally, although some political issues are raised in this study, however, there is no intention to delve into the political arena of the legal issues raised in this regard.

1.8 OUTLINE OF THE THESIS

In pursuance of the methodology of this study, Chapter One identifies the inadequacy of protection of the right in online communication, which should not be protected as an extension of the broad concept of privacy right in the Constitution. Rather, the right in an online communication should be protected as an independent right to the secrecy of online communication which will be at equilibrium with the conduct of an online criminal investigation provided adequate measures are put in place to address the abuse in this method of investigation.

Chapter Two describes and explains the complex and delicate practical operations of the techno-legal nature and features of online communication and OCI, which are central to the comprehension, integration and examination of issues in subsequent chapters in this study.

Regardless of whether the need to advance the debate on the protection of the right to the SOC is dependent on the conduct of an OCI, Chapter Three applies a multi-dimensional or holistic approach in its objectives to justify the need for the techno-legal protection of the right to the SOC in the RSA. This approach, which is *totally different* from previously applied approaches by other authors in the protection of the privacy, seeks to achieve the following main substantive and non-substantive law objectives.

Given the central and indispensable role that LEAs or LEOs play in the conduct of an OCI, which is the other side of the coin in this study, Chapter Four investigates the legal framework on the institutional and structural independence and transparency of the management of the affairs and activities of LEAs or LEOs in the RSA. In particular, this study examines the different thresholds for the appointment and skills required of LEOs, the operations and funding and the accountability and oversight of the six categories of LEAs recognised by RICA

in conducting an OCI in the RSA, keeping in mind the basic principles of separation of powers and checks and balances, amongst other principles.

Chapter Five applies the limitation principles to this study, with greater emphasis on the constitutional limitation of the right to the SOC. In addition, this chapter does not only serve as a direct or indirect way of limiting the powers of LEAs in the conduct of an OCI but also provides guidelines for the effective examination of subsequent chapters in this study.

Chapter Six examines the substantive and adjectival requirements for the application and issuance of a direction for the conduct of an OCI in the RSA.

Chapter Seven examines the role of stakeholders between the pre-and post-execution of an OCI to conclude the process involved in the conduct of an OCI in the RSA.

Chapter Eight does not only summarise the key findings in this study but proffers some key recommendations in pursuance of the findings made in chapters two to seven of this study.

My peaceful voyage to and in life is determined and influenced by the innovative and invaluable yet by the respective unpredictable, adverse and disgruntled online technologies and forces I do not understand, neither does anyone custodially comprehend their components, which aggravatingly become more complex and riskier, in particular, by the constant and endless hovering of the eagles with an aerial microscopic view of how I breathe in my online closet.

CHAPTER 2: THE TECHNO-LEGAL ASPECTS OF THE NATURE AND FEATURES OF ONLINE COMMUNICATION AND CRIMINAL INVESTIGATION

2.1 INTRODUCTION

This chapter describes and explains the complex and delicate practical operations of the techno-legal nature and features of online communication and OCI,[125] which are central to the comprehension, integration and examination of issues in subsequent chapters in this study. In some instances where the techno-legal regime is inadequate, a clinical analysis of the nature and features is conducted.

For instance, a critique is carried out on the self-imposed U.S. 'no server, no law' principle which hinders the effective conduct of an OCI in the RSA.[126] This principle controversially requires other countries —including the RSA— to seek for and obtain consent from the U.S. authorities before conducting an OCI in an Internet-based system despite committing a serious offence in the RSA.[127]

[125] This is one of the most used abbreviations in this study which is listed under the 'key words' at the abstract page, therefore, it may not be written in full in subsequent appearances.
[126] This is one of the most used abbreviations in this study which is listed under the 'key words' at the abstract page, therefore, it may not be written in full in subsequent appearances.
[127] For the examination of this controversial issue, see para 2.8 of this chapter.

2.2 THE USE OF ONLINE COMMUNICATION CHANNEL AS A PLATFORM FOR CONDUCTING CRIMINAL INVESTIGATION

2.2.1 Introduction

In this study, five channels of communication are identified through which contents, information or data can be communicated. The channels are broadcasting,[128] human agency, offline electronic communication,[129] online communication and postal services,[130] which relatively serve as platforms for law LEAs to conduct a criminal investigation.

Amongst these five channels, an online communication channel[131] is the object of examination in this study as opposed to an 'offline electronic communication' channel. These two channels are categorised under 'electronic communication', which is a broad and general term used in the society, which also includes broadcasting communication and other related types of electronic communications.

In online communication, six devices are considered in this study, which are landline telephone, facsimile machine, two-way radio communication, Internet, mobile cellular

[128] Wakefield A 'SA to miss digital migration deadline, but govt. says don't worry' http://www.news24.com/SouthAfrica/News/SA-to-miss-digitial-migration-deadline-but-govt-says-dont-worry-20150616 (Date of use: July 4 2015) (Wakefield http://www.news24.com/SouthAfrica/News/SA-to-miss-digitial-migration-deadline-but-govt-says-dont-worry-20150616 (Date of use: July 4 2015).

[129] For example, a computer which does not have an online connectivity but which has a memory stick which can be used for communication via copying of data into or from a memory stick is an offline electronic communication device as opposed to the use of the term '*online*' or 'cyber' device, which is the gravamen of this study, see generally paras 3.5.7.1 -3.5.7.15 of Chapter 3 of this study.

[130] Wakefield http://www.news24.com/SouthAfrica/News/SA-to-miss-digitial-migration-deadline-but-govt-says-dont-worry-20150616 (Date of use: July 4 2015). For the examination of the similarities and dissimilarities or distinction in these channels of communication of privacy, see generally paras 3.5.7.1 - 3.5.7.15 of Chapter 3 of this study. Section 1 of the POPIA.

[131] '*Online* communication' can also be referred to as 'on-demand *online* communication'. These two terms mean the same thing but for ease of reference, an *online* communication seems to be simpler, concise and specific term, which will be preferred to in this study as '*o*' communication, for example *o-mail*, instead of using the term 'e-mail' because the term electronic communication is too broad to convey the distinction between online communication as a unique form of electronic communication and offline electronic communication.

telephone and o-tag[132] system[133] in which an online agent assists in the transmission, and storage of the communication, thus making them 'indirect' means of communication in the context of this study.[134]

However, it is submitted that this study does not adopt the erroneous decision of the court in *Jamieson v Sabingo*, which describes telex and fax communications as 'direct' means of communication.[135] The fact that individuals are directly communicating through telex and fax with one another does not make the communication direct because a third party is in between their communication, which makes it an indirect communication.

2.2.2 Basic features of online communication

2.2.2.1 Online communication as an on-demand online communication

It is submitted that an online communication or on-demand online communication is characterised by an online networked, two-way (although sometimes one-way),[136] self-activated or initiated, voluntary (sometimes compulsory, such as an o-tag device), interactive[137] and self-participatory communication with or by a user by the connection of online networks by service providers or operators. Online communication is distinguished from a broadcasting communication, which is static[138] and always one-way communication. A broadcast does not have all the features described above in online communication.

---

[132] It is noted that for purposes of clarity in the use of terminology in this study, instead of using 'e-toll', rather '*o-toll*' will be used, which means '*online-toll*'. This is because the use of the word 'electronic' seems too broad. The scope of this study distinguishes between an online communication, which is connected to an online communication network and is the gravamen of this study as opposed to an offline communication which is not connected to a network. The latter is broad enough to be a subject of another LL. D research work.

[133] *Jamieson v Sabingo* supra 5; *Entores Ltd v Miles Far East Corporation* [1955] 2 QB 327(CA) 327 [1955] 2 All ER 493 (*Entores Ltd v Miles*); Eiselen *E-Commerce* 148; ITU 'Interception of Communications: Model Policy Guidelines and Legislative Text' (2012) 12.

[134] The definition of indirect communication in section 1 of RICA is 'the transfer of information…in whole or in part by means of a postal service or a telecommunication system.'

[135] The decision of the court in *Jamieson v Sabingo* supra 5 is based on the English case of *Entores Ltd v Miles* 327; Eiselen *E-Commerce* 148.

[136] It is one-way communication, for example, where a user sends a data from his or her email address to the same email address on the Internet or into 'mydropbox.com' for storage and safety purposes. However, traffic data message (for example, vehicular tracking and o-tag systems) is recorded and sent to an individual during the movement of a vehicle.

[137] Harper J 'It's modern trade: Web users get as much as they give' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 371 (Harper *It's modern trade: Web users get as much as they give*).

[138] Harper *It's modern trade: Web users get as much as they give* 371.

In online communication, there is a spontaneous feedback mechanism that indicates the status of communication. Feedback could be in form of a signal, for example, signalling of an engaged tone in a telephone communication when a call is made to another user, beeping of an o-tag in a vehicle monitored under traffic data system.[139] Feedback also comes where there is an instant voice response by the recipient if the recipient is available, otherwise, a voicemail recording system advises a caller to drop a message for the recipient if the latter is unavailable.

In addition, feedback could be in form of content message communications —such as a delivery report sent from a short message service 'SMS' in a phone or fax machine— or a silently or partially automated irresponsive communication.[140] In other channels of privacy communication, the feedback may not be spontaneous nor feedback available at all, such as a broadcast reception by listeners or viewers.

Online communication occurs in the following ways, namely: real-time or live and archived or stored communications;[141] content and non-content communication and Internet and non-Internet communication.

2.2.2.2 Inherent fiduciary relationship in the risk-based online communication

Because of the inherent high risks involved in online communication[142] between parties at a distance without knowing who is listening to the communication,[143] there is an inherent

[139] It is noted that *o-tag* system shows the picture of the passengers in a vehicle. For example, where an employee is expected to submit an *o-tag* bill to the human resource department for travel and subsistence claim, the submission is a breach of the right to privacy of the passengers whose pictures appear in the bill. This is because an *o-toll* bill could be compiled without necessarily displaying the pictures of the passengers, particularly where the number of passengers is not a criterion for the charging of a toll.

[140] A silent or partially automated irresponsive communication in an online communication device is one that is activated by the action or generation of information by the activity of an individual. For example, traffic data messages (in vehicular tracking and *o-tag* systems) are activated, recorded, and sent to an individual during the movement of a vehicle in the system. Section 1 of ECA.

[141] See the definition of real-time and archived communications and 'electronic communictaions' in section 1 of RICA; See section 1 of the ECTA for the defintion of data message which excludes voice in an automated form. However, automated voice communication can be classified under online communictaion such as a recorded voice message or report given by a vehicular tracking system or company; *Jamieson v Sabingo* supra 5; Eiselen *E-Commerce* 147- 152. A real-time communication can also be voiceless, for example, communications by body or sign language or other forms of communications which involve either audio-visual communication (such as Skype); Sections 1, 17(3), 18(3), 19(3), 30(1)(b), 35(1)(d) and (h),(2) and (3) and 36(4)(a)and (b) of RICA; See Eiselen *E-Commerce* 148 - 149.

[142] Eloff D 'Unscrambling the General Data Protection Regulation' http://www.derebus.org.za/unscrambling-the-general-data-protection-regulation/ (Date of use: 18 January 2019).

[143] Sloan I J *Law of privacy in a technological society* (1986) 56 (Sloan *Law of privacy in a technological society*).

fiduciary duty imposed in online communication, which arguably constitutes a 'specific confidential or utmost good faith relationship'. This relationship is between an expert,[144] agent or a service provider in the conscripted online communication, upon whom the duty to protect online communication lies and a user of an online communication device who relies on greater levels of privacy expectation in respect of the enormous and ubiquitous digital data transmitted in the 'online network vault'.[145]

In an online communication relationship, an online agent is legally and technically bound to securely transmit, and store an online communication[146] of users through the allocation of a

[144] See generally Alheit K *Issues of civil liability arising from the use of expert systems* (LL. D thesis Unisa 1997) 522, 526 and 527. (Alheit *Issues of civil liability arising from the use of expert systems*); Popoola O O *Statutory limitation of Internet service providers in decentralised peer-to-peer file sharing* (2012) (LL.M dissertation Unisa 2012) 6-20 ('Popoola *Liability of ISPs*').

[145] See paras 2.2 and 2.3 of this chapter. McQuoid-Mason *Privacy I*' 7; Van der Merwe D 'Criminal law' in Van der Merwe D, Roos A and Pistorius T (eds.) *Information communications and technology law* (2008) 62 - 63 and 67 - 70 (2008) (Van der Merwe *Criminal law*); Roos A 'Data protection' in Van der Merwe D et al *Information and communications technology law* (2008) 353 (Roos *Data protection*); Snail S and Papadopoulos S 'Privacy and data protection' in Van der Merwe D et al *Information communications and technology law* (2008) 277 - 278 (Snail and Papadoulos *Privacy and data protection*). It is noted that though this study is about the right to privacy, however both 'online network vault' and data in online communications which are capable of being protected, constitute intangible property recognized under s 25(4)(b) of the Constitution; Ebersohn G 'A common law perspective on computer-related crimes' 2004 *THRHR* 22 193 and 375; Rautenbach I M 'Introduction to the bill of rights' in LexisNexis *Bill of rights compendium* (2008) 1A66 (Rautenbach *Introduction to the bill of rights*); Van der Walt A J *The Constitutional property clause:* A Comparative analysis of section 25 of the South Africa Constitution of 1996 (1997) 63-65; Mostert H and Badenhorst P J 'Property and the Bill of Rights' in Butterworth's *Bill of Rights Compendium* (Issue 18) (2006) 3FB3; Roux T 'Property' in Woolman *et al* (eds.) *Constitutional Law of South Africa* (2003) 46.3(b)). Justice Binns-Ward J in *Absa Insurance and Financial Advisers (Pty) Ltd v Christaan Johannes Stephanus Moller & others* Case number: 20216/2014 at 3 (*Absa v Moller*); Ackerman J in *Bernstein v Bester NO* supra 67 and 77; Thorton L 'Telecommunication Law –An Overview' in Thorton L et al (eds) *Telecommunication law in South Africa* (2006) 25-26 (Thorton *Telecommunication law*).

[146] The following legislative provisions serve as direct and indirect guidelines on security issues that regulate or protect the operations of online communications in one way or the other: Sections 2(e) and 4(c) of General Intelligence Law Amendment Act ('GILAA') No. 11 of 2013 (*GILAA II*); Section 2 of National Strategic Intelligence Act ('NSIA') No 39 of 1994; Section 2 of National Strategic Intelligence Amendment Act ('NSIAA') No 37 of 1998; Section 2 of NSIAA No 67 of 2002; Sections 30(2)(a)(ii), 30(5)(a)(ii), 32(1)(b) and (c) and (2), 39, 40, 41, 44, 45, 46, 54 and 57 of RICA No 70 of 2002; Sections 2(h),(j),(m), (n) & (r), 29,30, 31, 36, 37, 38, 39, 40,41, 50-58, 73-78, 80-82 and 84 of ECTA No. 25 of 2002 and Sections 2(q), 8(2)(j), 35, 36 and 70 of ECA. Sections 6, 9, 14, 16, 17, 18, 22 and 29 of Electronic Communications Amendment Act ('ECAA') No. 1 of 2014; Sections 29-36, 37-41, 50-58 and 80-84 of ECTA; Standards Act (SA) No 29 of 1993; Cate F H *Privacy in perspective* (2001) 46; Blume P 'Data protection and privacy- Basic concepts in a changing world' in Wahlgren P (ed.) *Information and communication technology* –Scandinavian Studies in Law Vol. 56 at 153 (2010) 204-205 and 231-233 (Blume *Data protection and privacy*); Hiselius P 'ICT/Internet and the right to privacy' in Wahlgren P (ed.) *Information and communication technology- Legal issues Scandinavian studies in law* Vol. *56* 205 (2010) (Hiselius *ICT/Internet and the right to privacy*); Larsson C 'Telecom Operator's Incident Investigations' in Wahlgren P (ed.) *Information & Communication Technology – Legal Issues* – Scandinavian Studies in Law Vol. 56 (2010) 234 - 235 (Larsson *Telecom operator's incident investigations*); Cate *Privacy in Perspective* 23; Von Solms S H and Eloff J H P *Information Security* (2004) 7-130; Van der Merwe *Telecommunication law* 19-21; Standards Act No. 20 of 1993; Clough J *Principles of cybercrime* (2011) 135-136 (Clough *Principles of cybercrime*); Section 17(2)(e)(i) and (ii) of RICA.

'dedicated outband signal channel' in the network for each of the devices, technologies, networks, applications and services.[147] This relationship establishes 'an agreement of secrecy'[148] of communication between an agent and a user. The agreement arises from the need for an agent to guide against the breach of security in online communication, which has enormous and inherent levels of risks[149] than the other channels of private communication.

The agreement extends to the employees of the online agents, including clerks and stenographers who have knowledge of or come across a piece of information in the relationship.[150]

A breach of privacy of an offline communication —such as a telegram or sealed letter— is a *prima facie* invasion of privacy which constitutes a *strict* liability[151] imposed on infringers, including the press who controls and manages mass communication tools in the society.[152] It follows therefore that a *stricter* liability[153] is imposed for the breach of online communication which has cumulative and relatively higher levels of risks[154] than in the other *four channels* of privacy communication examined in this study.[155]

[147] An outband signal channel is 'a device that enables each piece of categorized data or work to pass through one channel of transportation' in the Open System Interconnection (OSI) model, while an inboard channel 'allows all kinds of information to pass through one channel of transportation in the OSI model', Veeraraghavan M and Wang H "A Comparison of In-Band and Out-of-Band Transport Options for Signalling" *Computer Communications and Networks 2007*, ICCCN 2007 1-7; ISO/IEC 7498-1:1994 "Information technology - Open systems interconnection - Basic reference model: The basic model" at 49; Popoola *Liability of ISPs* 7-8 and 18-19.

[148] SALRC 'Discussion Paper 109- Project 124 – Privacy and Data Protection' (2005) para 2.3.36 http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016) (SALRC http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016).

[149] Sloan *Law of privacy in a technological society* 56.

[150] Sloan *Law of privacy in a technological society* 79. Despite the fact that reference is made to professional secrecy in the offline world between a professional and a client, it is submitted that the underlying principle is that where there is an expectation of secrecy of information, adequate safeguards must be taken to guarantee its integrity and security, Sloan *Law of privacy in a technological society* 79.

[151] McQuoid-Mason D 'Privacy' in Woolmanet.al. *Constitutional Law of South Africa* (2013) 2nd ed. Revision Service 5 at 38-20 (McQuoid-Mason *Privacy II*); Section 51 of RICA; McQuoid-Mason *Privacy I*' 143 - 144; *Smith* supra 153.

[152] McQuoid-Mason *Privacy I* xxxix and 260; Paras 3.5.7.4 and 3.5.7.5 of Chapter 3 of this study.

[153] *Smith* supra 100 and 153.

[154] 'Schedule C of Directive for Internet Service Providers in terms of Section 30(7)(a) read with Section 30(2) of RICA and Regulations 5.1, 5.2, 6.1- 6.4(a) – (c), 7.12(a) & (b), 7.17 and 9.1(Schedule C of RICA).

[155] The five channels of privacy communication compared are:1) broadcasting; 2) human agency; 3) offline electronic communication devices; 4) postal services and 5) online communication devices.

2.3 SPECIAL FEATURES OF ONLINE COMMUNICATION

2.3.1 Non-compartmentalisation of and non-passworded compartmentalised online communication and criminal investigation

Despite the various precautions meant to secure the interoperable online communication devices, technologies, networks, applications and services, several technical inadequacies pose great challenges to the possible balance in the conflict between the protection of online communication and the conduct of an OCI.

The first challenge is the non-compartmentalisation or non-configuration of real-time and archived online communication devices,[156] technologies, networks, applications and services as opposed to the usual and relatively compartmentalised and secure offline privacy,[157] except in some circumstances in offline privacy, which may have some slight features of online privacy.[158]

In online communication, there is no button to be pressed by a LEA or LEO when conducting an OCI in a real-time telephone or voice communication of an individual to indicate the level of secrecy that an individual is communicating in the network, thus, there is no partial violation of privacy in a real-time online communication; its breach is absolute where an OCI is conducted. This inadequacy inevitably and consequentially reveals unlimited and irredeemable information about an individual when LEAs or LEOs conduct an OCI, particularly in contemporary interoperable online communications.[159]

---

[156] Online communication devices are landline telephone, two-way radio communication, facsimile machine, Internet, mobile cellular telephone and *o-tag* or *toll* devices or similar devices. It is noted that though an o-mail service is compartmentalised, it is not generally configured to have password for each of the compartments. In addition, password in Facebook is not in an encrypted format which exposes an individual to risks, see Roos 2012 129 *SALJ* 390 and 400-402; Grimmelman J 'Saving Facebook' (2009) 94 *Iowa LR* 1144 (Grimmelman (2009) 94 *Iowa LR* 1144); Basdeo 2012 2 *SACJ* 195-198; Chapter 7 of ECA; Sections 5(3)(e),(4)(c)(i)-(iv) and 6(a)-(d) of ECTA. Microsoft 'Set a password to help protect your Outlook information' https://support.office.com/en-us/article/Set-a-password-to-help-protect-your-Outlook-information-2589f1b1-c911-4b94-bceb-30ea098d6401 (Date of use: 12 June 2016).

[157] An offline privacy is usually and adequately compartmentalised and protected by a firewall, security lock or measure at every point of compartmentalization. For example, in an open plan house structure, a house is usually compartmentalised by dividing it into rooms, wardrobes and safes or vaults.

[158] For example, some offices and boarding schools have open plans, which may not have several compartments or gateways to the individuals in that environment. However, it is noted that despite this openness, individuals may still be allowed to use personal lockers or vaults, which, to a large extent, still bear the features of offline privacy compartmentalisation.

[159] Paras 2.3.1 - 2.3.3 of this chapter.

It is therefore submitted that the levels of risks in the protection of the structure and scope of compartmentalisation of online privacy are greater in online communication devices, technologies, networks, applications and services than in non-online communications, yet the latter is usually, relatively and adequately compartmentalised. For example, in an open plan house structure, it is usually compartmentalised by dividing it into rooms, wardrobes and safes or vaults, which to some extent demonstrate some level of privacy.

However, given the need to protect national and international security, health, safety, essential and emergency services and economic interests, and purposes; Cybercrime and Cybersecurity Bill ('CCB'), which is replaced by the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, provided for the declaration of critical information infrastructure and classification,[160] archiving, storing and protection of data in the declared critical information infrastructure held by government and non-government entities only.

This was done without making provision for private online communication compartmentalisation in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 or in any law.[161] The declaration of critical public information infrastructure demonstrated one of the ways of implementing the compartmentalisation principle in public infrastructure online communication because the use and meaning of the word 'classification' is arguably synonymous with compartmentalisation principle propounded in this study.[162]

Consequently, the Cybercrime Bill 2018-Amendments Proposed to Bill -B6 2017 has expunged the entire provision examined above, thus, critical public information is not specially protected in the Cybercrime Bill 2018- Amendments Proposed to Bill B6-2017.

---

[160] Classification of data means 'to assign a level of sensitivity, value and criticality to the data for purposes of security controls for the protection of the data', in section 57(12)(a) of CCB- B6-2017(CCB 2017). In a way, this means the configuration of data in online communication for government information infrastructure. However, section 57(12)(a) of the CCB B-2017 is expunged from the Cybercrime Bill 2018– Amendments Proposed to Bill – B6 2017 published on the 23 of October 2018.

[161] See Chapter 11 of CCB 2017, more particularly sections 57(2), (3), (4)(a), (5), (6) and (12)(a), which is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017. The omission in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 and other law on private data compartmentalisation is an implied consequential retention of the inherent**,** unimaginable and immeasurable risks in an online communication in which private individuals are exposed to in the non-compartmentalised online communication devices, technologies, networks, applications and services in the twenty-first century quick-silver technology era.

[162] Section 57(12)(a) of CCB 2017 is expunged from the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

The second technical challenge faced in the possible balance in the conflict between the protection of the right to the SOC and the conduct of an OCI bothers on the non-passworded and unprotected *internal units* of online communication with a PIN, firewall, security lock or measure. Therefore, one of the effects of this inadequacy is the revelation of unlimited and irredeemable information about an individual once there is an initial intrusion or logging into an individual online account by LEAs or LEOs.

Even where the American 'closed container' doctrine regards online communication as a sealed container, which is accessed by the execution of a search warrant,[163] its non-passworded compartmentalisation nature and feature exposes it to greater risks than in non-online communications because of the higher volume of data in online communication than the non-online communications. For example, although an e-mail communication is demarcated into an inbox, outbox, compose, sent, draft, etcetera, these demarcations are generally not individually passworded, thus absolute, unfettered and intrusive access into these devices, technologies, networks, applications and services can be obtained or secure.[164]

However, in some few occasions in archived communications involving commercial Internet services, an individual pays a fee for an e-mail communication which is configured and secure in compartments which require a PIN before accessing each of the compartments such as inbox, outbox, draft etc. However, aside from the fact that this fee is not within the reach of an average online communication user in the RSA, the United Nations has also declared the use of online communication as a fundamental right in the 21st century,[165] therefore, the declaration of this

---

[163] Rosen J 'The Supreme Court's Cell Phone Case Went Even Further than Privacy Advocates Had Hoped' http://www.newrepublic.com/article/118396/supreme-court-cellphone-case-went-further-privacy-advocates-hoped (Date of use: 30 June 2017) (Rosen http://www.newrepublic.com/article/118396/supreme-court-cellphone-case-went-further-privacy-advocates-hoped (Date of use: 30 June 2017); Van der Berg J 'Mobile Phone Evidence: Implications for Privacy in South African Law' http://ohrh.law.ox.ac.uk/mobile-phone-evidence-implications-for-privacy-in-south-african-law/ (Date of use: 25 June 2017 (Van der Berg http://ohrh.law.ox.ac.uk/mobile-phone-evidence-implications-for-privacy-in-south-african-law/ (Date of use: 25 June 2017). In *People v Diaz* Cal Rptr. 3d 105, 2011, the Supreme Court of California affirmed the judgement of the Court of Appeals denying the motion to suppress evidence obtained without warrant from the cell phone of Diaz upon lawful custodial arrest. However, in the latest case of *Riley v California* 573 U.S 2014, the Supreme Court unanimously held that 'police generally may not, without a warrant, search a digital information on a cell phone seized from an individual who has been arrested.

[164] Infringement could be '*trivial*, *technical*, *inadvertent*, *gross violent*, *deliberate* and *cruel'*, Van der Merwe *Unconstitutionally obtained evidence* 273; *R v Grant* (2009) 2 SCR 353 74; *State v Mark* 2001 1 *SACR* 572 578a and 588e; *R v Collins* 1987 28 *CRR* 122 (SCC) per Lamer J para 138 (*R v Collins*). In this study, there is a gross breach of the right to privacy in content data.

[165] Olivarez-Giles N 'United Nations report: Internet access is a human right' https://latimesblogs.latimes.com/technology/2011/06/united-nations-report-internet-access-is-a-human-right.html (Date of use: 25 December 2018).

right cannot be enforced or fully enforced if a fee is attached to its enjoyment in terms of the right to the passwording of the compartments of online communication.

Consequently, given the existence of the above features in online communication, the same nature and features apply when an interception occurs, therefore, the same risks apply in the conduct of an OCI.

Although the South Africa legislature does not recognise the need to configure e-communications,[166] legislation should be enacted to regulate the configuration of the compartmentalisation and passwording of online communication devices, technologies, networks, applications and services used by private individuals into several reasonable continua of secrecy interests.[167] A legislation in this regard will prevent liability against LEAs where certain information is unnecessarily revealed during the conduct of an OCI.

2.3.2 Convergence or interoperability of online communication devices, technologies, networks, applications and services

Online communication can be carried out on independent, and interoperable (or colloquially called 'converging')[168] platforms. Interoperability means that while online communication devices, technologies, devices, networks and applications can maintain their independence in online communication, they are also now able to simultaneously or dependently operate or converge with each other for better outputs or services.

In other words, hitherto, the six online communication devices had limited functional capacities in online communications because they operated independently. However, due to the exponential advancement of technologies, networks, applications and services, these devices are now able to engage in various interactive, cooperative and interchangeable operations and functions, which create certain technical and operational complexities.[169] According to Clough, some of these complexities include the transmission of data over a variety of networks in many

[166] Section 57(12)(a) of CCB-B6-2017, which is expunged in the from the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[167] Paras 3.7 and 3.8 of Chapter 3 of this study where the continuum of privacy interests is examined.
[168] Thornton *Telecommunications law* 25-26; Sections 8(2)(e), 36(2)(b) of the ECA; Section 8(3)(g) of the ECTA.
[169] See Chapter 7 of the ECA; See also sections 5(3)(e), (4)(c)(i) - (iv) and 6(a)-(d) of the ECTA.

countries via different media platforms before reaching their destination, making it difficult to establish where interception takes place.[170]

In the interoperable relation between Internet and non-Internet based systems, it is submitted that despite the dichotomy in the two systems, the indispensable or inevitable, complex and complicated principle of interoperability (or 'convergence') of technologies, networks, applications, services and devices enables online communication systems to interchangeably, effectively and beneficially operate, converge or engage in online communication. However, given the fusion of operation in online communications, stakeholders involved in the conduct of an OCI are faced with the difficulty of identifying which technologies, networks, applications, services and devices are applicable or in operation when conducting an OCI.

Consequently, the difficulty raises the question on the determination of different thresholds that will be required for OCI compliance since each of the technologies, networks, applications, services and devices require different reasonable ground standards before an OCI is conducted through them.[171]

2.3.3 The concept of online conscription

2.3.3.1 Introduction

In procuring evidence in the offline world —through human agency, for example—[172] conscriptive evidence is obtained by LEAs when an individual is generally compelled to assist or participate in the construction, creation or discovery of evidence.[173] Conscription is also a situation where someone is forced to supply evidence against his or her wish[174] via a statement, body or hair samples, teeth impressions or through other forms of real evidence.[175]

---

[170] Clough *Principles of cybercrime* 135-136.

[171] For the examination of the standards of proof required to embark on the conduct of an OCI, see generally Chapter 6 (para 6.4) of this study.

[172] Paras 3.5.7.1 – 3.5.7.15 of Chapter 3 of this study.

[173] *State v Pillay and others* 2004 (2) SACR 419(SCA) 445 B-J, 446J-447B (*State v Pillay*); Van der Merwe *Unconstitutionally obtained evidence* 250**.**

[174] *State v Pillay* supra 431, G-432A, 445 B-J, 446J-447B; Van der Merwe *Unconstitutionally obtained evidence* 250**.**

[175] *State v Pillay* supra 447C-D; *Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others* 2008 (2) SACR 421 (CC) (*Thint*) 142 And 155; Hubbard, Brauti and Fenton *Wiretapping* at 10-26.10., 10-26.11 and 10-27 to 10-39; Van der Merwe *Unconstitutionally obtained evidence* 202-203 and 210.

Although the supply or production of evidence is known to the target, however, the supply of such evidence is not consented to by the supplier of such evidence, which contravenes the protection of the right against self-incrimination,[176] and other rights, which, arguably, include privacy. In terms of the confession and other statements made by an individual, the offline conscription principle generally regards unconstitutionally obtained evidence as inadmissible.[177]

Given the various forms of erroneous automatic or default technical recording and processing of information[178] that take place in the operation of every online communication device,[179] which is regarded as primary conscription, it is argued that automatic online conscription occurs as soon as a user activates an online communication device. Put differently, online conscription occurs whether or not a user activates a special application on the device, which results in online conscription.

In some instances, a device does not have to be switched on before an online conscription occurs. The automatic occurrence of online conscription lays the foundation (amongst other perspectives)[180] for the proposition in Chapter Three of this study that an online communication attracts greater risks than non-online communications, therefore, the former should be accorded the right to the SOC as opposed to the general right to privacy that is assigned to non-online communication.[181]

However, there is the absence of legal pronouncement by the Constitutional Court on the occurrence or existence of online conscription, while there are express, and implied erroneous and contradictory decisions by the Supreme Court of Appeal and High Court on the applicability of offline conscription to online communication, leading to the outright denial of the recognition of the legal existence of online conscription.[182] The courts, in their

[176] *Nel v Le Roux No & Others* Case No: CCT 30/95 para 3 (*Nel v Le Roux*); *State v Pillay* supra 430B-F, 431G-432A, 445B-J and 446 A-447B-J; *State v Naidoo* supra 483 G-H (N); Section 84(9) of POPIA.
[177] Section 35(5) of the Constitution; Van der Merwe *Unconstitutionally obtained evidence* 198-201 and 257.
[178] See the definition of 'processing' in sections 1 and 20 of the POPIA.
[179] Section 30 of RICA; *State v Pillay* supra 420 H - I, 421 D - I, 427 I - 428 D, 430 E - F, 433 I - 434 F, 447 C - E and 448 D.
[180] The special features of online communication in para 2.3 of this chapter as justification for the right to the secrecy of online communication in Chapter Three, more particularly para 3.5 of this study.
[181] See Chapter 3 of this study, more particularly para 3.5.
[182] *State v Pillay* supra 421 A-B, 432 A - H, 445 - 446 C - I and 447 D-F; *State v Naidoo* supra 483 F-I; Van der Merwe *Unconstitutionally obtained evidence* 250.

consideration of the applicability of the concept of offline conscription to online conscription, have omitted to consider the undeniable unique and universal nature and features of online communication as the basis for their erroneous decision.

One of the unintended consequences of the outright denial of the existence of conscription in online communication by the courts is that it makes it difficult for the objective consideration of the application of section 35(5) of the Constitution in appropriate cases of admissibility of online conscription and its exception.

However, this study argues otherwise because of the overwhelming proof that online conscription occurs or exists because its occurrence or existence is technically and legally inevitable in online communication.

2.3.3.2 Applicability of the concept of offline conscription to online conscription

As a corollary to the foregoing introduction on offline conscription, it is very 'easy to extract sensitive personal data from',[183] 'monitor ideas and then track them back to people'[184] in online communication. In every online communication where there is an act of commission or omission, there is a digital footprint or vacuum that is left behind which reveals and tracks every activity and detail about the preferences and behaviour of a user,[185] the record of which lasts for years to come.[186] This is made possible by several software applications,[187] one of which is cookies and tracking application, which helps in finding frequently visited websites

[183] Carr *Tracking is an assault on liberty* 366.
[184] Carr *Tracking is an assault on liberty* 367.
[185] Swire P P and Ahmad K (eds.) 'Part 6: Online Privacy' in Swire P P and Ahmad K *Privacy and surveillance with new technologies* (2012) 329-330 (Swire and Ahmad (eds.) *Part 6: Online Privacy*); Harper *It's modern trade: Web users get as much as they give* 372.
[186] Vlahos J 'Surveillance society: New high-tech cameras are watching you' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 107 (Vlahos *Surveillance society: New high-tech cameras are watching you*).
[187] Pop-ups and direct advertisements are other forms of conscription used on the Internet, Swire P P and Ahmad K (eds.) 'Introduction' in Swire P P and Ahmad K *Privacy and surveillance with new technologies* 1 (Swire and Ahmad (eds.) *Introduction*).

by users by 'linking one online session to another'[188] for commercial and other purposes including selling of products and services.[189]

Cookies application enables the harvesting of invaluable and unbelievable detailed data from online databases without the awareness or consent of the user.[190] Essentially, everyone is a suspect in online communication[191] even if you are an anonymous user in online communication.[192] The sensitivity of a software application used in online conscription is such that the most insignificant information or opinion left online by an individual in different sites or places is picked up by the various applications that allow conscription[193] or such information is picked up by an online agent who regularly reports the activities of a user to the corporate or human agent.[194] In some of these instances above, the person carrying out the surveillance might be the government itself.[195]

The installation of the application of cookies raises the question, whether the warrantless interception of yesteryears has become the online conscription of today because warrantless interception is indiscriminately still continuing, given that surveillance technologies or software applications 'rarely go unused or un-abused once they are available'?[196] This is because the conscription of online communication, including the mobile cellular telephone, is a routine activity[197] which is technically 'made wiretap-ready with built-in ''backdoor'' surveillance capability'[198] and legally required that Online Communication Service Providers[199] —including social media— must ensure that online communication equipment is

[188] Swire and Ahmad (eds.) *Part 6: Online Privacy* 329-330; Harper *It's modern trade: Web users get as much as they give* 372.
[189] Swire and Ahmad (eds.) *Introduction* 1.
[190] Thompson *GPS monitoring* 285; Carr *Tracking is an assault on liberty* 365.
[191] Swire and Ahmad (eds.) *Introduction* 11.
[192] Carr *Tracking is an assault on liberty* 366 and 367.
[193] Carr *Tracking is an assault on liberty* 367.
[194] Vlahos *Surveillance society: New high-tech cameras are watching you* 105.
[195] Swire and Ahmad (eds.) *Introduction* 1.
[196] Wood G 'Prison without walls' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 310 (Wood *Prison without walls*).
[197] Crump *Geolocational Privacy and Surveillance Act* 283 and 285.
[198] Swire and Ahmad (eds.) *Part 4: Backdoor surveillance* 192.
[199] This study adopts the term 'online communication' or 'Online Communication Service Provider' to specifically deal with the unique nature, features and issues in this study as opposed to 'offline electronic communication', both of which are categorised under '*electronic communication*'. Electronic communication is a broad and general word or term used in the society, which also includes broadcasting communication and other related types of electronic communications, which do not fall into this study. In *Offline electronic communication* (for example, a computer which does not have online connectivity, but which has a memory stick which can be

intercept friendly and ready.[200] Analogically, the fact that 'smoking is a surreptitious threat to health' is the same way that cookies application is a surreptitious threat to privacy.[201]

Another remarkable digital footprint in online communication is where a predictive text software application is installed in online communication which enables texts to be predicted before a user concludes the writing of the word or sentence in an o-mail composition or SMS on a mobile cellular telephone.[202] The prediction is made possible by the initial messages that a user had typed or sent which are kept in the memory of the software application to lead or direct a user in the next online communication or purported online communication, which is now generally described as one of the activities involved in ML application.[203]

In summary, the foregoing descriptions generally explain online conscription concept, which occurs in any contemporary society, including the RSA and any other country in which an online communication operates. For instance, in the United States, a former chief of NIA said that users of an online communication do not have the right not to be tracked as consumers,[204] which unequivocally and effectively means that online conscription is undeniable and a necessary evil in online communication in the contemporary society.

2.3.3.3 Origins of the concept of online conscription

In the late 18th century, Jeremy Bentham- an English Philosopher- predicted that we will be living in a world of online 'panopticon' or a 'sentiment of an invisible omniscience'.[205] This

used for communication via copying of data into or from a memory stick is not the same with a computer that is connected to an online network.

[200] Section 30 of RICA; McCullagh D 'FBI: we need wiretap-ready websites- Now' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 194 (McCullagh *FBI: we need wiretap-ready websites- Now*).

[201] Harper *It's modern trade: Web users get as much as they give* 373.

[202] Madrigal A 'I'm being followed: How Google-and 104 other companies- Are tracking me on the web' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association: U.S., 2012) 347 (Madrigal *I'm being followed: How Google-and 104 other companies- Are tracking me on the web*).

[203] Waldron S, Wood C and Kemp N 'Use of predictive text in text messaging over the course of a year and its relationship with spelling, orthographic processing and grammar: Predictive Text and Literacy Skills' https://www.researchgate.net/publication/302917761_Use_of_predictive_text_in_text_messaging_over_the_course_of_a_year_and_its_relationship_with_spelling_orthographic_processing_and_grammar_Predictive_Text_and_Literacy_Skillshttps://www.researchgate.net/publication/302917761_Use_of_predictive_text_in_text_messaging_over_the_course_of_a_year_and_its_relationship_with_spelling_orthographic_processing_and_grammar_Predictive_Text_and_Literacy_Skills (Date of use: 21 February 2020).

[204] Madrigal *I'm being followed: How Google-and 104 other companies- Are tracking me on the web* 347.

[205] Vlahos *Surveillance society: New high-tech cameras are watching you* 101.

prediction describes a situation where a prison warder (Online Communication Service Provider) watches the inmates (users of online communication) in prison (online communication) without the inmates having knowledge that they are being watched.[206] Essentially and undoubtedly, online communication is a prison where all users of online communication are captured and sentenced to life imprisonment, without any option to opt out.

The origins of the concept of online conscription can be traced to two key specific perspectives —amongst others— which are the economic and technical perspectives.

First of all, one of the origins of the concept of online conscription, which commenced in the twenty-first century[207] is in the business or economic world, which is traceable to the monitoring of the business of the U.S. Department of Agriculture by the Soviets and in other instances in the general business world.[208] Till date, the greater part of surveillance is still conducted by the private sector, ranging from the activities of the banks to advertising companies,[209] such that the worst dictator in history has never imagined happening in our lifetime.[210]

Given this origin, LEAs now borrow a leaf from the private sector by engaging in the use of massive and powerful 'dragnet surveillance' programs which involve the drawing of links and making of predictions from the enormous quantity of data collected from private data[211] for planning purposes, protecting public health and preventing crime such as terrorism and many more.[212]

In addition, one of the origins of online conscription is the technical aspect of cookies application, which has been described above.[213] Cookies application has been an integral part of web browsing from the inception of the Internet, which has dominated discussion all these years.[214]

---

[206] Vlahos *Surveillance society: New high-tech cameras are watching you* 101.
[207] Swire and Ahmad (eds.) *Introduction* 14.
[208] Landau *Lawful electronic surveillance in the face of new technologies* 226 - 227; Crump *Geolocational Privacy and Surveillance Act* 282.
[209] Data mining by banks is used in detecting and stopping credit card fraud while data of consumers is sold to companies to improve sales and profit, Swire and Ahmad *Introduction* 14-15.
[210] The Economist *Learning to live with big brother* 23; Carr *Tracking is an assault on liberty* 366.
[211] Swire and Ahmad *Introduction* 14.
[212] The Economist *Learning to live with big brother* 23.
[213] See para 2.3.3.2 of this chapter.
[214] Harper *It's modern trade: Web users get as much as they give* 373.

Aside from the use of cookies, a mobile cellular telephone is technically and inevitably a tracking device which locates a user in the wireless network to enable a Telecommunication Service Provider know which specific cell a user is located to send the signal to the cell for online communication to occur.[215] Without specifically placing a user of a mobile cellular telephone on the radar, conscription already occurs by the mere usage of a mobile cellular telephone by an individual.[216]

In other words, for an individual to prevent being conscripted in online communication —in terms of revealing the movement or contact list or their identity— total abstinence from the use of a mobile cellular telephone is, perhaps, the only way out.[217] However, abstinence seems difficult to accomplish or practice in contemporary society where a cellular telephone has become part of human anatomy,[218] for example, an offer of employment can now be made via an e-mail and acceptance via an SMS,[219] which establishes the indispensability of online communication. Alternatively, such an individual must be prepared to use a satellite telecommunication device,[220] which is not connected to the network of Telecommunications Service Providers and not legally allowed for general public use in the RSA unless approved under a special licence.[221]

2.3.3.4 Overview of the status quo of the concept of online conscription

Conscription can be described as a scenario where a person accesses a place with a microchip[222] or conducts online surfing at home or elsewhere and realises that someone is watching from afar.[223] A person leaves behind, and the system highlights a data trail of every keystroke, word,

---

[215] Swire and Ahmad (eds.) *Part 5: Locational tracking* 245; Swire P and Ahmad K ‘‘‘Going dark’’ versus a ‘‘Golden age for surveillance’’’ in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 238 (Swire and Ahmad *Going dark v Golden age for surveillance*).

[216] Swire and Ahmad *Going dark v Golden age for surveillance* 238.

[217] Swire and Ahmad *Going dark v Golden age for surveillance* 240.

[218] *Riley v California* and *U.S v Wurie* 9, 16-17 and 28 of the Opinion and p 6 of the minority decision by Alito J; Swire and Ahmad (eds.) *Part 5: Locational tracking* 245; Thompson *GPS monitoring* 250. In the U.S., cellphone users are more than the population of the U.S., Crump *Geolocational Privacy and Surveillance Act* 274.

[219] *Jafta v Ezemvelo KZN Wildlife* (2008) 10 BLLR 954 (LC) or (2009) 30 ILJ 131 (LC) (*Jafta v Ezemvelo*).

[220] Brennan T J and Macaulay M K ‘Remote Sensing Satellites and Privacy: a framework for policy assessment’ 1995 Vol. 4 No 3 *Law, Computer & Artificial Intelligence* at 233-249.

[221] Section 32 of ECA No 35 of 2005.

[222] The Economist *Learning to live with big brother* 25 and 33.

[223] Swire and Ahmad (eds.) *Introduction* 1; The Economist *Learning to live with big brother* 25 and 33; Madrigal *I’m being followed: How Google-and 104 other companies- Are tracking me on the web* 340-341, 345–346 and 353.

statement or move made, through a strong binocular[224] on a computer where the Internet Protocol address or another form of logging-in key is traceable to your identity.[225]

Every move made by a user of online communication is an invaluable tiny quantity of information, which does not go 'unmonetised' or unutilised by someone who is most likely to be a marketer[226] or advertising companies[227] and lately politicians for electioneering benefit or campaign,[228] amongst others. Thus, users of online communication are like pawns in the hands of service providers who forever competitively and strategically take advantage of users of online communication in the exchange of their data for financial gain[229] and for other invaluable benefits by other beneficiaries.

The abovementioned scenario is not fiction because the 'person' —online agent— that is permanently armed with the binocular lives inside your online communication.[230] The 'man' stores billions of data relating to your online habits or patterns in his archives in every transaction that you make —which lasts forever.[231] The information gathered becomes very powerful in the hands of marketers who use and analyse the information in a dossier to determine the possible future behaviour of an online communication user.[232]

The invaluability of this data includes but not limited to storing, identifying and analysing of individual grocery items, reading preferences, queries,[233] travel history, last o-mail login,

[224] Swire and Ahmad (eds.) *Introduction* 1. The Economist *Learning to live with big brother* 25 and 33; Madrigal *I'm being followed: How Google-and 104 other companies- Are tracking me on the web* 340-341, 345–346 and 353.
[225] Vlahos *Surveillance society: New high-tech cameras are watching you* 99–100; Carr *Tracking is an assault on liberty* 366.
[226] Madrigal *I'm being followed: How Google-and 104 other companies- Are tracking me on the web* 340-341, 345–346 and 353.
[227] Angwin J 'How much should people worry about the loss of online privacy?' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012)336 (Angwin *Loss of online privacy*); Madrigal *I'm being followed: How Google-and 104 other companies- Are tracking me on the web* 340-344.
[228] See the alleged 2016 U.S. election interference by Russia, CNN '2016 Presidential Campaign Hacking Fast Facts' https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html (Date of use: 12 December 2018).
[229] Madrigal *I'm being followed: How Google-and 104 other companies- Are tracking me on the web* 343.
[230] Swire and Ahmad (eds.) *Introduction* 1; Carr *Tracking is an assault on liberty* 368.
[231] Vlahos *Surveillance society: New high-tech cameras are watching you* 107.
[232] Carr *Tracking is an assault on liberty* 239; The Economist *Learning to live with big brother* 25 and 33; Angwin *Loss of online privacy* 336; Madrigal *I'm being followed: How Google-and 104 other companies- Are tracking me on the web* 340-344.
[233] Vlahos *Surveillance society: New high-tech cameras are watching you* 99–100; Carr *Tracking is an assault on liberty* 369; The Economist *Learning to live with big brother* 25 and 33.

wife's name or choice of shoes,[234] religious practices, job records, medical records, loyalty cards,[235] obesity and anxiety status,[236] political philosophy or associates, faithfulness with lover or partner.[237] Sometimes, racial profiling is conducted, which is not only wrong but it is ineffective.[238] All of this is stored until a time when no data can be stored for free, though the discounted sale of space is now being offered for Internet usage.[239]

Although the billions of data gathered in online communication are personal or extremely personal information, however, it becomes difficult to determine when it is used to manipulate a user of online communication where the information is put into different uses or purposes.[240] Different uses will include where a marketer uses the knowledge of the gathered information for customised advert campaign targeting a user of online communication.[241]

Another purpose of conscription, which is meant to manipulate users, is found in an insurance contract where the insurer relies on the records of the online movement of an insured in the previous year to raise the prospective premium or deny insurance coverage.[242] In these instances, it is difficult or impossible for users to determine whether there is a breach of his or her right and if users know how much information companies know about him or her.[243]

However, considering the other side of the coin from the economic or commercial perspective, Google, which is one of the key players in online conscription, invests millions of dollars on free services such as Google mapping tools, Google search engine, Gmail and many more.[244]

---

[234] Vlahos *Surveillance society: New high-tech cameras are watching you* 104; Madrigal *I'm being followed: How Google-and 104 other companies- Are tracking me on the web* 342.
[235] The Economist *Learning to live with big brother* 26 and 31-32.
[236] Carr *Tracking is an assault on liberty* 369.
[237] Angwin *Loss of online privacy* 336; Madrigal *I'm being followed: How Google-and 104 other companies- Are tracking me on the web* 340-344; *States v Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010); Crump *Geolocational Privacy and Surveillance Act* 279.
[238] Khera F Y 'Laptop searches and other violations of privacy faced by Americans returning from overseas travel' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 171 (Khera *Laptop searches and overseas travel*)
[239] Vlahos *Surveillance society: New high-tech cameras are watching you* 100.
[240] Vlahos *Surveillance society: New high-tech cameras are watching you* 107.
[241] Carr *Tracking is an assault on liberty* 369.
[242] Blumberg A J and Eckersley P 'On locational privacy, and how to avoid losing it forever' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 327 (Blumberg and Eckersley *Locational privacy*).
[243] Carr *Tracking is an assault on liberty* 369.
[244] Francis J 'Facebook's convergence conundrum- Merging Facebook Messenger, WhatsApp and Instagram is a risky gamble and there isn't a good enough reason to do so.' https://www.itweb.co.za/content/mYZRXv9Ppd8qOgA8 (Date of use: 12 February 2019).

Google provides these free services from which commercial online conscription occurs because it avails itself the opportunity of trading —in the online communication collated from individuals for advertising or marketing purposes with third parties.[245] Supporters of the free flow of information in online communication argue that innocent people have nothing to fear where their information is collated or collected and that collection does not constitute use.[246]

However, privacy advocates counter the ''I've got nothing to hide' argument[247] by positing that data mining has fundamentally changed the nature of surveillance[248] where everyone that uses an online communication is in a prison of 'total surveillance', which records every move of the mouse.[249] Where such communication is personal information, unauthorised persons are prohibited from disclosing such information save where there is knowledge of disclosure by the data subject or by law because such personal information is regarded as a secret.[250]

It does seem that commercial online conscription will persist, given the high-level government participation in online conscription resulting in the building of mass databases.[251] The compellability of the business and economic uses of online communication in government to government (G2G), government to business (G2B) and government to citizens (G2C) and vice versa at domestic and international levels[252] and social uses of online communication devices in modern society[253] —including court proceedings— is unequivocally recognised by the government of the RSA.[254]

The compellable use of online communication in the above instances resulting in the building

[245] Harper *It's modern trade: Web users get as much as they give* 373.
[246] Swire and Ahmad (eds.) *Introduction* 14.
[247] Blumberg and Eckersley *Locational privacy* 327.
[248] Swire and Ahmad (eds.) *Introduction* 14.
[249] Vlahos *Surveillance society: New high-tech cameras are watching you* 100-101.
[250] Section 20 of POPIA.
[251] The Economist *Online privacy* 359-360.
[252] Moyo A 'Only 3.5% of SA's households don't have phones' https://www.itweb.co.za/content/JOlx4z7kVpv56kmW (Date of use: 26 June 2017); Bawa *ROICA* 331; Affidavit in support of the Notice of Motion in *AmaBhungane v Minister of Justice* supra 125-136, more particularly paras 126 and 133; Regulations 5.1 & 5.2 of Schedule C of Directive for Internet Service Providers in terms of Section 30(7)(a) read with section 30(2) of the RICA No. 28271 Government Gazette, Notice 1325 of 28 November 2005 (Schedule C of RICA); SALRC paras 4.2.38 – 4.2.39 http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016).
[253] Chapter 7 of ECA and ss 5(2), (3)(1)(e), (4) (c) (i) -(iv) and 6(a)-(d) of ECTA.
[254] De Jager J 'Electronic evidence' in Schwikkard P J et al *Principles of evidence* (2017) 437(De Jager *Electronic evidence*); *State v Miller* supra 70.

of mass databases[255] by the government of the RSA confirms the existence of online conscription. In the U.S., the government is reluctant to impose regulation on the private sector collection or collation of online communication because it is beneficial to the government,[256] thus encourages online conscription.

In support of the role of the government in recognising the existence of online communication conscription, government, in a bid to control crime, turns its focus on the compiled mass dossier of digital data and behaviour of people —including innocent people.[257] Therefore, it is disheartening for individuals to note that their personal online communication is the 'fuel for the World Wide Web', from where the government gathers information of individuals in the society. This analogy confirms the rule that the less individuals supply their personal information online, the more bankrupt is the Internet resource.[258] The web relies on the further rule that says 'garbage in, garbage out' which means that if individuals do not send out information to the web, there is no information to be collated or collected by the web for dispatch to surfers.[259]

As much as the promise by advertisers that the available data of users will not be used for advertising purposes, it is the right of a user to be informed of the use of data,[260] and stop or protest against data collection[261] or processing[262] for unethical, unlawful or illegal purposes such as the use of data for election manipulation or other forms of manipulation, anti-competitive or trust issues, amongst others.[263]

Essentially, online conscription has eroded the rights of an individual, for example, the rights

[255] The Economist *Online privacy* 359-360.
[256] The Economist *Online privacy* 359-360.
[257] Swire and Ahmad *Introduction* 14.
[258] Harper *It's modern trade: Web users get as much as they give* 373.
[259] Harper *It's modern trade: Web users get as much as they give* 371.
[260] Section 18 of POPIA; See 'right to be informed' in Eloff D 'Unscrambling the General Data Protection Regulation' http://www.derebus.org.za/unscrambling-the-general-data-protection-regulation/ (Date of use: 18 January 2019).
[261] Madrigal *I'm being followed: How Google-and 104 other companies- Are tracking me on the web* 347; Section 14(1)(c) of POPIA.
[262] Sections 11 (3) & (4) and 14(6) of POPIA; See 'right to restrict data processing' in Eloff D 'Unscrambling the General Data Protection Regulation' http://www.derebus.org.za/unscrambling-the-general-data-protection-regulation/ (Date of use: 18 January 2019).
[263] See the alleged 2016 U.S. election interference by Russia, CNN '2016 Presidential Campaign Hacking Fast Facts' https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html (Date of use: 12 December 2018).

'to be forgotten after the use of data', 'not to be tracked' or not to be subjected to geographical surveillance in the POPIA,[264] even where there is no such law or consent to retain such information. In fact, no law requires that online communication should be conscripted. What the law requires is that Online Communication Service Provider must install interception devices in their communication devices.[265]

In the final analysis, one of the ways that online conscription may not occur in the RSA is to comply with the provision of section 51(9) of the ECTA,[266] which provides as follows:

> A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.[267]

Section 68 of the POPIA also prohibits the use of personal information for direct marketing purposes because the provision requires the user of personal information to comply with the code set out by the Regulator for such uses of information, which in this case, is for marketing purposes.[268]

However, it is important to note the difficulty involved in fully complying with the provisions of the POPIA and ECTA in terms of the occurrence of the concept of online conscription,[269] because privacy breaches arising from marketing of online data occur behind the scene, which may not be detected immediately, thus prevents or delays the enforcement of the right of an individual in the POPIA and ECTA.

---

[264] Section 14(3) - (8) of POPIA; Heyink M 'Elizabeth de Stadler and Paul Esselaar 'A guide to the Protection of Personal Information Act' http://www.derebus.org.za/guide-protection-personal-information-act/ http://www.derebus.org.za/guide-protection-personal-information-act/ (Date of use: 11 June 2018).

[265] Section 30 (1)(a), (2)(a)(i) and (3)(a)(i) of RICA.

[266] The ECTA.

[267] Section 51 (9) of the ECTA.

[268] See 'right to object' in Eloff D 'Unscrambling the General Data Protection Regulation' http://www.derebus.org.za/unscrambling-the-general-data-protection-regulation/ (Date of use: 18 January 2019).

[269] Sections 2 and 5 and Chapter 3 of the POPIA and Chapter VIII of the ECTA, more particularly section 51(3) and (6) of the ECTA.

2.3.3.5 Jurisprudence of the concept of online conscription in South Africa

In online communication, conscription of evidence does not involve real evidence but involves a confessed or admitted statement[270] or inevitable impression made in both real-time and archived communication of content and non-content data.

Drawing on the offline concept of conscription of evidence,[271] an individual in online communication is generally compelled, forced to supply or assist or participate in the construction, creation or discovery of online evidence against his or her wish immediately he or she legally or equitably activates any form of online communication.

In RICA and its directive, provisions are prescribed for the compulsory installation of an online communication device with interception capability and for the compulsory or automatic duplication, recording and storage of both real-time and archived communication respectively,[272] thus resulting in online conscription as broadly described in section 71 of the POPIA.[273]

It is important to note that section 71(3) of the POPIA allows a user of online communication to make a representation before a responsible party is allowed to make use of the automated processed information and that the responsible party is expected to prove the rationale for the automated processing of online information.[274] However, it does not subtract from the fact that conscription would have occurred *ab initio* in section 71(1) of the POPIA in the public interest before section 71(3) applies.

Although the Supreme Court of Appeal held that there was an unlawful tapping of a telephone line in *State v Pillay*,[275] however, it unequivocally pronounced on the non-existence of online

---

[270] *State v Naidoo* supra 526 B - D.
[271] *State v Pillay* supra 431 G-432A, 445 B-J, 446J-447B; Van der Merwe *Unconstitutionally obtained evidence* 250.
[272] See the Preamble to RICA and section 30(1)(a) & (b) of RICA.
[273] See section 71(1) of the POPIA.
[274] See 'right related to automated decision making and profiling' in Eloff D 'Unscrambling the General Data Protection Regulation' http://www.derebus.org.za/unscrambling-the-general-data-protection-regulation/ (Date of use: 18 January 2019).
[275] *State v Pillay* supra 420 I. See para 3.5.7.8 of this study for further examination of the concept of conscription.

conscription in this case,[276] in contrast with the definition or description of the techno-legal approach and context of online conscription in this study. However, the High Court in examining the facts in *State v Naidoo* on the one hand waveringly denies the recognition of the existence of some of the nature and features of online conscription but on the other hand, unconsciously, erroneously and contradictorily affirms the legal existence of the elements of online conscription.[277]

In *State v Naidoo,* without the required factual matrix, two suspects —amongst others— were arrested by the SAPS after which they were released to 'trick confession or admission out of them' in their telephone conversation, which breaches the right against self-incrimination.[278] The conscripted telephone conversation evidence would not have been obtained, but for the general compellable use of online communication, devices and the subsequent participation of the two suspects in the construction, creation or discovery of the telephonic statement in which an OCI was simultaneously or immediately triggered off after the release of the suspects.[279] Accordingly, it is submitted that the facts in this case squarely corroborates the existence of the concept of offline conscription.[280]

In addition, arguably, based on the definition and description of an offline conscription principle and the instructive facts and ratio in *State v Naidoo* above, once a suspect is released on bail, online conscription is triggered off. It is therefore argued that if online conscription could take place while a suspect is on bail —who perhaps might ultimately not be prosecuted due to lack of sufficient evidence, it therefore follows that an OCI of an accused person during the criminal trial will certainly occur. For the prosecuting authority to proceed in a criminal trial impliedly means that it has a reasonable prospect of succeeding in the trial based on the sufficiency of the evidence, which must have been obtained in online communication, which is a further justification for the occurrence of online conscription.

[276] *State v Pillay* supra 447D-F.
[277] *State v Naidoo* supra 481C, 483F-I; 510F-J-511A-B. See para 2.3.3.1 of this study on the definition of offline conscription.
[278] *State v Naidoo* supra 480 D and 510F-J-511A-B; *Nel v Le Roux No* supra 3; Van der Merwe *Unconstitutionally obtained evidence* 250-251.
[279] *State v Pillay* supra 431G- 432A and 447D-F.
[280] *State v Pillay* supra 430B-F, 431 G-432A, 445 B-J, 446A - 447B -D; *State v Naidoo* supra 483 G-H; *Thint* supra 142 and 155; *Nel v Le Roux No* supra 3; Van der Merwe *Unconstitutionally obtained evidence* 202, 203, 210 and 250; Hubbard, Brauti and Fenton *Wiretapping* 10-26.10., 10-26.11 and 10-27 to 10-39.

In *State v Miller*, the High Court also contradicts itself by describing the existence of the nature and features of online conscription on the one hand and blaming users of online communication for consenting to bear the risks involved by the use of cellular telephones on the other hand as follows:

> 'The cell phone is *an integral part* of *modern-day life*, and there are *very few people who do not make use thereof*. *It provides instant, mobile and private communication to the users*. The cell phone is *ideally suited to the commission of crime*, whether for common law offences or under the more complex regime of POCA. Indeed, *hardly a day goes by in this court that we do not read or hear of the involvement of cellular communication in the commission of crime*…After all, *nobody has obliged anyone to make use of cellular communication* in a case such as this. If any of the accused elected to do so, *they willingly ran* the *risk* that *those communications may later* be *detected by* the *authorities*'[281]

Essentially, it is submitted that the immediate foregoing quote ostensibly or otherwise sums up the existence of some of the nature and features of online conscription in the following conjunctive ways, namely:

a) the existence of the twenty-first century indispensable and instant use of online communication devices by individuals;

b) the corresponding presumption by LEAs that every user of online communication is an automatic and instant suspect based on the expectation that online communication devices will be used by individuals for the commission of a crime; and

c) as a corollary to paragraphs (a) and (b), the instant readiness or mind-set of LEAs to simultaneously, spontaneously or automatically embark on an OCI as soon as a SIM-card or any form of an online communication device is activated.

However, contrary to the decision in *State v Miller*, more particularly paragraph (b) above, which expresses grave fallacy in the ratio of the court,[282] this study opines that in as much as the cellular telephone may be used for the commission of a crime, its primary or only purpose

[281] *State v Miller* supra 70 and 71. Italics mine.
[282] *State v Miller* supra 70 and 71. Italics mine.

of invention and reason for use is not restricted to crime commission. Arguably, the ratio of the court can be likened to the analogy that since cars are mostly used by armed robbers to commit car hijacking, the purpose of the invention and general reason for the use of a vehicle is to commit a crime.

Therefore, a precedent of this nature exposes users of cellular telephones to greater risks than the already existing inherent technical online conscription because the court erroneously, impliedly, stylishly and irrationally establishes a belief that every user of cellular telephones is expected to waive his or her right when using a cellular telephone. This belief negatives the argument for the protection of the invaluable asset in online communication, which is the gravamen of this study.[283]

Put differently, the High Court in *State v Miller* states that there is the foreknowledge that the use of mobile cellular telephone exposes a user to risks in the use of online communication, therefore the court blames users for waiving their right by still going ahead to use mobile cellular telephones; consequently, users should not turn around to complain about the invasion of their right to privacy in online communication.[284]

Essentially, the decision of the High Court is compelling users to comply with the Latin phrase that says that '*volenti non fit injuria*', which means that a user who waives his right to privacy by using a mobile cellular phone should not later turn around and complain about the invasion of his or her online communication by LEAs. In the U.S., the submission that users who are concerned about online communication breaches are at liberty not to use the Internet is tantamount to a coercive or compelling waiver of the right in online communication. The U.S. position is not only significantly myopic, reckless, defective and 'unproductive',[285] but draconian and conscriptive in nature and substance. The submission is short of saying that should you dislike air pollution, one must discontinue breathing or living.[286]

[283] See generally Chapter 3 of this study.
[284] *State v Miller* supra 70 and 71.
[285] The Economist *Online privacy* 360. 'We need to take personal responsibility for the information we share whenever we log on. But no amount of caution will protect us from the dispersal of information collected without our knowledge. If we're not aware of what data about us are available online, and how they're being used and exchanged, it can be difficult to guard against abuses', see Carr *Tracking is an assault on liberty* 368.
[286] The Economist *Online privacy* 360; Carr *Tracking is an assault on liberty* 368.

The High Court decision in the RSA holds users of online communication accountable for the reality of the existence of online conscription in online communication. The reality is to the effect that the moment an individual uses an online communication device, the right to online privacy is at risk and automatically and impliedly waived. This is because the inherent technical nature of an online communication brings the communication of a user into a 'dragnet'.[287] The inherent nature of online conscription can be likened to a chain of events, transactions or activities that a user of an online communication goes through.

The chain of events commences with the compulsory use of an online communication device in modern society. The compulsion emanates from the unavoidable,[288] indispensable and involuntary[289] second-by-second, minute-by-minute or day-by-day[290] immediate creations or uses of the online communications for personal, social, governmental and business or economic activities or enablers.[291] Consequently, LEOs who, *ab initio*, are at liberty to simultaneously violate the right to online communication, conclude the chain of events in online conscription by conducting an OCI based on the belief that every mobile cellular telephone communication is used or is likely to be used for the commission of crime.[292]

This belief generally places LEOs at liberty to inherently, irresponsively, unrestrictively, speculatively and perpetually access, obtain or discover archived and real-time content and meta or traffic data[293] without the knowledge, consent of or notice to the user of an online communication device in the covert conduct of OCI.[294] Accordingly, these events, transactions

---

[287] Affidavit in support of the Notice of Motion in *AmaBhungane v Minister of Justice* supra 125-136, more particularly paras 126 and 133; Regulations 5.1 and 5.2 of Schedule C of RICA; In SALRC 4.2.38 – 4.2.39 http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016), it states that 'Individual consent' justifies exceptions to some privacy principles. However, 'consent' is meaningless if people are not given full information or have no option but to consent in order to obtain a benefit or service. People have the right to withdraw their consent'.

[288] *Jafta v Ezemvelo* where a contract was held to be valid via an o-mail and accepted via an SMS, see De Jager *Electronic evidence* 437.

[289] *State v Miller* supra 70 and 72; Para 44 of the Respondents Affidavit in *AmaBhungane v Minister of Justice*.

[290] Watney *Cybercrime and investigation* 334.

[291] Watney *Cybercrime and investigation* 336. National Cybersecurity Policy Framework No. 39475 of 2015 paras 1 (of p 5), 1.2, 1.7, 2.1 and 8.1 and Eiselen *E-Commerce* 141-142.

[292] *State v Miller* supra 70 and 71. Italics mine.

[293] Blackman C and Srivastava L (eds.) *Telecommunication regulation handbook* – Tenth Anniversary Ed. (2011) vii, 3, 4, 5, 6, 7 and 23 (Blackman and Srivastava (eds.) *Telecommunication regulation handbook*); Watney *Cybercrime and investigation* 336; National Cybersecurity Policy Framework No. 39475 of 2015 at paras 1(of p 5), 1.2, 1.7, 2.1 and 8.1.

[294] Section 16(7)(a) of RICA; Electronic Front Foundation 'International principles on the application of human rights to communications surveillance'; *Web Call (Pty) Ltd v Stephen Andre Botha & Another* Case No: A 50/2014 18 (*Web Call v Botha*); *Absa v Moller* supra 6; Regulations 5.1 & 5.2 of Schedule C of RICA.

or activities create an atmosphere that `enables the use of an online communication device to become a 'fearful tool' in contemporary society.[295]

Essentially, the above immediate description implies that the communication of a user is trapped[296] between the devil (OCI) and the deep blue sea (online communication) from which LEAs or LEOs conduct an OCI, which is generally covert in nature. Without the indispensable use of an online communication device by an individual in the first place, conscription would not exist. Stated differently, it is submitted that the natural effect of the general use of an online communication automatically results in an online entrapment, which is equivalent to online conscription, and the reality in online communication in contemporary society.

The notion that the knowledge or unofficial advice that parties to a telephone conversation should beware of the possibility of interception is controversial, contradictory and surprisingly has mixed effect or blessing in online communication,[297] which breaches the right to the SOC and the duty to conduct an OCI as distinctively explained as follows.

First of all, without mincing words, the notion[298] is unimaginably and controversially consequential in the use of every online communication that is activated. The notion, which is compelling, constitutes a coercive consent to intercept or it constitutes a waiver of right in online communication.[299] The compelling nature is such that though the notion is advisory, which may or may not be taken, however, it is an instructive advice that is issued to and adversely affects every user of an online communication who has become enslaved to the use of the indispensable online communication tool and the consequential online conscription in contemporary society.

Secondly, the notion that the knowledge or unofficial advice that parties to a telephone conversation should beware of the possibility of interception[300] is contradictory. The contradiction arises from the fact that the notion is an unconscious notice or reminder of the

[295] Affidavit in support of the Notice of Motion in *AmaBhungane v Minister of Justice* supra 125–136, more particularly para 133.
[296] In *State v Odugo* 2001 (1) SACR 560 (W) evidence arising from entrapment was admitted, Van der Merwe *Unconstitutionally obtained evidence* 278-281 and 280-281, more particularly 280; *State v Miller* supra 70.
[297] *State v Naidoo* supra 525 C-D; McQuoid-Mason *Privacy II* 38-33; *State v Miller* supra 16, 35- 37 and 57-63.
[298] *State v Naidoo* supra 525 C-D; McQuoid-Mason *Privacy II* 38-33; *State v Miller* supra 16, 35- 37 and 57-63.
[299] *State v Naidoo* supra 525 C-D; McQuoid-Mason *Privacy II* 38-33; *State v Miller* supra 16, 35- 37 and 57-63.
[300] *State v Naidoo* supra 525 C-D; McQuoid-Mason *Privacy II* 38-33; *State v Miller* supra 16, 35- 37 and 57-63.

existence of online conscription, creating an alert or caveat in users of online communication and defeating the essence of the general nature of the covert *modus operandi* of an OCI, which is a dragnet and fearful tool.[301] The defeat arises from the fact that users of online communication are not generally and legally supposed to know about the pre or post conduct of an OCI, yet the notion does the opposite, thus the notion becomes counter-productive.

Thirdly, though the notion that the knowledge or unofficial advice that parties to a telephone conversation should beware of the possibility of interception[302] is controversial and contradictory as earlier described, however in disguise, it ironically has the effect of actually reducing, combating or even preventing the commission of some offences, which is a blessing in disguise. This is because it becomes difficult —if not impossible in some instances— for the commission or quick commission of some offences if users are afraid, careful or unable to use online communication to commit an offence based on the notion that the knowledge or unofficial advice that parties to a telephone conversation should beware of the possibility of the conduct of an OCI.[303]

Though this segment examines the jurisprudence of online conscription in South Africa, nonetheless, there is an acknowledgement of the existence of online conscription in some foreign jurisdictions in some ways. In noting the minority decision of the U.S. Supreme Court in *Riley v California* and *U.S v Wurie*[304] in online conscription with concurrence in this study, Alito J held that the use of a mobile cellular telephone is now 'an important part of human anatomy' in recognition of the autonomous or independent right in online communication.[305] It is acknowledged that the majority of the Americans use and carry mobile cellular

[301] *Mgomezulu v NDPP* (338/06) 2007 (ZASCA) 129 (RSA) paras 4 and 6 (*Mgomezulu v NDPP*) (*Mgomezulu v NDPP*); Regulations 5.1, 5.2, 6.1, 6.2, 6.3, 6.4(a)-(c) and (e) (more particularly (b)), 6.5, 7.11, 7.13 (a) & (b), 11.4(b), 11.1 -11.4 (e) &(f), 11.5, 12.7 , 12.9 (a) & (b), 12.13 and 16.9(a) & (b) of Schedule A of RICA and Regulations 5.1, 5.2 and 6.1- 6.4 (a) – (c) of Schedule C of RICA categorically, technically, legally and otherwise caution and prohibit LEAs from intercepting in a way that a target will know about the interception.

[302] *State v Naidoo* supra 525 C-D; McQuoid-Mason *Privacy II* 38-33; *State v Miller* supra 16, 35 - 37 and 57-63.

[303] *State v Naidoo* supra 525 C-D; McQuoid-Mason *Privacy II* 38-33; *State v Miller* supra 16, 35 - 37 and 57-63.

[304] *Riley v California* and *U.S v Wurie* supra 9, 16-17 and 28 of the Opinion and p 6 of the minority decision by Alito J where the court held the use of cell phone is now 'an important part of human anatomy'.

[305] *Riley v California* and *U.S v Wurie* supra 9, 16-17 and 28 of the Opinion and p 6 of the minority decision by Alito J.; Blumberg and Eckersley *Locational privacy* 313.

telephones,[306] which are also seen as tools of crime commission[307] and for this reason, entitle LEAs to embark on routine online conscription.[308]

Similarly, in the RSA, the use of an o-mail to make an offer of employment and acceptance of same via an SMS have become part of the human anatomy or life.[309] The submission in the U.S. that online conscription is the price that users pay in return for the huge enjoyment of the benefit derived from the massive investment in online communication[310] is arguably a coercive and compelling waiver of the right in online communication.

In Canada, the court acknowledges the existence of online conscription, but such acknowledgement is held with a caveat. The court in Canada held that although a voluntary consent is given by an individual to LEAs to intercept an online communication, an order of the court is still required to intercept.[311] This requirement in Canada is an indication that compels one to propose that automatic but yet a voluntary waiver of the right in online communication is practicably not feasible, otherwise it would constitute a coercive waiver.

In the RSA, although no court direction is required to confirm the exercise of the waiver of rights in online communication,[312] yet the grant of written consent on each occasion by a customer of a Telecommunication Service Provider to provide or grant access relating to the customer's online communication to anyone specified by the customer[313] must be unequivocal,[314] given the complex and delicate nature of online communication. Further, the right to waiver must include the right to withdraw the consent or to cool-off at any time for any reason whatsoever, if the user of online communication is dissatisfied with the earlier consent decision taken in this regard.

Finally, it seems generally difficult to deny or divorce the automatic or inevitable technical existence of the nature and features of online conscription in or from online communication, from which the covert conduct of OCI occurs, thus online communication is synonymous with

[306] Swire and Ahmad (eds.) *Part 5: Locational tracking* 245.
[307] Swire and Ahmad (eds.) *Part 4: Backdoor surveillance* 192.
[308] Swire and Ahmad *Introduction* 14; The Economist *Online privacy* 359-360.
[309] *Jafta v Ezemvelo* supra.
[310] The Economist *Online privacy* 357.
[311] Hubbard, Brauti and Fenton *Wiretapping* 3-20.7 to 3-20.8.
[312] Section 20 of POPIA.
[313] Section 14 of RICA.
[314] *NM v Smith* supra 22, 23, 41, 43, 56, 59, 61, 78, 80, 103, 137, 158 and 183.

and *inseparable* from online conscription and vice versa. Whether a user of online communication is aware or not of the possibility of an online interception, online conscription still occurs anyway because online conscription is an automatic activity or process in online communication.[315]

Although the courts in the RSA do not believe in the automatic existence of online conscription in an online communication from the moment an individual uses an online communication device,[316] the worst scenario that should generally be permissible, though without conceding, is to equitably or reasonably regard an online communication as a quasi, passive, indirect, and implied conscription.

Nevertheless, although controversial, an offline entrapment is the only effective alternative way of detecting the commission of some crimes.[317] Thus, procuring evidence through an OCI in online conscription is an effective alternative procedure in gathering evidence, which should generally be permissible and considered for admissibility in appropriate instances.[318]

2.3.3.6 Forms of online conscription

a. Non-criminal online conscription

One of the best descriptions to assign to non-criminal online conscription is to refer to the description of online marketing and advertising, which results in online conscription as described above.[319] Basically, marketing requires that for a business to identify and satisfy consumer needs; companies need to have an 'extensive data collection' of consumers.[320] Related to the marketing belief expressed above[321] is 're-targeting', which is a concept that enables a marketer to drop cookies on an online visitor who does not buy any item on a website but who is reminded of other items that may be of interest in future purchases.[322]

---

[315] *State v Naidoo* supra 525 C-D; McQuoid-Mason *Privacy II* 38-33; *State v Miller* supra 16, 35- 37 and 57-63.
[316] *State v Pillay* supra 447D-F; *State v Naidoo* supra 510F-J-511A-B; *State v Miller* supra 70.
[317] Van der Merwe *Unconstitutionally obtained evidence* 278.
[318] Para 7.8 of Chapter 7 of this study for the examination of the admissibility of evidence obtained in an online conscription.
[319] See paras 2.3.3.3 - 2.3.3.4 of this chapter.
[320] Swire and Ahmad (eds.) *Part 6: Online privacy* 330.
[321] See paras 2.3.3.2 - 2.3.3.4 of Chapter 2 of this study.
[322] Madrigal *I'm being followed: How Google-and 104 other companies- Are tracking me on the web* 344-345.

However, the danger in the above-described marketing, advertising and retargeting scenarios is that companies use the collected personal data to predict, influence or manipulate the thoughts and behaviour of consumers in an 'invisible' way,[323] thus, consumers become enslaved to the whims and caprices of the marketing and advertising companies.

Another instance of non-criminal online conscription, which is found in a foreign jurisdiction is the storage of the DNA of all British citizens and visitors in a database for administrative purposes.[324] In as much as this type of online conscription is encouraged or protected, which also helps in combating crime (*inter alia*), however, the storage of DNA of all individuals poses serious risks in the protection of the right to the SOC in the same or similar way that the increasing foreign campaign, justification and use of microchips in the body of an employee for ingress and egress purposes in an office or other restricted areas.[325] Therefore, the abovementioned instances constitute non-criminal online conscription

b. Criminal online conscription

First and broadly, it is submitted that criminal online conscription is derived from non-criminal conscription, which entails the collation or collection of online data innocently or neutrally stored or recorded by private and public entities for general utility purposes. However, in pursuance of combating crime in the interest of the public, the various stakeholders involved in collating, transmitting, storing and dealing with information[326] are obliged to cooperate in surrendering such non-criminal information to LEAs to conduct an OCI[327] of serious offences or in exceptional circumstances. In a way, criminal online conscription impliedly entails the use of the retrospected online conscription of data.

In the U.S., third parties such as Internet Service Providers, libraries, phone companies and political parties —amongst others— are obliged to hand over personal data of individuals — from the stored online conscription— to FBI and CIA without court direction or consent of an individual for international terrorism.[328]

[323] Carr *Tracking is an assault on liberty* 369.
[324] The Economist *Learning to live with big brother* 29.
[325] The Economist *Learning to live with big brother* 25 and 33.
[326] See para 6.11 of Chapter 6 of this study. The quadripartite stakeholders are the LEAs, court, Online Communication Service Providers and Interception Centre.
[327] The Economist *Learning to live with big brother* 26.
[328] The Economist *Learning to live with big brother* 30.

Second and narrowly, criminal online conscription occurs in a situation where a court order is directed at the prospective online communication of a target to conduct an OCI of a serious offence.

Third and specifically, a criminal online conscription occurs in special circumstances, for example, where prisoners are monitored by online communication devices outside the prison walls to reduce congestion.[329] Special monitoring devices for restricted persons are built on the principle of 'Exclusion and Inclusion' zones.[330] The device may exclude an individual from going to an area while at the same time requires the individual to be at a venue at a particular time, such as being in school during the period of a correctional program.[331] The online communication device can also be used to build up and record a map of the movement of the individual in a correctional program.[332]

A criminal online conscription could also come in form of an online communication house arrest device through the use of a radio-frequency-based technology that is tied to the ankle of an individual with a transmitter around the house.[333] An alarm goes off if the individual goes too far from the transmitter, which indicates that the individual has gone beyond the approved zone.[334] Other devices monitor real-time locations of criminals up to few meters.[335] A device could also simultaneously notify the perpetrator and the LEA of the development around a perpetrator by instructing the perpetrator to leave the prohibited environment, otherwise, the alarm would trigger or increase in volume.[336]

Finally, it is submitted that the above instances constitute criminal online conscription.

2.3.3.7 Permissible instances of online conscription

Arguably, the foregoing discussions attempt to establish the existence of techno-legal nature and features of online conscription, which, according to the components of an offline

[329] Wood *Prison without walls* 290-292; Swire and Ahmad (eds.) *Part 5: Locational tracking* 246; Crump *Geolocational Privacy and Surveillance Act* 273 and 280; Wood *Prison without walls* 305.
[330] Wood *Prison without walls* 298.
[331] Wood *Prison without walls* 298.
[332] Wood *Prison without walls* 298.
[333] Wood *Prison without walls* 296 – 297.
[334] Wood *Prison without walls* 296 – 297.
[335] Wood *Prison without walls* 297.
[336] Wood *Prison without walls* 297.

conscription principle, is an unlawfully or unconstitutionally obtained evidence, therefore considered for admissibility or otherwise in section 35(5) of the Constitution of the RSA.[337] This is opposed to the U.S. principle of admissibility of unlawfully obtained evidence, which outrightly does not admit unlawfully obtained evidence.[338]

Nonetheless, it is submitted that it is generally permissible to regularise the use of online conscription as a source of gathering evidence in an online communication notwithstanding the unlawfulness of online conscription as a source of evidence gathering. This is because, despite the unlawfulness of the evidence obtained from online conscription, the evidence cannot always be categorised as void evidence. This is because its voidness creates a regrettable, irredeemable and injusticeable lacuna in the administration of justice in the twenty-first-century quick-silver technology era, which compellingly places every evidence obtained in online communication as automatically inadmissible.

The nature of the permissibility of evidence obtained from online conscription is important such that it does not outrightly regard an online conscription as a piece of void evidence. However, the nature of the permissibility regards online conscription as a voidable form of evidence, which practically gives effect to the pragmatic application of section 35(5) of the Constitution, which —instead of outrightly rejecting evidence obtained from online conscription— may admit unlawfully obtained evidence subject to the conditions provided in section 35(5). Since online conscription is a necessary technical evil,[339] which automatically occurs in every online communication because online communication is a necessity in contemporary society,[340] the occurrence of online conscription is inevitable.

According to the words of Jager on the admissibility of evidence, he observes that the unavoidable use of online communication has led to an increase in the use of online evidence in judicial proceedings in the RSA,[341] therefore, online evidence cannot *ab initio* be outrightly inadmissible save where it is statutorily void, which constitutes double jeopardy.[342] The jeopardy comprises the unavoidable technical online conscription and the online conscription

[337] Section 35(5) of the Constitution; Van der Merwe *Unconstitutionally obtained evidence* 198 - 201 and 257.
[338] Van der Merwe *Unconstitutionally obtained evidence* 199.
[339] Sections 18 and 38(1) of POPIA.
[340] *State v Miller* supra 70.
[341] De Jager *Electronic evidence* 437. *State v Miller* supra 70.
[342] Paras 7.8.2 - 7.8.5 of Chapter 7 of this study.

that does not comply with statutory requirements that regulate the technical online conscription.

It is submitted that the voidability principle, which is neither here nor there, seeks to strike a balance in the conflict of interests between a victim and a perpetrator of crime. In this regard voidability principle arguably states that the most preferred option or solution that can be advocated in a situation where evidence can only be obtained unlawfully —through online communication, which is ordinarily used for lawful activity— is to permit the unlawfulness of online conscription in some instances in section 35(5) based on the alternative necessity to conduct an OCI in the interest of the public.[343]

The regularisation of the unlawfulness of evidence obtained from online conscription is ordinarily permissible with regards to criminal online conscription,[344] save in some non-criminal online conscription cases where there is an unequivocal written consent of the right of the customer to waiver in section 14 of RICA[345] subject to the flexible application of section 35(5) of the Constitution.[346]

Therefore, this study proposes that five specific instances of online conscription -amongst others- are generally permissible in law because of the necessity of conducting an OCI in some circumstances.[347] These instances below assist in applying the proportionality principle by classifying the application of online conscription according to the exigency and the degree of serious offences in the various categories.

In other words, the proportionality principle in this regard states that the more serious an offence, the earlier, and deeper an online conscription takes place through the conduct of an OCI in terms of the opportunity and duration of the conduct of an OCI. It is noted that although RICA provides for the duration of the conduct of an OCI,[348] however, it does not make provision on the extent to which an OCI could be *retrospectively* or *prospectively* conducted before this study.[349] It arguably follows that an OCI has always been conducted

[343] *State v Naidoo* supra 520H.
[344] Para 2.3.3.7 of this chapter.
[345] See the concluding remarks of para 2.3.3.5 of this chapter. Section 14 of RICA.
[346] Para 2.3.3.6 of this chapter.
[347] *State v Naidoo* supra 520 H.
[348] Sections 16 (6), 17(1), 20(4), (5), (6) and 21(5)(e) of RICA.
[349] Para 2.5.2 of this chapter.

disproportionately where LEAs have always been *retrospectively* and *perpetually* conducting an OCI in the RSA.[350]

However, in Canada, an OCI of all categories of serious offences is conducted with respect to *only future* online communications of a user commencing at a time after obtaining a court order.[351] Thus, the proposed five instances below seem reasonably and justifiably proportionate in the conduct of an OCI in the RSA than in Canada which restricts itself to the conduct of an OCI in future online communications only.

It is noteworthy to consider the uniqueness of the proportionality principle in the permissibility of online conscription as proposed in this study when conducting an OCI in the RSA. This is because it may be misleading or mischievously tempting to apply the offline proportionality principle to the conduct of an OCI by unrestrictively, retrospectively and perpetually conducting an investigation. The misleading part is that since there is no retrospective restriction of investigating offline conscription, LEAs believe that there should not be any retrospective restriction in engaging in online conscription.

Therefore, the belief by or understanding of LEAs is that the proportionality principle should not apply to an online communication once access into the online communication of a user has been legally secure. However, even in common law offline principle, it provides for three levels of the reasonable continuum of secrecy of offline communication,[352] thus, at some point, there must be a limit to which LEAs can access an online communication. The three levels give effect to the application of the offline proportionality principle, which determines the limits or how deep LEAs can intrude into the privacy of an individual subject to the seriousness of an offence.[353]

Nevertheless, in the case of online conscription, since the conduct of an OCI is an alternative method of investigation, which is only resorted to after LEAs would have complied with the requirements in the 'necessity' principle,[354] LEAs are not expected to proceed beyond the approved level of intrusion in an online communication subject to the seriousness of an offence

[350] Para 2.5.2 of this chapter.
[351] Hubbard, Brauti and Fenton *Wiretapping* 4-2 and 4-2.10 to 4-2.12.
[352] Para 3.7 of Chapter 3 of this study.
[353] Para 3.8 of Chapter 3 of this study.
[354] Para 6.5 of Chapter 6 of this study.

committed. It would therefore not be surprising for a reader of this study to contest some of the propositions propounded below, one of which is the 'mid-spective' online conscription which has a unique but simplified mathematical calculation[355] to proportionately make a distinction between it and other instances proposed below in paragraphs (b)-(d).

No matter how small the margin of proportionality is in the mathematical calculation in these instances or in the opportunity and duration of the conduct of an OCI, especially in paragraph (d), the significance of applying the proportionality principle attempts to strike a balance in the conflict between the protection of the right to the SOC and effective conduct of an OCI. In effect, the normative or qualitative value or functionality of the mathematical calculation in the distinction or margin in these instances should be considered on merit, rather than considering the quantitative value of the narrow distinction in paragraph (d), which may be misleading to dismiss the distinctive functions in these instances.

a. Preservative blanket online conscription

It is submitted that a preservative blanket online conscription is permissible in online communication, though subject to the provisions of the POPIA.[356] This instance of online conscription occurs where LEAs, without the existence of sufficient factual matrix required to justify the conduct of an OCI of an offence at any of the relevant corresponding stages of crime commission,[357] access, obtain or discover data in online communication in pursuance of a court order due[358] to the vulnerability of loss or modification of an online data.[359] Since the conduct of this type of an OCI is very intrusive, certain stringent conditions are fulfilled before a court grants such a direction.[360]

Amongst the conditions proposed is that a full bench of three judges of the High Court considers a real-time interoperable audio-visual or audio *Popoola QOCI* application procedure

[355] See para 2.3.3.7 (d) of this chapter below.
[356] Chapters 3 and 4 of the POPIA. Distributing data to a third party should not be allowed, Thompson *GPS monitoring* 249.
[357] Paras 6.3.3.2 (c) - (e), 6.3.3.3(c)-(e), 6.3.3.4 (c)-(d) and 6.3.3.5 (c)-(e) and 6.4.5 – 6.4.7 of Chapter of this study.
[358] Para 6.4.3 of Chapter 6 of this study.

[359] Sections 40 - 43 of CCB 2017; Arts 29(3), (4) & (5), 31(3)(a) of Council of Europe 'Chart of Signatures and Ratifications of Treaty 185 - *Convention on Cyber Crime* -Status as at 02/06/2017 (CoE CoCC).
[360] Paras 6.3 - 6.6 of Chapter 6 of this study on the requirements for the conduct of various forms of OCI directions.

in a preservative blanket online conscription.[361] In this procedure, it requires that an OCI cannot be conducted without the quadripartite parties who are engaged in the interoperable procedure —namely: LEAs, court, Online Communication Service Providers and Interception Centre. The online interception system is configured in such a way that LEAs cannot have access to the interception system without an online application to and direction by the court.[362] The signal is sent to the Online Communication Service Provider while the Interception Centre is only able to intercept if the online signatures of the three other stakeholders are approved in their various online signatures before the delivery of the signal to the Interception Centre.[363]

However, since a preservative order does not require the usual factual matrix to justify the conduct of an OCI of any relevant offence at any of the relevant corresponding stages of crime commission, the preserved data is not accessed but routed to the Interception Centre for fear of giving an impression that the conduct of an OCI is complete for the information to be released to the LEAs.

Alternatively, without any form of access by LEAs, Online Communication Service Provider and Interception Centre in the *Popoola QOCI* protocol;[364] the Online Communication Service Provider —as the exclusive security administrator of the data in the intervening period— stores the data in trust for the Court for further directive from the Court.

An Online Communication Service Provider administers the data —without knowing the preserved content— until such time that there is a sufficient factual matrix to conduct an OCI by which time the data or content is then routed to the Interception Centre for dispatch to LEAs, otherwise, the data is destroyed at a point in time determined by the court if no further fact is gathered to proceed with the conduct of an OCI according to the forms of the proportionality principle.[365] It is noted that while the data is exclusively kept with the Online Communication Service Provider in a preservative blanket online conscription process, the online system is configured in a manner that no one has access to the data including the quadripartite.

[361] See paras 2.5.1, 2.5.2, 2.11.3, 2.11.4 and 6.11 of this study on the application of the *Popoola QOCI* application.
[362] Para 6.11 of Chapter 6 of this study.
[363] Para 6.11 of Chapter 6 of this study.
[364] Para 6.11 of Chapter 6 of this study.
[365] Para 5.4 of Chapter 5 of this study.

According to the general OCI proportionality principle espoused in this study,[366] it is proposed that, save where the Court decides otherwise, a preservative OCI is more reasonable, rational and justifiable for the investigation of offences that could lead to the declaration of the state of emergency or constitute actual or potential threats to the State of the RSA, public safety or security in section 16(5)(a)(ii) and (b) of RICA.[367] In this regard, given the complex and delicate nature and features of online communication,[368] it is submitted that a preservative blanket order may not be granted in 'general serious offences',[369] save where the effect of the commission of a general serious offence is irreversible.

b. Absolute retrospective online conscription

As a corollary to the first permissible instance of online conscription above, it is permissible to conduct an absolute retrospective OCI into the online communications of a user before and after committing a serious offence. The collection of information in this instance is both *retrospective* and *perpetual* in time, which is not limited to the time of committing the offence. For example, if a serious offence was committed on 26 June, 2016 and detected on 26 June, 2018, a retrospective OCI allows the gathering of information earlier than 26 June 2016 and into the future till the period permitted by the court, subject to the proportionality and 'first fact factor' principles.[370]

In this instance, a full bench of three judges of the High Court considers a real-time interoperable audio-visual or audio *Popoola QOCI* application,[371] the procedure of which ends at the Interception Centre which grants access to LEAs to conduct an OCI in pursuance of the direction of the court.

According to the general OCI proportionality principle espoused in this study,[372] it is proposed that, save where the court decides otherwise, an absolute retrospective OCI is more reasonable, rational and justifiable for the investigation of offences that could lead to the declaration of the

[366] Paras 5.3.4, 5.3.6 and 5.4 Chapter 5 of this study.
[367] Paras 6.3.3.2(e), 6.3.3.3(e), 6.3.3.4(d), 6.3.3.5(e), 6.4.5 -6.4.6 of Chapter 6 of this study.
[368] Paras 2.3 of Chapter 2 and Chapter 3 of this study.
[369] Paras 6.3.3.2 (b), 6.3.3.3(b), 6.3.3.4(b) and 6.3.3.5 (b) of Chapter 6 of this study.
[370] Paras 2.5.2 of this chapter.
[371] See para 6.11 of Chapter 6 of this study on the application of the *Popoola QOCI* application.
[372] Para 5.3.4, 5.3.6 and 5.4 of Chapter 5 of this study.

state of emergency or offences that constitute actual or potential threats to the State of the RSA, public safety or security in section 16(5)(a)(ii) and (b) of RICA.[373]

This is because embarking on an absolute retrospective conduct of an OCI for offences that are not in the aforementioned categories will be disproportionate to the level of intrusion that will occur in online communication. The more serious an offence, the more LEAs will go back in time to retrieve the communication relating to the commission of an offence.

c. Retrospective online conscription

It is permissible to conduct a retrospective OCI[374] into the online communication of a user before and after the detection of the commission of a serious offence. The collection of information is not conducted perpetually in time but limited to the time of the commission of the offence. For example, if a serious offence was committed on 26 June, 2016 and detected on 26 June, 2018, the conduct of a retrospective OCI does allow the gathering of information earlier than 26 June, 2018. However, the conduct of a retrospective OCI allows for the collection of information up to 26 June, 2016 and into the future till the period permitted by the court, subject to the proportionality and 'first fact factor' principles.[375]

In *State v Naidoo*, LEAs unlawfully approached MTN and Vodacom —two of the mobile cellular telephone operating companies in the RSA— without applying to the court to conduct a mass retrospective non-content OCI to determine who made some telephone calls in the night of the robbery incident in the vicinity.[376] On granting their request, which was a retrospective non-content OCI, LEAs proceeded to court to prospectively monitor the landline telephone of one Mrs R.[377]

According to the general OCI proportionality principle espoused in this study,[378] it is proposed that, save where the court decides otherwise, a retrospective OCI is more reasonable, rational and justifiable for the investigation of offences in section 16(5)(a)(ii) and (b) of RICA in most

[373] Para 6.3.3.2 (e), 6.3.3.3(e), 6.3.3.4 (d), 6.3.3.5(e) of Chapter 6 of this study.
[374] *State v Miller* supra 66. See also para 2.3.3.6 of this study titled 'Forms of online conscription'.
[375] Para 2.5.2 of this study.
[376] *State v Naidoo* 480 supra H.
[377] *State v Naidoo* 480 supra H.
[378] Paras 5.3.4, 5.3.6 and 5.4 of Chapter 5 of this study.

serious offences[379] and other related offences in this category than the other classes of offences. This is because embarking on the retrospective conduct of an OCI in offences that are not in the aforementioned categories will be disproportionate to the level of intrusion that will occur in any online communication. The more serious an offence, the more LEAs will go back in time to retrieve the communication relating to the offence, otherwise, a prospective OCI is conducted in generally serious offences.

d. 'Mid-spective' online conscription

It is permissible to conduct a 'mid-spective' OCI, which is a term coined in this study to describe online conscription that is conducted in the online communication of a user which is at the mid-point or reasonable region of the mid-point between the time of committing a serious offence and its detection. Besides, the midpoint is calculated into the future. For example, if a serious offence was committed on 26 June, 2016 and detected on 26 November, 2018, the mid-point where an OCI is conducted commences 26 June 2017 and into the future till the period permitted by the court, subject to the proportionality and 'first fact factor' principles.[380]

Given that a two-year period is in between the date of commission and detection of an offence in the above illustration, the midpoint is a year after the commission of the serious offence or a year before the detection of the commission of the offence.[381]

According to the general OCI proportionality principle espoused in this study,[382] it is proposed that, save where the court decides otherwise, a mid-spective' OCI is more reasonable, rational and justifiable for the investigation of 'more serious offences'[383] than other classes of offences.

e. Prospective online conscription

It is permissible to conduct a prospective OCI[384] into the future online communication of a user after the commission of a serious offence, which is the same and only way an OCI is conducted

[379] Paras 6.3.3.2(d), 6.3.3.3 (d), 6.3.3.4(d) and 6.3.3.5(d) of Chapter 6 of this study.
[380] Para 2.5.2 of this study.
[381] See the caveat on the significance of the quality than the quantity of evidence obtained in mid-spective conscription in para 2.3.3.7 (d) of this chapter.
[382] Paras 5.3.4, 5.3.6 and 5.4 of Chapter 5 of this study.
[383] Paras 6.3.3.2(c), 6.3.3.3(c), 6.3.3.4(c) and 6.3.3.5(c) of Chapter 6 of this study.
[384] See para 2.3.3.6 (b) of this study; *State v Naidoo* 480 supra H.

in Canada in all categories of offences.[385] This type of OCI conduct does not go back into the past communication of a user before the commission or detection of the commission of an offence. For example, if a serious offence was committed on 26 June, 2016 and was detected on 26 June, 2018, the conduct of a prospective OCI allows for the collection of information commencing after 26 June, 2018 till the period permitted by the court, subject to the proportionality and 'first fact factor' principles.[386]

According to the general OCI proportionality principle espoused in this study,[387] it is proposed that, save where the court decides otherwise, a prospective OCI is more reasonable, rational and justifiable for the investigation of 'general serious offences' than the other classes of offences.[388] 'General serious offences' are the least sets of offences recognised for investigation by the conduct of an OCI in RICA.[389] An OCI is generally not used for conducting less serious or minor offences —save in some exceptional circumstances—[390] because the levels of intrusion in online communication are more serious than in non-online communication.

2.3.3.8 Conclusion

If Google, etc. had not been engaging in online conscription, it would not have had the success it has had or would not have been able to provide information to users the way it has been.[391] Aside from the online conscription by Google and other search engines, online conscription exists technically and statutorily in the domestic operation of the online communication services despite the denial by the courts in the RSA of the existence of online conscription. Given these facts, it is more difficult for consumers to exercise control over their personal information, thus, new policy and regulation on online communication are urgently needed.[392]

[385] Hubbard, Brauti and Fenton *Wiretapping* 4-2 and 4-2.10 to 4-2.12.
[386] Para 2.5.2 of this study.
[387] Paras 5.3.4, 5.3.6 and 5.4 of Chapter 5 of this study.
[388] Paras 6.3.3.2(b), 6.3.3.3(b), 6.3.3.4 (b) and 6.3.3.5(b) of Chapter 6 of this study.
[389] Paras 6.3.3.2(b), 6.3.3.3(b), 6.3.3.4 (b) and 6.3.3.5(b) of Chapter 6 of this study.
[390] One of the special circumstances is where a less serious or minor offence is considered under the first stage of crime commission which poses 'severe national risk' in the RSA.
[391] Harper *It's modern trade: Web users get as much as they give* 374.
[392] The Economist *Online privacy* 357.

2.4 THE CONSTITUTIONALITY OF THE CONDUCT OF COVERT OPERATION IN ONLINE CRIMINAL INVESTIGATION

Although the obligation to conduct an OCI, which is a covert method of investigation,[393] is not provided in the Constitution, however, the obligation falls under the omnibus power of the LEAs to investigate offences in online communication. This power is one of the measures recognised in section 36 of the Constitution to limit the right to the SOC in online communication, as examined in this study.[394]

Notwithstanding that the conduct of an OCI falls under the general powers of LEAs to limit any right in section 36 of the Constitution, the non-recognition and non-protection of the specific power of LEAs to conduct an OCI in the Constitution is incongruous. This is because this defect in the Constitution creates an atmosphere that undermines the requisite recognition, protection and adequacy of the regulation of the conduct of an OCI by stakeholders in various ways.

This constitutional defect ranges from the non-recognition and non-protection of the activity of an OCI as a specialised profession and as a complex, delicate and unique method of investigation to the inadequate regulation on the accountability and oversight of stakeholders involved in the investigation of crime,[395] including the conduct of an OCI. Consequently, this defect contributes to the breach of the conduct of an OCI by the stakeholders.

Accordingly, one of the ways of curing this constitutional defect is to imperatively and simultaneously consider the reasonableness, rationality and justification of the conduct of an OCI in the Constitution side by side the protection of the right to the SOC as an independent

---

[393] The Constitutional Court generally describes covert investigation, though not in the context of OCI, see *Bernstein v Bester No* supra 37 and 38. Although the Judge President's Regulation under the repealed Interception and Monitoring Act No 127 of 1992 was published, the operation of OCI was shrouded in absolute secrecy while some of the provisions were inadequate, see *State v Naidoo* supra 504 D-G and 515 B (N). Sections 2, 198(c), 199(4), (5), (6), 205(2) and (3) and 210(a) of the Constitution require that intelligence and security services be statutorily regulated or implemented. It has been held by the court that secrecy makes transparency, impartiality and checks and balances and oversight difficult, if not impossible to practice in the conduct of OCI, *Primemedia v Speaker, National Assembly* supra 17 of majority decision and paras 14, 20 and 36 of Savage J.

[394] Chapter 5 of this study examines several issues in section 36 of the Constitution relating to the conduct of OCI of serious offences, which limits the right to the SOC; SALRC 2.3.36 http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016).

[395] Paras 2.5 - 2.11 of Chapter 2 and chapters 4 -8 of this study.

right in section 14 of the Constitution.[396] This consideration is the basis for the similar and specific constitutional protection of the obligation to conduct an OCI in online communication,[397] given the natural conflict between the two divides, which can fundamentally be managed by the recommendation made herein in an attempt to strike a balance in the conflict between these two subject matters. The philosophical constitutionalism for this proposition is further and extensively addressed under the need for the constitutional protection of the right to the SOC.[398]

2.5 NATURE AND FEATURES OF ONLINE CRIMINAL INVESTIGATION

2.5.1 Introduction

In its nature and features,[399] an OCI is an alternative procedure used in conducting a criminal investigation in a wired or wireless online network, device, technology, application and services in content and non-content or metadata communications,[400] real-time and archived or stored communications and Internet and non-Internet based platforms[401]which must by law have interception devices or solutions.[402]

In the conduct of an OCI, there are four key stakeholders whose roles are examined in subsequent chapters in this study.[403] The quadripartite role-players who are involved in the interception of data are: i) a 'LEA' or 'LEO' who makes an OCI application before; ii) the 'Court' for consideration and communication of its decision —whether granted or not to; iii) the 'Online Communication Service Providers' for appropriate action or inaction to; iv) the 'Interception Centre' which executes the appropriate action or inaction from the decision of the Court.[404]

---

[396] Paras 2.2.2.2 and 2.3.1 - 2.3.3, Chapter 3 of this study, more particularly para 3.11, Chapter 6 and Chapter 8, more importantly para 8.6.
[397] Paras 2.5 - 2.11 of Chapter 2 and chapters 4 -8 of this study.
[398] Para 3.11 of this study.
[399] Art 18(18) and 24(2)(b) and (4) of TOCC and Art 25(3) of CoE CoCC.
[400] Sections 1 and 1, 12, 13, 14, 15, 17, 18 and 19 of RICA; Berkowitz R 'Packet Sniffers and Privacy: Why the No-Suspicion-Required Standard in the USA Patriot Act is Constitutional' 2002 7 *Computer Law Review and Technology Journal* 2-8 (Berkowitz 2002 7 *Computer Law Review and Technology Journal*); Watney *Cybercrime and investigation* 340.
[401] Sections 1, 12, 13, 14, 15, 17, 18 and 19 of RICA.
[402] Caproni *Lawful electronic surveillance* 206; Sections 28(1)(ii), 29(3)(a), (4), (5)(b), (7)(c) and (8)(a), 30 (1)(a) and (b), (2), (3), (4) and (5), 31(1)(a), (2)(a) and (b) and 44 of RICA.
[403] The roles of these key players are examined in chapters 4, 6 and 7 of this study.
[404] Para 6.11 of Chapter 6 of this study.

2.5.2 Nature and features of the practice of online criminal investigation

Conducted at any time of the day and night and without the issuance of any prior or post-notice by LEAs to the user of online communication,[405] an OCI, as aforementioned, is a covert method of investigation,[406] which is conducted through a wired or wireless online network,[407] including Bluetooth technology[408] to investigate serious offences committed offline and online.

An OCI is a complex, delicate and unique form of investigation derived from the broad offline and online terms or concepts of 'interception', 'monitoring' and 'surveillance',[409] which are interchangeably, positively[410] or negatively and ubiquitously applied or used in conducting an investigation. What makes an OCI ubiquitous,[411]complex, delicate and unique in the broad concept of 'interception', 'monitoring' and 'surveillance' is the same or similar nature and features that make the protection of the right to the SOC complex, delicate and unique in the broad concept of privacy in section 14 of the Constitution,[412] the inadequacy of which gives birth to the right to the SOC.

Intercept means 'the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the':

(a) monitoring of communication through a monitoring device;

(b) examination, inspection or viewing of the substances of an indirect communication; and

(c) diversion of indirect communication from its originally intended destination to another

[405] Section 16(7) of RICA.
[406] 'Corruption thrives in secret places, and avoids public places, and we believe it is a fair presumption that secrecy means impropriety', see 'My child, if there is nothing wrong with bio-scope, why then must they always be screened in the dark', Van der Vyver *State secrecy* 48.
[407] Watney *Cybercrime and investigation* 334; Van der Merwe *Telecommunication law* 13- 21.
[408] *State v Terrence Brown* supra 6.
[409] Sections 1 and 22 of RICA.
[410] See the latter part of this para for the illustration of the positive use of an online interception for the benefit of a user of an online communication.
[411] Thornton *Telecommunications law* 25-26.
[412] See generally paras 2.2 and 2.3 of this study where the foundation for the protection of the right to the SOC is introduced and highlighted through the general and special features of online communication.

destination.[413]

'Monitor' includes the act of listening to or recording communications through a monitoring device, while 'monitoring' has a corresponding meaning'.[414]

Surveillance is not identified nor defined in RICA. However, surveillance is rooted from the French word '*surveiller'*, which has been used in the spying, espionage and warfare environment for about two centuries[415] and is regarded as a 'back-door' or clandestine method of search which is conducted absenting the knowledge or permission of the residents.[416]

Generally, in this study, the conduct of an OCI includes online cloning of data,[417] 'dataveillance',[418] decryption and retention or preservation of data or online communication.[419]

Although the abovementioned concepts could be negatively used to limit the right to the SOC under the concept of an OCI, however, the use of these concepts may not necessarily or always connote a negative stance in some circumstances.[420] From the beneficial or positive sense, surveillance is used for everyday activity, such as weather forecasts or prediction, day planning or future planner, flying aircraft, anticipating drought, etc.[421] In RICA, interception and monitoring may also be used for positive purposes such as quality control,[422] emergency and technical purposes.[423]

As previously mentioned, an OCI is an alternative method of investigation, which requires that other methods of investigations must have been conducted or attempted before embarking on an OCI.[424] However, an OCI may be conducted in the first instance of an investigation where

---

[413] Section 1 of RICA; Watney *Cybercrime and investigation* 339-342; Newton H *Newtons' telecom dictionary* 2006 (22nd ed.) 484 (Newton *Newtons' telecom dictionary*).
[414] Section 1 of RICA.
[415] Swire and Ahmad *Introduction* 2.
[416] Swire and Ahmad (eds.) *Part 4: Backdoor surveillance* 191.
[417] *Okundu v State* supra 7 and 12.
[418] 'Dataveillance is the tracking of metadata', White A 'A Brief History of Surveillance in America: With wiretapping in the headlines and smart speakers in millions of homes, historian Brian Hochman takes us back to the early days of eavesdropping' (Date of use: https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/ (Date of use: 18 June 2018).
[419] Watney *Cybercrime and investigation* 339-342.
[420] Swire and Ahmad *Introduction* 3.
[421] Swire and Ahmad *Introduction* 2-3.
[422] See also the meaning of monitor, Newton *Newtons' telecom dictionary* 599.
[423] Sections 6 -11 of RICA, amongst others.
[424] Section 16(2) (e) & (5)(c) of RICA; Para 6.5 of Chapter 6 of this study.

the other methods may not yield the desired outcomes under different circumstances provided in RICA.[425] These outcomes require special conditions for such an application to succeed.[426]

Upon filing a written application in court, the execution of an OCI may commence in both retrospective, and prospective ways on the date or thereafter of the issuance of a direction from court because there is no clear provision in RICA on the application or limitation of the retrospective or prospective conduct of an OCI in RICA, though the Court is empowered to issue the conduct of an OCI for a determinable period.[427] In certain urgent or exceptional instances, an oral application and direction is made to and granted by the court, in which RICA does not also state whether it is an automatic retrospective conduct of an OCI.[428]

An OCI is conducted for a period, which impliedly, may not exceed three months at a time.[429] However, upon a review by the court, a direction may be extended beyond three months in certain instances.[430] An OCI is conducted in real-time communication on an on-going basis, where required, provided no OCI direction already exists.[431] However, a perpetual OCI may not be conducted in archived or real-time communications in terms of other Acts such as the CPA.[432] Regarding the general application of other Acts, this study contests the general conduct or applicability of an OCI in section 205 of the CPA or *vice versa*.[433]

The provision of various durations of the conduct of an OCI introduces the 'interception duration proportionality' principle to this study, which prescribes that the duration of an OCI is dependent on the degree of serious offences committed.[434] It is submitted that the 'interception duration proportionality' principle requires that the duration of the conduct of an OCI must be subject to the first set of available facts gathered by LEAs in the conduct of an OCI of such serious offence to determine how long an OCI will be conducted or continued.

[425] Section 16(2) (e) & (5)(c) of RICA; Para 6.5 of Chapter 6 of this study.
[426] Section 16(2) (e) & (5)(c) of RICA; Para 6.5 of Chapter 6 of this study.
[427] Sections 23(10) and 26 (3) of RICA; Para 2.3.3.7 of this chapter.
[428] Sections 23 (10) and 26 (3) of RICA; Para 2.3.3.7 of this chapter.
[429] Sections 16(6)(d), 17(1), 20(3)(a) and (b), (4), (5) and (6) and 21(5)(e) of RICA.
[430] Section 20(3)(a) and (b), (4), (5) and (6) of RICA.
[431] Section 17(1) of RICA.
[432] Section 15(2) and 16(6)(d) of RICA.
[433] Paras 2.7 and 6.12 of this study.
[434] Para 5.4.5 of Chapter 5.

It is expected that the court considers or compels the application of this principle as one of the conditions in the direction to conduct an OCI which compels a LEO to discontinue the conduct of an OCI once leading or first facts are gathered to switch over to a less intrusive method and accordingly continue with the investigation. This concept which this study titles as 'first fact factor' ('FFF') seeks to strike a balance in the conflict between the protection of online communication and conduct of an OCI.

In the alternative where the court might omit or fail to include the foregoing condition, a LEO would, in advance, be expected, in good faith under oath as a routine practice, rely on or act upon and report this first set of facts to the court to reasonably switch over to a less intrusive method of investigation instead of continuing with the conduct of an OCI. Because an OCI is an alternative method of investigation, the switching over from an OCI to non-OCI is done after a period of the conduct of OCI, whereas the former method is earlier in the stipulated deadline in the OCI direction issued by the court. The reliance on the ''FFF' is the basis upon which further investigation in a non-OCI procedure is conducted or continued upon which an OCI can be reviewed[435] which further justifies the consideration of the 'interception duration proportionality' principle.

In the reviewed Cybercrime Bill 2018–Amendments Proposed to Bill B6-2017,[436] Online Communication Service Providers are expected to conduct an OCI within 'five ordinary working court days', though an extension of time for the same period is provided for in the Cybercrime Bill-Amendments Proposed to Bill B6-2017.[437]

In the U.S., despite the refusal by the service provider to allow LEAs have access to online communication, a month was used by LEAs to decode a 'WhatsApp' communication in the investigation of a murder case without any assistance from the service provider.[438] In a bomb

[435] Section 20(3), (4), (5) and (6) of RICA.
[436] The CCB B6- 2017. It is noted that CCB was first published in 2015 (CCB-2015) and replaced by the 2017 edition which has not been enacted as at the time of the submission for examination of this thesis. It is however replaced with the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017.
[437] Section 20(3)(a) & (b)(i) & (ii) and (7)(a) of CCB 2017 is replaced with sections 21(3) (a) &(b)(i) & (ii) and (7)(a) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[438] Glover S 'Facebook's refusal to help police on murder case proves it is morally callous' http://www.dailymail.co.uk/debate/article-6132479/STEPHEN-GLOVER-Facebooks-refusal-help-police-murder-case-proves-morally-callous.html (Date of use: 5 September 2018).

investigation, the U.S. Marshals Service reduced the forty-two-day conduct of an OCI to *two days*.[439]

In the U.S., the duration of the use of GPS monitoring has not been agreed by the court.[440] On the one hand, in *US v Jones*, 28 days was spent in tracking Jones with the use of a GPS tracking device installed under his car.[441] On the other hand, tracking an individual for four months is a constitutional breach, which is unacceptable.[442] Generally, long-term monitoring is a serious issue, unlike short term monitoring.[443]

In summary, based on the practice in the RSA —supported by the practice in the U.S., which though is not consistent— three months initial duration for the conduct of an OCI[444] is not a reasonable and rational standard duration for the general conduct of an OCI in the RSA. This is because it has been established above that an OCI can be conducted faster or quicker with an absolute, comprehensive and intrusive outcome. Therefore, the **'**interception duration proportionality' principle, as is propounded in this study, is drawn on the already established practical duration of investigation threshold in the RSA, which is an average of *three days* duration of investigation[445] based on the procedural condition required to conduct an OCI[446] of 'general serious offences'.

2.5.3 Conclusion

Therefore, the general nature and features of the theory of any type or form of OCI derived from the broad concept of interception, monitoring and surveillance are conducted through a wired or wireless non-compartmentalised, non-passworded compartmentalised, interoperable

[439] Landau *Lawful electronic surveillance in the face of new technologies* 218.
[440] Thompson *GPS monitoring* 251 and 255.
[441] Thompson *GPS monitoring* 248.
[442] Thompson *GPS monitoring* 255; Crump *Geolocational Privacy and Surveillance Act* 278.
[443] Thompson *GPS monitoring* 249 and 254.
[444] Sections 16 (6), 17(1), 20(4), (5), (6) and 21(5)(e) of RICA.
[445] NIA 'Investigations on Mr. Macozoma' 13 and 20; *State v Terrence Brown* supra 6 and 8; *Beheersmaatschappij Helling I NV and Others v Magistrate, Cape Town and Others* 2007 (1) SACR 99(C) para 101 (*Helling v Mag*); Swart H 'Secret state: How the government spies on you' https://mg.co.za/article/2011-10-14-secret-state/ (Date of use: 12 December 2016)(Swart https://mg.co.za/article/2011-10-14-secret-state/ (Date of use: 12 December 2016).
[446] Section 16(2)(d)(ii) and (e) and (5)(b) and (c) of RICA.

and conscriptive online communication network[447] including Bluetooth technology.[448]The conduct of an OCI of offline and online serious offences in content and non-content data, real-time and archived communication and Internet and non-Internet based platforms is relatively faster, more complex, exponential, delicate,[449] ubiquitous,[450] absolute, comprehensive and intrusive[451] than the conduct of an investigation in non-online communication channels, platforms or circumstances.[452] Therefore, an element of transparency should be introduced to the conduct of an OCI.[453]

2.6 CONDUCT OF ONLINE CRIMINAL INVESTIGATION IN CONTENT AND NON-CONTENT DATA

2.6.1 Conduct of online criminal investigation of content data

The conduct by LEAs of an OCI of content data exposes the entire data of a user of online communication to great risks, the effects of which are diverse according to the nature and features of the type of content data that an OCI is being conducted in.

According to the International Telecommunication Union, data is treated differently according to the nature and features of its risk in online communication.[454] In one of the features of offline communication, Berkowitz states that the nature of content data[455] is such that it is equivalent to a letter sealed in an envelope sent through the post office, the infringement of which is intrusive if opened and read.[456] This is because content data may generally have enclosed in it the most confidential data, which an individual has the power to keep away from everybody,

---

[447] Watney *Cybercrime and investigation* at 334; Van der Merwe *Telecommunication law* 13- 21.
[448] *State v Terrence Brown* para 6. Bluetooth technology operates in a network that does not have an online agent as a service provider. Although an OCI can be conducted in a Bluetooth technology, however, it is noted that the scope of this study excludes the conduct of an OCI in Bluetooth technology network, which is arguably sufficient to constitute another LL. D study.
[449] Caproni *Lawful electronic surveillance* 212.
[450] Thornton *Telecommunications law* 25-26
[451] Sections 1, 12, 13, 14, 15, 17, 18 and 19 of RICA.
[452] See paras 3.5.7.1 – 3.5.7.15 of the attached Table of Contents where 13 criteria are developed to establish the higher levels of risks in privacy protection in online communication than in a non-online communication.
[453] Hunter and Smith 36 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).
[454] ITU 'Interception of Communications: Model Policy Guidelines and Legislative Text' (2012) 12.
[455] Content data includes voice and non-voice contents, see the term 'indirect communication' in section 1 of RICA.
[456] Berkowitz 2002 7 *Computer Law Review and Technology Journal* 2-8; Watney *Cybercrime and investigation* 340.

such as a will, details of an invention or trade secret, among other things.[457] It is reasonable to conclude that content data usually and relatively enjoys a deep or core secrecy level and value.

2.6.2 Conduct of online criminal investigation of non-content data

An OCI is conducted in non-content data, the effects of which are diverse according to the nature and features of the type of non-content online data that an OCI is being conducted in. Although there is no uniform definition of non-content data,[458] however, it consists of meta and traffic data in online communication.[459]

The conduct of an OCI in non-content online data does not relatively disclose as much information as that of content data, thus, it is reasonable to state that the interpretation of non-content data may not be conclusive. Non-content online data, such as traffic data, is likened to the address and route of online communication, as opposed to the content of online communication.

---

[457] Berkowitz 2002 7 *Computer Law Review and Technology Journal* 2-8; Watney *Cybercrime and investigation* 340. See the definition of the term 'content' in section 1 of RICA. The terms 'purports' and 'means' highlight the subjective nature of what an individual considers to be reasonably private to him that he has the power, competence and self-determinism to choose what he excludes from the public or publicity. Section 1 of RICA; Watney *Cybercrime and investigation* 340.

[458] Gratton E *Internet and wireless privacy - A legal guide to global business practices* (2003) 7-12 (Gratton *Internet and wireless privacy*); See the latter part of the definition of the term 'communication-related information' in s 1 of RICA; Geomans C and Dumortier J 'Enforcement Issues - Mandatory Retention of Traffic Data in the EU: Possible Impact on Privacy and Online Anonymity' in C Nicoll et al (eds) *Digital Anonymity and the Law: Tensions and Dimensions* (2003) 162-172 (Geomans and Dumortier *Traffic Data: Privacy and Online Anonymity*); Edwards L and Howells G 'Anonymity, Consumers and the Internet: Where Everyone Knows You're a Dog' in Nicoll C et al (eds.) *Digital Anonymity and the Law: Tensions and Dimensions* (2003) 216-217 and 222 - 224 (Edwards and Howells 'Anonymity, Consumers and the Internet'); Watney *Cybercrime and investigation* 340.

[459] Gratton *Internet and wireless privacy*' 7 -12. See the latter part of the definition of the term 'communication-related information' in section 1 of RICA No 70 of 2002. See also Geomans and Dumortier *Traffic Data: Privacy and Online Anonymity* 162-172; Edwards and Howells 'Anonymity, Consumers and the Internet' 216-217 and 222-224; Watney *Cybercrime and investigation* 340. Berkowitz 2002 7 *Computer Law Review and Technology Journal* 2-8; Larsson *Telecom operator's incident investigations* 234-235; Currie I and De Waal J *The Bill of Rights Handbook* 6 ed. (2013) 295 (Currie and De Waal *Bill of rights*); Volonino L 'Electronic Evidence and Computer Forensics' 2003 12 *Communications of the Association for Information Systems* 459; Whitcomb C M 'A Historical Perspective of the Digital Evidence: A Forensic Scientist's View' (2002) 1 *International Journal of Digital Evidence* 1-4; Basdeo 2012 2 *SACJ* 198. See generally the provisions of POPIA; Snail and Papadoulos *Privacy and data protection* 275; Section 1 of the ECTA; Section 1(t) of the ECTA Amendment Bill [B-2012]; Section 1 of the ECA; Ncube C B 'Watching the Watcher: Recent Developments in Privacy Regulation and Cyber-surveillance in South Africa' 2006 13 *SCRIPT-ed* 349; Weber R H 'Internet of things-Need for a new legal environment?' 2009 25 *Computer Law & Security Report* 522-527 (Weber 2009 25 *Computer Law & Security Report*); Weber R H and Weber R *Internet of things – Legal perspectives* (2010) 1 (Weber and Weber '*Internet of things-Legal perspectives*); Roos 2012 129 *SALJ* 382-383.

Other general examples of non-content online data include records showing the numbers dialled in online communication, origin of calls or communications made, signal, location, destination, route, switch, date, duration, termination and size of online communication, type of service carried out, type of equipment used or other records indicating the activities of a user in non-content data communications.[460] In these examples, it is submitted that the interpretation of the fact gathered from the activity in non-content online data may relatively be inconclusive in some circumstances, subject to the type of issue that is being investigated.

Similarly, although an OCI may be conducted in a non-content data, which indicates a visit to a criminal defence lawyer, AIDS treatment centre, psychiatrist, strip club, plastic surgeon, gay bar, abortion clinic, etc., however, one can only express an insignificant or non-conclusive opinion in these instances, should an individual be investigated for an offence which may have a bearing in the foregoing instances.'[461]

Non-content data can be classified into four main categories namely: geographic-traffic data,[462] status or metadata, technical-traffic data and socio-economic traffic data.

2.6.2.1 Conduct of online criminal investigation of geographic traffic data or geo-locus data

An OCI is conducted in traffic data, the effects of which, amongst others, indicate or reveal the physical location, positioning or movement of an individual, object or substance in an online communication network.[463] Examples of geographic traffic data include, *inter alia*: a) smart interaction systems such as GPS[464] and Google Maps Street View;[465] b) a software application in a mobile cellular telephone indicating where a picture was taken or where other transactions

[460] Id.
[461] Crump *Geolocational Privacy and Surveillance Act* 278 - 279.
[462] ITU 'Interception of Communications: Model Policy Guidelines and Legislative Text' (2012) 11. Articles 2(b) & (c), 5, 6, 7, 8 & 9 of Directive 2002/58/EC of the European Parliament and of the Council on Privacy an Electronic Communications of 12 July 2002 ('Directive 2002/58/EC'). Article 1(d) of CoE CoCC.
[463] ITU 'Interception of Communications: Model Policy Guidelines and Legislative Text' (2012) 11. Articles 2(b) & (c), 5, 6, 7, 8 & 9 of Directive 2002/58/EC of the European Parliament and of the Council on Privacy an Electronic Communications of 12 July 2002 ('Directive 2002/58/EC'). Article 1(d) of CoE CoCC.
[464] Gratton *Internet and wireless privacy* 29-36 and 299 -305; Roos 2012 129 *SALJ* 390; Thompson S A and Warzel C 'How to Track President Trump' https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html (Date of use: 12 January 2018).
[465] Snail and Papadoulos *Privacy and data protection* 275.

took place; and c) a vehicular tracker, which gives feedback to a mobile cellular telephone about the location of a vehicle.

The increasing collection of location information,[466] which is 'pervasively, silently, and cheaply' conducted is contentious and worrisome.[467] The use of a mobile cellular telephone supplies invaluable 'past and present' locational information about a user.[468] This is because it takes every seven seconds for a mobile cellular telephone to be registered on the next available network,[469] thus, the continuous registration on the next network —subject to 'the size of the coverage area of each cell tower'— strongly and steadily indicates the precision with which a user of a mobile cellular telephone can be monitored.[470] In finding an easy and best resolution to this contention, it is arguably imperative to build systems that do not, in the first place, automatically collate or collect data, which '...is a reasonable objective that can be achieved with modern cryptographic techniques'.[471]

Considering the decision of a foreign court on the conduct of an OCI in a GPS in *Malone v the United Kingdom*,[472] it was held that GPS device generates precise and enormous data about an individual to the extent of recording and reconstructing an individual's movement to every second and to a particular building or position in a building.[473]

Additionally, the installation of a GPS, which is an invaluable method of crime investigation,[474] was used to track the car of a suspect in the U.S., the application of which was described as an efficient, precise and powerful method of investigation because of its costs saving benefits.[475] The efficiency, preciseness, invaluability and cost-effectiveness of the use of a GPS to conduct an OCI —which are supposed to be a blessing in conducting an investigation— are

[466] Blumberg and Eckersley *Locational privacy* 314 and 316.
[467] Blumberg and Eckersley *Locational privacy* 315.
[468] Crump *Geolocational Privacy and Surveillance Act* 274.
[469] Crump *Geolocational Privacy and Surveillance Act* 274.
[470] Crump *Geolocational Privacy and Surveillance Act* 275.
[471] Blumberg and Eckersley *Locational privacy* 316.
[472] *Malone v United Kingdom* 8691/79 [1984] ECHR 10 (2 August 1984) 7 EHRR 14, (1985) 7 EHRR 14, [1984] ECHR 10 URL: *http://www.bailii.org/eu/cases/ECHR/1984/10.html* (Date of use: August 7 2015).
[473] Rosen at 1 http://www.newrepublic.com/article/118396/supreme-court-cellphone-case-went-further-privacy-advocates-hoped (Date of use: 30 June 2017); Swire and Ahmad (eds.) *Part 5: Locational tracking* 245.
[474] Rosen at 1 http://www.newrepublic.com/article/118396/supreme-court-cellphone-case-went-further-privacy-advocates-hoped (Date of use: 30 June 2017; Swire and Ahmad (eds.) *Part 5: Locational tracking* 245.
[475] *U.S. v Jones* see Thompson *GPS monitoring* 250 and 258; Swire and Ahmad (eds.) *Part 5: Locational Tracking* 246; Crump *Geolocational Privacy and Surveillance Act* 273 and 280; Wood *Prison without walls* 305.

unjustifiably and indiscriminately used by LEAs in the RSA who rely on the application of section 205 of the CPA as a short-cut to section 16 of the RICA.

The latter section requires the fulfilment of more conditions before conducting an OCI.[476] In the U.S. case of *U.S. v Jones*, the court held that a warrant must be obtained before the use of a GPS device to track vehicles of suspects, though the decision does not refer to the tracking of human beings via GPS device.[477] However, it is submitted that the effect of non-compliance with section 16 of RICA may be diminished or moribund where government —as part of the State function— permanently installs CCTV cameras in general public areas to the extent of monitoring only the geographic movement of people or object.[478]

2.6.2.2 Conduct of online criminal investigation of meta or status data

An OCI is conducted in an online meta or status data, which entails or reveals the non-content or non-verbal expression of the state of affairs, standing, condition or process of things or persons in an online communication network. The online status or metadata, which, in some respect, is like geographic traffic data, is synonymous with the o-tag[479] system that is attached to a vehicular o-toll payment system, vehicular and pedestrian non-payment o-access card system, household o-monitoring system (or *Internet* of *things*) and similar devices. The conduct of an OCI in all these instances relatively breaches the right in an online communication at a different continuum of secrecy of online communication interests.[480]

Another example of status or metadata includes a tracker or monitoring device which is used for the safety, security and functionality of a vehicle battery or other devices in a vehicle, which a geographic traffic data system may not have the capability to perform. The intrusion into this type of metadata may not be too grievous. This is because a battery tracker focuses more on

[476] This study submits that the use of a GPS under section 205 of the CPA by the OPP to locate the movement of some individuals around the property of the family of Gupta who are accused of State Capture seems unjustifiable. This is because section 205 of CPA does not comply with the full requirements of the provisions of RICA, particularly section 16, see para 6.12 of Chapter 6 of this study.

[477] *US v Jones*, 132 S. Ct 945 (2012); Swire and Ahmad *Introduction* 9-10; Swire and Ahmad (eds.) *Part 5: Locational tracking* 245 -247.

[478] See para 2.6.2.1 of this chapter.

[479] This study adopts the term 'online' communication, which seems more appropriate to describe the specific type of communication which distinguishes it from the broad terminology of electronic communication, which comprises both offline electronic and online communications. Because the scope of this study is limited to online network communication, it seems more appropriate to adopt the term '*online*' or '*o*'.

[480] Para 3.8 of Chapter 3 of this study.

battery safety, security and functionality, which may not have an impact or direct impact on the privacy of an individual.

Also included in meta or status data is an imbedded o-medical chip or tag or monitoring system which conducts a routine or periodic medical check-up in the body of an individual where there is a medical condition or abnormality of any nature which is programmed into the system for medical attention where such condition or abnormality exists.[481] The conduct of an OCI in this type of data is greatly intrusive which can be placed on the same level with the innermost sanctum of online communication[482] if the legality does not even fall under the category of a polygraph test, which has been held not to be a conclusive form of testing the oral evidence of an individual.[483]

In summary, it is generally suggested that metadata should not be automatically stored by LEAs.[484]

2.6.2.3 Conduct of online criminal investigation of technical-traffic data

As previously mentioned,[485] an OCI is conducted in technical-traffic data, the effects of which indicate dialled numbers, the origin of calls or communications made, signal, location, destination, route, switch, date, duration, termination or size of the communications, type of service carried out, type of equipment used or other records indicating the activities of a user in online communication.[486]

It is submitted that the technical-traffic data also includes the data involved in the technical operation by Online Communication Service Providers, which include the services carried out by ethical hackers who are by law permitted to test the efficacy of the integrity and security

---

[481] Savini L 'Human microchipping is here and it's about to rock your skin's world' https://www.allure.com/story/rfdi-microchip-implant-in-skin (Date of use: 12 December 2018).
[482] See para 3.8.1 of Chapter 3 of this study.
[483] *FAWU obo Kapesi and 31 others v Premier Foods Limited t/a Blue Ribbon Salt River & Another* (2010) Case NO: C640-07 paras 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54 and 55 (*FAWU v Premier Foods*).
[484] Right2Know 34 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).
[485] See para 2.6.2 of this study where the examples are generally mentioned in the introduction of non-content data.
[486] Para 2.6.2 of this chapter.

system of an online communication network by hacking into the system developed by an organisation without a court direction.[487]

At the end of the hacking session, a report is expected to be submitted to the organisation or principal who authorised the test for a proper policy decision. However, there is no express regime for report mechanism. Worse still, ethical hackers are exonerated from criminal responsibility if it is established that an ethical hacker has committed a crime in the course of the performance of his or her task.[488]

2.6.2.4 Conduct of online criminal investigation of socio-economic traffic data

An OCI is conducted in socio-economic, 'social graph' or 'mapping' traffic data, which is a form of mass surveillance or profiling that is increasingly applied in the socio, economic, business or market space. [489] An investigation is conducted in this type of data, which relates to the information that is made available in an online communication form or refers to information which means, purports to mean or indicate the social interactions; marketing, economic and business preferences; and moral and cultural beliefs and purposes of users.[490] This type of data is the same or similar to the description of the economic perspective of conscription and non-criminal online conscription.[491]

Other instances where an OCI is conducted in socio-economic traffic data include an investigation on: 'searches on your PDA for services and businesses near your current location'; 'services telling you when your friends are nearby'; 'Free Wi-Fi with ads for businesses near the network access point you are using'; 'parking meters you can call to add money to, and which send you a text message when your time is running out'. These systems not only pose a dramatic threat to locational privacy[492] for socio-economic benefits by

[487] Sections 10 and 11 of RICA.
[488] Section 49(2)(b) of RICA.
[489] ITU 'Interception of Communications: Model Policy Guidelines and Legislative Text' (2012) 11. Articles 2(b) & (c), 5, 6, 7, 8 & 9 of Directive 2002/58/EC of the European Parliament and of the Council on Privacy an Electronic Communications of 12 July 2002 ('Directive 2002/58/EC'). Article 1(d) of CoE CoCC; Swire and Ahmad *Going dark v Golden age for surveillance* 239; Gratton *Internet and wireless privacy* 11-12.
[490] ITU 'Interception of Communications: Model Policy Guidelines and Legislative Text' (2012) 11. Articles 2(b) & (c), 5, 6, 7, 8 & 9 of Directive 2002/58/EC; Article 1(d) of CoE CoCC.
[491] Para 2.3.3 of this chapter.
[492] Blumberg and Eckersley *Locational privacy* 314.

marketing companies but monitor the socio-economic lifestyle of an individual which enables marketing companies to predict the lifestyle of an individual.

2.7 CONDUCT OF ONLINE CRIMINAL INVESTIGATION IN REAL-TIME AND ARCHIVED COMMUNICATION

2.7.1 Comparison of risk level in real-time and archived communication

The comparison of risk level in the conduct of an OCI in real-time or live and archived or stored communications is complex, dynamic and controversial. Attempts by the government to make a distinction between these forms of communication seem 'meaningless'.[493] While the government argues that real-time communication deserves a higher level of privacy than archived communication, the breach of the latter is no less important than the former simply because archived communication is stored.[494]

This is because what LEAs would then do is to ensure that a usual real-time GPS communication which should be accorded prime risk importance, attention and protection would then be delayed so that it is recorded as an archived 'historical' GPS to reduce the higher level of risks and protection before accessing the records.[495] It is noted that the type of data involved in this instance is a GPS.

Nonetheless, it is submitted that relying on the communication technology protocol perspective, unrecorded real-time voice content communication is given or granted technical priority access to an online communication than recorded real-time voice content communication and archived communication. Since unrecorded real-time voice content communication is quicker to make than recorded real-time voice communication and archived communication, unrecorded real-time voice communication is exposed to greater risks than the recorded real-time voice communication and archived communication.

The higher risks in the former include the known fact that it is more reasonable that an

[493] Crump *Geolocational Privacy and Surveillance Act* 280 - 281.
[494] Crump *Geolocational Privacy and Surveillance Act* 280 - 281.
[495] *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 840 (S.D.Tex. 2010); Crump *Geolocational Privacy and Surveillance Act* 280-281.

unrecorded real-time voice content communication is expected or more probable to be made immediately after the occurrence of an incident before recorded real-time voice communication and archived communication could take place. The unrecorded real-time voice content communication is more likely to be the first point of call to make in a time of crisis or urgency, in terms of the timing of the discovery or gathering of first information by LEAs,[496] thereby exposes unrecorded real-time voice content communication to higher risks than the recorded real-time voice content communication and archived communication.

In other words, the first set of information that is discovered by LEAs once a voice communication is activated can be acted upon without having to wait till the end of the voice communication. This is unlike archived communication, which though has its dedicated channel of communication, the delivery in communication or to the recipient may be delayed because it is not granted technical priority right in online communication.[497] Therefore, it is submitted that the levels of protection attached to these two forms of data should be relatively considered in the context in which they are used or in accordance with the proportionality principle.[498]

2.7.2 Conduct of online criminal investigation of real-time communication

An OCI is conducted in the real-time communication of a user who initiates an oral –voice-communication with another person or persons in live communication.[499] An OCI is capable of being conducted in online communication that is ongoing or spontaneously or simultaneously available to the designated receiver.[500]

An OCI is conducted in the momentary or transitory communication that takes place in the network in real-time voice communication. However, real-time communication also occurs where a caller leaves or drops a message in an automated voicemail service of the device of a

[496] Section 23 of RICA.

[497] Veeraraghavan and Wang "A Comparison of In-Band and Out-of-Band Transport Options for Signaling" *Computer Communications and Networks 2007*, ICCCN 2007 1-7; ISO/IEC 7498-1:1994 "Information technology – Open systems interconnection – Basic reference model: The basic model" at 49; Popoola *Liability of ISPs* 7-8 and 18-19.

[498] See paras 5.3.4, 5.3.6 and 5.4 of Chapter 5 of this study.

[499] Section 1 of RICA.

[500] Section 1 of RICA for the defintion of the terms 'real-time communication-related information' and 'electronic communictaions' and section 1 of the ECTA for the defintion of data message which excludes voice in an automated form; *Jamieson v Sabingo* supra 5; Eiselen *E-Commerce* 147-152.

recipient. Essentially, it is submitted that every communication that is stored in the online communication network must have gone through real-time communication before it is stored.

It is submitted that an OCI may be conducted in real-time *voiceless* communication. For example, an OCI can be conducted in a live communication involving body or sign language or other forms of communication, such as visual communication in Skype communication that does not have a voice impact.

There is no general legal requirement for the automatic or routine recording of real-time content data by a service provider except in pursuance of an interception direction.[501] However, an individual may activate a voicemail facility to record a communication[502] or a recording can occur where a user carries out the task of recording such communications on their devices as may be required under RICA provisions.[503]

2.7.3 Conduct of online criminal investigation of archived communication

An OCI is conducted in archived communication, which entails having access to the recording of unrecorded real-time voice communication and recorded voice communication or storage of non-real-time communications.[504] An archived communication generally enables an individual to initiate or receive communication at his or her convenience, which is automatically stored in the memory of online communication networks and devices.[505] Archived communication can be obtained in all online communication devices.[506]

[501] Sections 17(3), 18(3), 35(1)(d) and (h), (2) and (3) and 36(4) (a) and (b) of RICA.
[502] Eiselen *E-Commerce* 149.
[503] Sections 4, 5, 6 and 8 of RICA.
[504] Section 1 of RICA for the definition of archived communication.
[505] Sections 1, 18(3)(a), 19(3) and 30(1)(b) of RICA.
[506] Sections 1, 18(3)(a), 19(3) and 30(1)(b) of RICA.

2.8 CONDUCT OF ONLINE CRIMINAL INVESTIGATION IN AN INTERNET-BASED PLATFORM

2.8.1 Introduction

An OCI can be conducted in an Internet-based communication system.[507] The investigation relies on independent or interoperable telecommunication technologies whose functions are based on Internet operating systems,[508] devices, technologies, networks, software applications, and services. In any Internet communication system, communication is usually routed through centralised and decentralised[509] cross-border networks, spectrums, signals, protocols and servers, which are spread across the globe.[510]

In an Internet based communication relating to a user who is temporarily or permanently resident in the RSA, two servers are involved in the communication. First, a centralised server is located in the host foreign state —for example, in the U.S. or elsewhere where the U.S. chooses to locate the server.[511] Second, a decentralised server is hosted in the RSA where services are provided to the users in response to the operating, technical, business, ethical and legal needs, norms, standards and risks in the RSA.[512]

In an Internet-based communication, the ITU and ICANN do not grant to one State an exclusive sovereign online communication spectrum, network, protocol or signal to manage and control

---

[507] Popoola *Liability of ISP* 6-10.

[508] See ISO/IEC 7498-1:1994, "Information technology–Open systems interconnection–Basic reference model: The basic model" at 32, 33, 35, 37, 41, 46 and 49; Newton *Newtons' Telecom dictionary* 785; Reed C *Internet law: Text and materials* 2nd ed. (2004) 106 (2004) (Reed *Internet law: Text and materials*); Downing D A, Covington M A and Covington M M *Dictionary of Computer and Internet Terms* (2000) 12, 120–121 (Downing, Covington and Covington *Dictionary of Computer and Internet terms*); Lee L C and Davidson J S *Intellectual Property for the Internet* (1997) 21 (Lee and Davidson *Intellectual Property for the Internet*); Dean T *Network+ Guide to networks* (2000) 4, 38, 40, 41- 42 and 43 (Dean *Network + Guide to networks*).

[509] Modern day technologies rely on 'borderless and decentralised technologies', Minnaar A 'Organised crime and the 'New more sophisticated' criminals within the cybercrime environment: How 'Organised' are they in the traditional sense' 2016 29(2) *Acta Criminologica*: *Southern African Journal of Criminology* at123 and 124 (Minnaar 2016 29(2) *Acta Criminologica*: *Southern African Journal of Criminology* at123 and 124); Minnaar A 'The difficulties of implementing cybersecurity measures as a foundational preventive cyberterrorism measure' in Plywaczewki E (ed.) *Current problems of the penal law and criminology* 6th ed. (Bialystok : Temida 2) 585-609; Minnaar A 'Crackers', cyberattacks and cybersecurity vulnerabilities: The difficulties in combating the 'new' cybercriminals' *Acta Criminlogica: Southern African Journal of Criminology, Special Edition 2/2014 : Research and practice in Criminology and Criminal Justice*: 129 - 144.

[510] See CoE CoCC generally.

[511] Para 2.8.3.3 of Chapter 2 of this study.

[512] Para 2.8.3 of this chapter on the examination of the justification for 'no server, but law' principle which speaks in favour of this study.

the global online network but grant equal or coordinate rights, powers and mandates to the international community for cross-border connectivity and operability purposes.[513] To further clarify the confusion on the monopoly of Internet-based communication, arguments are canvassed for the opposing principles of 'no server, no law' on the one hand and 'no server, but law' on the other hand below.

2.8.2 The argument in favour of 'no server, no law' principle

In the Internet technology-based investigation under the principle of '*no server, no law*', the U.S. authorities strongly believe that they are entitled to the absolute control and management of the Internet.[514] Their management of the Internet includes the exclusive reservation of the right, power, and mandate to grant consent to LEAs from other states[515] —including the RSA— before an OCI is conducted relating to offences committed in the RSA, which the RSA has sovereign mandate to investigate.[516] This belief is based on the invention of 'an unplanned and disjointed sequence of events' by the U.S. authorities.[517] It is also their position that servers owned by U.S. entities are hosted in the U.S.[518] as well as outside the U.S. under the control and management of U.S. authorities or entities[519] —including where cloud computing is involved.[520]

The belief by the U.S. authorities is that their right to grant consent extends to the domestic Internet communication within the RSA, given that every Internet storage communication technically goes to the servers in the U.S. before it is communicated to the user in the RSA.[521]

---

[513] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* at 43.

[514] Cajani F 'Technologies and business vs law- Cloud computing, data access and data retention: A legal perspective from the state which is conducting an investigation' 8 https://rm.coe.int/09000016802f241b (Date of use: 21 March 2016 (Cajani https://rm.coe.int/09000016802f241b (Date of use: 21 March 2016). The control by the U.S. authorities include the Internet Corporation for Assigned Names and Numbers (ICANN), Blackman and Srivastava (eds.) *Telecommunication regulation handbook* 222.

[515] Cajani 8 https://rm.coe.int/09000016802f241b (Date of use: 21 March 2016).

[516] Cajani 8 https://rm.coe.int/09000016802f241b ((Date of use: 3 June 2016).

[517] Cajani F 'Interception of communications: Skype, Google, Yahoo! and Microsoft tools and electronic data retention on foreign servers: a legal perspective from a prosecutor conducting an investigation' http://journals.sas.ac.uk/deeslr/article/view/1884 (Date of use: 21 March 2016 (Cajani http://journals.sas.ac.uk/deeslr/article/view/1884 (Date of use: 21 March 2016); Cajani 9 https://rm.coe.int/09000016802f241b (Date of use: 3 June 2016).

[518] Blackman and Srivastava (eds.) *Telecommunication regulation handbook* 222.

[519] Cajani http://journals.sas.ac.uk/deeslr/article/view/1884 (Date of use: 21 March 2016); Cajani 9 https://rm.coe.int/09000016802f241b (Date of use: 3 June 2016).

[520] Lindberg A and Svensson D 'IT Law from a Practitioner's Perspective' in Wahlgren P (ed.) *Information and Communication Technology-Legal Issues* Vol. 56(2010) 12 - 23.

[521] Para 155 of the Applicants' Affidavit in *AmaBhungane v Minister of Justice* supra.

Essentially, the U.S. authorities claim they are entitled to the just and legal —and not equitable— right to manage and control their servers to protect the online secrecy of the U.S. populace and have 'effective control over a defined area'.[522]

Despite that there is no litigation —as a relevant unequivocal proof— on the damage or allegation of (actual or potential) risk of damage to the network of the U.S. server[523] by the ordinary use of the Internet server for OCI purposes by LEAs in the RSA, some authors still believe that non-compliance with the 'no server, no law' principle is an everyday breach of the territorial integrity of the U.S.[524] under the strict interpretation of international law.[525]Arguably, the U.S. principle is fallaciously premised on a physical principle under the assumption that where a State official accidentally crosses a border, such official violates the sovereignty of the other State into which the official crosses, even if such official is unaware of the cross border trespass.[526]

The rationale in favour of the U.S. principle is further sourced from other assumptions and jurisprudence in other jurisdictions as shown below.

Firstly, although the exclusive legal right to Internet patent by the U.S. has expired, it still has inherent equitable protection of Internet patent right[527] including the encryption of specific Internet server that the U.S. deploys to its users —such as Gmail, Skype and other VoIPs. Accordingly, the equitable right makes it difficult for unauthorised persons or authority such

[522] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 66.

[523] Osula A *Remote search and seizure of extraterritorial data* (PhD thesis Estonia 2017) 35-36 (Osula *Remote search and seizure of extraterritorial data*); Von Heinegg W H 'Territorial sovereignty and neutrality in cyberspace' 2013 89 *Int'l L. Stud.*129 (Von Heinegg 2013 89 *Int'l L. Stud.*); Schmitt M N (ed.), *Tallinn manual on the international law applicable to cyber warfare* (2013) 16.

[524] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 64 and 65 and Osula *Remote search and seizure of extraterritorial data* 35, 36 and 37.

[525] Ryngaert C *Jurisdiction in international law* (2nd ed.) (2015) 34; Osula *Remote search and seizure of extraterritorial data* 35.

[526] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 74.

[527] Lehman B A "Intellectual property and the national information infrastructure: Report of the working group on intellectual property rights" in Perrit Jr H *Law and the information superhighway: Privacy, access, intellectual property, commerce and liability* (1996) 76 (Lehman *Intellectual property and the national and global information infrastructure*); Hance O *Business and law on the Internet* trans. SD Balz (1996) 39-40 (Hance *Business and law on the Internet* (1996); Pistorius T "Formation of Internet contracts: An analysis of the contractual and security issues" 1999 11 *SA Merc. LJ* 282; Gringras C *The laws of the Internet* (1997) 2; Downing, Covington and Covington *Dictionary of Computer and Internet Terms* 243 and Popoola *Liability of ISPs* paras 2.2 and 2.3.

as LEAs in the RSA to have access to an Internet server to enable the U.S. authorities to have control of the security of their servers.[528]

Secondly, since different OCI regimes exist for 'U.S. persons' and 'non-U.S. persons' under FISA,[529] it is presumed that the 'no server, no law' principle is impliedly meant to offer additional Internet protection mechanism for 'U.S. persons'. The protection is done by prohibiting non-U.S. authorities from having access to the data of the 'U.S. persons' who reside outside the US or reside in the U.S. and communicate over the Internet with individuals who are residing outside the U.S. The protection of 'U.S. persons' outside the territory of the U.S. is one of the instances of the exercise of the extraterritoriality of the U.S. authorities in international law.[530] This is also in pursuance of the case of *United States v Verdugo-Urquidez,* which protects within and outside the U.S. the right of U.S. citizens and non-US citizens who have a political affinity with the U.S. as opposed to other persons.[531]

Thirdly, in Europe, concerted efforts are being made to ensure the reciprocal cooperation and respect for judicial decisions taken in respect of an OCI which gives support to the U.S. principle of 'no server, no law' by ensuring the recognition of decisions emanating from the U.S. on the conduct of an OCI and implemented through Interpol platform.[532] This is made possible by the inclusion of a MLA procedural provision in the Council of Europe on

[528] Cajani 5 https://rm.coe.int/09000016802f241b (Date of use: 21 March 2016); Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 23; Swart H 'Communication surveillance by the South African intelligence services' 2016 at 11-13 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use: 13 August 2016) (Swart http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use: 13 August 2016).

[529] Sections 1801(a), (b), (c), (f) & (j), 1803 (a), (b) & (c), 1804, 1844, 1881, 1881A (a), (i)(3) & (c)(2), 1881B (d) & 1881D of Foreign Intelligence Surveillance Act (50 U.S.C.); Jimenez A (ed.) A *Privacy- An overview of federal law governing wiretapping and electronic eavesdropping* (2010) 59 and 64-66 (Jimenez (ed.) *Wiretapping and electronic eavesdropping*).

[530] Georgieva I 'Privacy under Fire-Foreign Surveillance under NSA and the GCHQ' (2015) 110; *Advisory Opinion to the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) ICJ Rep. 2004, 136 para 106 -113.

[531] *United States v Verdugo-Urquidez* 494 U.S. 259 (1990); Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 38.

[532] Council of Europe European Convention on Mutual Assistance in Criminal Matters ETS no. 030 1959 which is pursuance of the Schengen Convention; Directive on the European Investigation Order; Osula *Remote search and seizure of extraterritorial data* 20; United Nations Office on Drugs and Crime 'Comprehensive Study on Cybercrime' (2013) 222 (UNODC *Study on cybercrime* (2013) also adduces to the support both countries involved must obtain a court order.

Convention on Cyber Crime to enforce reciprocity[533] in the absence of an international convention.[534]

Fourthly, since an individual can disguise the source or origin of the geographical location of Internet communication —in Google or Microsoft, for example— it is genuinely difficult, if not impossible for LEAs in the RSA to, on their own, even with 'reasonable effort',[535] locate the Internet server that stores the data of a user. If a LEA is unable to locate an Internet server on their own, the server owners, hosts and actors —such as the U.S. authorities— are the most ethically, equitably or legally qualified authorities to have access to such data by unravelling the geographical source or origin of the server.[536]

Fifthly and finally, from the international law of contract or commercial law point of view, it is submitted that since a server owner or lessor —which does not necessarily have to be a patent owner like the U.S. authorities— allows the use of their server, it is presumed that such owner or lessor has control of the management of the server. The management of the server includes access to the data in the RSA by the lessor —i.e. the U.S. authorities— otherwise, the refusal by the RSA to grant access to the lessor —the U.S. authorities— would be tantamount to an infringement of the right to the cyberspace of the lessor.[537] One of the consequences of a breach is that the RSA will be seen as compromising the technical security of the U.S. server if the latter is not allowed access to the data on its server in the RSA where a commercial agreement exists.

Based on the foregoing argument, it may be posited that essentially, the U.S. authorities are entitled to the legal —and not equitable— right to manage and control their servers to protect the privacy of the U.S. populace and have 'effective control over a defined area' by requiring foreign states —such as the RSA— to seek and obtain consent from the U.S. authorities before the RSA conducts an OCI in the RSA.[538]

---

[533] Art 23 and 25 of Council of Europe 'Chart of Signatures and Ratifications of Treaty 185 - *Convention on Cyber Crime* -Status as at 02/06/2017 (CoE CoCC); Osula *Remote search and seizure of extraterritorial data* 22 and 37.

[534] Art 27, 28 and 29(4) of CoE CoCC; Osula *Remote search and seizure of extraterritorial data* 22.

[535] What constitutes 'reasonable effort', which is both a technical and political question is unsettled in law, Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 74.

[536] Cajani 4 -7 https://rm.coe.int/09000016802f241b (Date of use: 21 March 2016); Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 74.

[537] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 12.

[538] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 66.

2.8.3 The argument in favour of 'no server, but law' principle[539]

2.8.3.1 Introduction

The U.S. principle of '*no server, no law*' contradicts the jurisprudence of the independence of territorial sovereignty of a State established in the *Lotus* case about a century ago[540] and lately, in the U.S. *Playpen* case.[541]

Concerning online communication, the sovereignty principle recognises the independent power and mandate of the RSA to conduct an OCI of serious offences committed in the RSA, subject to international public law obligation regulating universal offences, which other States may investigate in the comity of nations.[542]

It is argued that the U.S. principle on 'no server, no law' principle compromises the cyber territorial sovereignty, integrity and equality of the RSA and the privacy of its citizens. In turn, given the expediency and other reasons for embarking on the use of an OCI, the U.S. principle adversely impacts on the effective conduct of an OCI in the RSA if the U.S. authorities would exercise exclusive right to control and manage access to data of such individuals on an Internet platform[543] where no offence has been committed in the U.S. Therefore, this study will bring the objection to the application of the U.S. principle in conducting an OCI in the RSA. It is on record that there is no published or known judicial precedent or literature by any authority or on behalf of the RSA on the objection of the U.S. principle.

The objection to the U.S. principle of '*no server, no law*' is gaining tremendous global support according to the United Nations survey carried out.[544] The survey reveals that two-thirds of the sixty-nine respondent States regard as impermissible the cession of the right of cross-border

---

[539] ITU 'Interception of Communications: Model Policy Guidelines and Legislative Text' (2012) 12.
[540] *SS Lotus, France v Turkey* 1927 P.C.I.J. (Ser A) No. 10 (decision No. 9) 45 (*Lotus*); Osula *Remote search and seizure of extraterritorial data* 45.
[541] The U.S. court held that the *object of search* is the *computer* which is *located where* the *suspect is* referred to as the '*final destination*' and *not the server from which LEAs* are *conducting their OCI*. *United States v Levin* 15-10271-WGY, 2016 WL 2596010 (D. Mass. 2016) 14; Osula *Remote search and seizure of extraterritorial data* 33.
[542] Art 6 of UNODC 'Model Legislative Provisions Against Organised Crime' 2012 at 25; Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 26.
[543] *Kaunda & others v President of the Republic* Case CCT 23/04 54, 209, 227 and 228b (*Kaunda v President*).
[544] UNODC *Study on cybercrime* (2013) 220-223.

access to data from a domestic state —such as the RSA— to a foreign State where an Internet server is hosted.[545] The objection attempts to permanently remove the influence and control of Internet governance from the U.S. authorities and make Internet governance the 'collective responsibility of a neutral and autonomous international forum', which has met stiff resistance from the U.S. authorities.[546]

In support of this objection are the courts and authorities in Belgium,[547] Canada,[548] France,[549] Ireland[550] and China[551] which hold various views against the U.S. principle. The growing global support by international organisations and States posits that a flexible approach to conducting cross-border OCI requires more concrete norms and conglomeration of the domestic law, treaty,[552] MLA and the European Investigation Order.[553] This support is gathering momentum amongst States on the movement from MLA to mutual recognition on trans-border access.[554]

In objecting to the U.S. principle, this study supports the parallel creation and adoption of '*no server, but law*' principle which states that the U.S. authorities shall not have an exclusive right over the Internet particularly in conducting an OCI[555] of serious offences committed within the

[545] UNODC *Study on cybercrime* (2013) 220-223.
[546] Blackman and Srivastava (eds) *Telecommunication regulation handbook* 222-223.
[547] *Yahoo! Inc* [2015] supra and *Yahoo! Inc* [2013] supra; Osula *Remote search and seizure of extraterritorial data* 25 and 31.
[548] *eBay Canada Ltd v M.N.R.* (2008), 330 D.L.R (4th) 360, 53 B.L.R (4th) 202 (F.C.A) paras 3,17, 48 and 51 (*eBay Canada*).
[549] *UEJF et Licra* c. *Yahoo! Inc. et Yahoo France* supra; *Michaels* https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2281&context=faculty_scholarship (Date of use: 21 March 2016).
[550] *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 13 Mag. 2814 WL 1661004 (S.D.N.Y. 2014) (*Microsoft I*); *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp*., No. 14–2985 (2d Cir. 2016) 2 (*Microsoft II*).
[551] France-Presse A 'China has shut down 13,000 websites since 2015–Xinhua' https://www.rappler.com/technology/news/192173-china-shut-down-websites-since-2015 ((Date of use: 7 May 2018).
[552] Even though art 1 of CoE CoCC does not define 'publicly available' platform (or 'open source') and 'lawful and voluntary consent'', art 32(b) of CoE CoCC provides for the free flow of data (including meta or traffic data from a computer used by an individual) which can be obtained from the server of a Party. For example, the information about the sites visited by an individual is publicly available on the server.
[553] Miettinen S *Criminal Law and Policy in the European Union* (2013) 178; Osula *Remote search and seizure of extraterritorial data* 37.
[554] Miettinen S *Criminal Law and Policy in the European Union* (2013) 178; Osula *Remote search and seizure of extraterritorial data* 37.
[555] *Yahoo! Inc* [2015] supra and *Yahoo! Inc* [2013] supra; *eBay Canada* supra 3, 17, 48 and 51; *UEJF et Licra* c. *Yahoo! Inc. et Yahoo France* supra; *Microsoft II*; *Microsoft I*; Osula *Remote search and seizure of extraterritorial data* 25 and 31; *Michaels R* 'Some Fundamental Jurisdictional Conceptions as applied in Judgment Conventions' 9-10

territory of the RSA or elsewhere under an international public law obligation other than in the U.S. In supporting the '*no server, but law*' principle, this study develops four theories to demystify the U.S. principle as follows.

2.8.3.2 Impact of intellectual property perspective on 'no server, *but* law' *principle*

From the intellectual property perspective; since the Internet was invented in 1962,[556] the claim for patent right in the invention of the Internet by the U.S. authorities is extinct because the U.S. authorities have enjoyed the 20-year patent reign. The multiple and complex intellectual property rights[557] that the U.S. authorities are claiming over the Internet are not exclusive to them.

In contributing to the technical operation of the Internet, Sir Timothy John Berners-Lee, an English engineer, invented the 'world wide web' in 1989,[558] which is a fundamental technical and operational requirement for Internet communications.

The invention or ownership of the Internet does not in any way under intellectual property treaties and U.S. Patent Act grant such rights as proclaimed by the U.S. principle of 'no server, no law', neither does patent law restrict the use, and accessibility of data (i.e. the conduct of an OCI) on the Internet to the State of origin of the patent owner only.[559] Similarly, no law or treaty prohibits the RSA from hoisting, installing, and providing security for its indigenous servers to cater for the needs of the RSA including storage facility, thereby nullifies the U.S. principle.

---

https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2281&context=faculty_scholarship (Date of use: 21 March 2016; Blackman and Srivastava (eds) *Telecommunication regulation handbook* 146 -147. 2016 (Michaels 9-10 https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2281&context=faculty_scholarship (Date of use: 21 March 2016).

[556] Patent filed between1861 – 1994 in the U.S lasted 17 years and 20 years for patent filed after 1995, see art 33 of the Agreement on Trade-Related Aspects of Intellectual Property Rights of 1994 (TRIPS) and Patent Cooperation Treaty and Title 35 of the United States Code.

[557] Blackman and Srivastava (eds) *Telecommunication regulation handbook* 146 -147.

[558] Berners-Lee T J 'World Wide Web Foundation' https://webfoundation.org/about/sir-tim-berners-lee/ (Date of use: 3 June 2016).

[559] Patent filed between1861 – 1994 in the U.S lasted 17 years and 20 years for patent filed after 1995, see art 33 of TRIPS and Patent Cooperation Treaty and Title 35 of the United States Code.

The intellectual property perspective demonstrates that the intellectual property on the Internet is a *res nullius* or public utility or servitude.[560] The Internet is constituted by the international 'interconnection of diverse stores of information',[561] public or common networks, intangible wealth, utilities, assets or resources supplied by the global consumers who store data in their local or domestic servers. The power and usefulness of the Internet is derived from the "openness" of its databases.[562] Arguably, as one of the vested interest groups of public trustees and custodians of online information of the people of the RSA, LEAs have the right, power, and mandate to, in the interest of the public, curb crime by conducting an OCI[563] on the Internet without recourse to the consent requirement of the U.S. authorities. The curbing of crime constitutes a form of 'utility' that is incidental to the right, power and mandate of LEAs in the RSA to conduct an OCI.[564]

In summary, no one country can lay absolute claim to the invention or utility of the technical components of the Internet when it relates to the conduct of an OCI via an Internet-based system.

2.8.3.3 Impact of technology perspective on 'no server, but law' principle

The operations or uses of Internet technology point to the direction that although an Internet server is located in the U.S., the data —be it content or meta or traffic data— that is being saved in the U.S. server is generated and useful in the local environment of the RSA. In Internet communication, a copy of the data generated or terminated in the RSA is retained or located in the decentralised server[565] or cloud-computing server in the online territory of the RSA. Therefore, based on the 'utility' and 'necessity' principles[566] formulated in this study, the data should primarily be used in the public interest of the RSA for purposes of executing its constitutional mandate in conducting an OCI of offences committed in the RSA subject to its obligation under international law without any hindrance of obtaining consent from the U.S. authorities or foreign authority.

[560] *Fometo* case and *Bristol* case; Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 74.
[561] Carr *Tracking is an assault on liberty* 367.
[562] Carr *Tracking is an assault on liberty* 367.
[563] For the constitutional mandate of SAPS to investigate, see s 205(3) of 1996 Constitution.
[564] Arts 14 and 15(3) of CoE CoCC.
[565] Regulation 4.1(a) &(b), 4.7, 7.13 of Schedule C of RICA.
[566] Arts 14 and 15(3) of CoE CoCC.

For example, subject to the international public law obligation regulating universal offences, which mandates other States to investigate an offence in the comity of nations,[567] an OCI is conducted in the RSA: a) where the offence occurs[568] in the RSA and b) where a domestic Internet communication takes place[569] between parties who are physically present in the RSA[570] only. In the alternative, LEAs in the RSA can as well conduct an OCI in the RSA where: a) the offence occurred in the RSA; b) the communication must have originated or have been generated in the RSA[571] or terminated in the RSA,[572] even where it is an incomplete communication -i.e., where it is a missed call.[573]

Using the global technical system or geographical location technology,[574] four technologies or applications, amongst others, directly or indirectly support the possibility of '*no server, but law*' principle. These are geo-location, caching, cloud computing network and proxy technologies.

a. Using geo-location technologies to conduct online criminal investigation in South Africa

An OCI can be conducted in the RSA by relying on the principle derived from geo-location technologies. A GLT or GRT is an application used on the Internet to limit the storage of data or service provision to a decentralised and geographical server location.[575] The location is close

[567] Art 6 of UNODC 'Model Legislative Provisions Against Organised Crime' 2012 at 25; Koops and Goodwin 83 *Tilburg Law School Research Paper* 5/2016 at 26. ++

[568] Art 10 (3) & (4) of the United Nations Convention on the Use of Electronic Communications in International Contracts (UNECOMIC).

[569] Art 19 of CoE CoCC.

[570] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 8.

[571] Section 9 (2)(a) of ITU 'Interception Policy & Legislative Text' (2012).

[572] Section 9 (2)(a) of ITU 'Interception Policy & Legislative Text' (2012).

[573] Paragraph 39 of Section III (Explanatory Notes to Model Legislative Text on Interception of Communication) of ITU 'Interception Policy & Legislative Text' (2012).

[574] Roos *Data Protection* 320.

[575] GLT is an application that limits the network reach to a particular location or excludes the network from a location. One of the benefits of a GLT is that it maximises speed, which is one of the targets of an Internet service provider, *CompuServe, Inc. v. Patterson* 89 F.3d 1257 (6th Cir. 1996) https://www.law.cornell.edu/copyright/cases/89_F3d_1257.htm (Date of use: 14 April 2017); *Zippo Manufacturing v Zippo Dot Com Inc*. 952 F. Supp. 1119 (W.D. Pa. 1997) https://cyber.harvard.edu/property00/jurisdiction/zippoedit.html (Date of use: 14 April 2017), *Panavision International L.P v Toeppen* No. 97-55467 https://caselaw.findlaw.com/us-9th-circuit/1286135.html (Date of use: 14 April 2017; Rosenblatt B 'Principles of Jurisdiction' 5-6 https://cyber.harvard.edu/property99/domain/Betsy.html. (12 June 2016) (Rosenblatt 5-6 https://cyber.harvard.edu/property99/domain/Betsy.html. (Date of use: 12 June 2016); Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 44.

to a user —for example, in the RSA, which constitutes the forum or jurisdiction— without necessarily transferring the data to the U.S. server location to invoke jurisdiction.[576]

The business model of most Online Communication Service Providers —including advert companies— is to technically allow advertisers have access to and target people's 'eyeballs' in particular demography by selling online space to advertisers according to the needs and interests of the demographics.[577]

Whether it is the commission of an offline or online serious offence, any of the following factors or circumstances is or determines the jurisdiction, forum State or location to conduct an OCI where a user of online communication:

i) is physically resident[578] in the RSA despite using a U.S. domain name or e-mail address;[579]

ii) has the closest relationship with the contract[580] benefit;

iii) is 'knowingly contacted or reached out' to by the service provider; [581]

iv) receives 'intentionally directed' communications or services from a service provider[582] — which is meant to reach every Internet user— which goes beyond the geographic location

[576] *CompuServe, Inc. v. Patterson* supra https://www.law.cornell.edu/copyright/cases/89_F3d_1257.htm (Date of use:14 April 2017; *Zippo Manufacturing v Zippo Dot Com Inc* https://cyber.harvard.edu/property00/jurisdiction/zippoedit.html (Date of use:14 April 2017), *Panavision International L.P v Toeppen* https://caselaw.findlaw.com/us-9th-circuit/1286135.html (Date of use: 14 April 2017); Rosenblatt 5-6 https://cyber.harvard.edu/property99/domain/Betsy.html. (Date of use: 12 June 2016); Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 44.

[577] Harper *It's modern trade: Web users get as much as they give* 372.

[578] *Zippo Manufacturing v Zippo Dot Com Inc* supra; *Panavision International L.P v Toeppen* supra; Rosenblatt 5-6 https://cyber.harvard.edu/property99/domain/Betsy.html. (Date of use:12 June 2016).

[579] Art 6 (5) of UNECOMIC.

[580] Art 6(2) of UNECOMIC.

[581] *CompuServe, Inc. v. Patterson* supra, *Zippo Manufacturing v Zippo Dot Com Inc* supra, *Panavision International L.P v Toeppen* supra; Rosenblatt 5-6 https://cyber.harvard.edu/property99/domain/Betsy.html. (Date of use: 12 June 2016; Art 31(3)(e) African Union Convention on Cyber Security and Personal Data Protection ('AUCCSPDA').

[582] *CompuServe, Inc. v. Patterson* supra*; Zippo Manufacturing v Zippo Dot Com Inc* supra, *Panavision International L.P v Toeppen* supra; Rosenblatt 5-6 https://cyber.harvard.edu/property99/domain/Betsy.html. (Date of use:12 June 2016); Art 31(3)(e) African Union Convention on Cyber Security and Personal Data Protection ('AUCCSPDA').

of the Online Communication Service Provider to the other parts of the world to where the user of online communication is located;[583]

v) commercially, more interactively, and purposefully receives Internet services as a 'target audience';[584]

vi) uses as the geographical place or location of the cause of action;[585]

vii) is accurately, precisely and physically located by GPS application,[586] similar to identifying caller location for emergency services.[587]

Where any of the instances above occurs to a user of Internet communication in the RSA, there is no mandate on the part of the LEAs in the RSA to seek for consent from the U.S. or other foreign authorities providing Internet server services before embarking on an OCI on the Internet if a serious offence occurs in the RSA subject to its obligation under international law to conduct an OCI regarding offences committed in other jurisdictions.

To further demonstrate that GLT can be used for a particular forum or location —which though can be accessed in other parts of the world aside from the RSA— is that for example, Google offers its services in six South African languages to the residents of the RSA to, arguably,

---

[583] *Maritz Inc v Cybergold* 947 F. Supp. 1328 (E.D. Mo. 1996) https://law.justia.com/cases/federal/district-courts/FSupp/947/1328/1453704/ (Date of use:14 April 2017); *Inset Systems, Inc. v. Instruction Set, Inc* 937 F. Supp. 161 http://www.internetlibrary.com/pdf/Inset-Systems-Instruction-Set.pdf (Date of use:14 April 2017); *Benusan Restaurant Corp. v. King* 126 F.3d 25 (2d Cir. 1997) https://law.justia.com/cases/federal/appellate-courts/F3/126/25/497864/ (Date of use: 14 April 2017); *Graphic Controls Corp. v. Utah Medical Prods., Inc.* No. 97-1551 https://caselaw.findlaw.com/us-federal-circuit/1139689.html (Date of use: 14 April 2017); *Hearst Corp. v. Goldberger* 1997 U.S. Dist. LEXIS 2065 1997 WL 97097 http://www.internetlibrary.com/pdf/Hearst-Corp-Goldberger-SDNY.pdf (Date of use: 14 April 2018); Rosenblatt 5-6 https://cyber.harvard.edu/property99/domain/Betsy.html. (Date of use: 12 June 2016) *R v Taylor* (1997), 121 C.C.C (3d) 353, 42 C.R.R (2d) 371 (B.C.C.A.), affd [1998] 1 S.C.R. 26, 121 C.C.C. (3d) 353; However, some cases are opposed to the principle that is attempted to be proved, *McDonough v. Fallon McElligott, Inc* 1996 U.S. Dist. Lexis 15139 (S.D. Cal. August 5, 1996); Hubbard, Brauti and Fenton *Wiretapping* 6-20; Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 8.

[584] Spencer A B 'Jurisdiction and the Internet: Returning to traditional Principles to Analyse Networked-Mediated Contracts' 2006 *University of Illinois Law Review* No 1 at 79, 81, 85, 86, 87, 91, 93, 94, 97, 98 and 105 (Spencer 2006 University of Illinois Law Review No 1); *Cybersell, Inc. v. Cybersell, Inc* No. 96-17087 https://caselaw.findlaw.com/us-9th-circuit/1136902.html (Date of use: 14 April 2018); Rosenblatt 7 https://cyber.harvard.edu/property99/domain/Betsy.html. (Date of use: 12 June 2016).

[585] *Calder v Jones* 465 U.S. 783 (1984); Spencer 2006 *University of Illinois Law Review* No 1 71-72, 91, 92, 93 and 94.

[586] Hubbard, Brauti and Fenton *Wiretapping* 4-75.

[587] Blackman and Srivastava (eds) *Telecommunication regulation handbook* 143-145.

recognise the RSA as a forum State in an Internet-based communication. These languages are Afrikaans, IsiXhosa, IsiZulu, Northern Sotho, Sesotho and Setswana.[588]

b. Using caching technology to conduct online criminal investigation in South Africa

An OCI can be conducted in the RSA through a caching server or caching technology which enables an individual to access data from a decentralised or interim memory server located[589] in the RSA once a prior communication had taken place in or from the RSA. After the first communication by an online communication user, the decentralised server keeps a copy of the communication located closer to the user or located outside U.S. authorities[590] such as the RSA. Subsequently, accessing data in or from the RSA does not technically and necessarily have to come from the original or central storage system in the U.S.[591]

Therefore, there is no breach of the principle of territoriality or extraterritoriality against the U.S.[592] by or in the RSA because LEAs in the RSA would be presumed to be accessing data from the decentralised or domestic jurisdictional cyber precinct in the RSA[593] when conducting an OCI in the RSA.

Generally, most member States in Europe engage in the practice of 'no server, but law' principle.[594] In Germany, it is believed that there is no need to go elsewhere to locate a data that is communicated within Germany when conducting an OCI because a mirrored copy in the caching system would have been created in Germany where the suspect accesses the server.[595] Therefore, the RSA is at liberty to adopt the same or similar practice that excludes the U.S. authorities from having the powers to grant consent when the RSA wants to conduct an Internet-based OCI of a serious offence that occurs in the RSA.

---

[588] Google https://www.google.co.za/?gws_rd=ssl (Date of use: 20 May 2017).
[589] UNODC *Study on cybercrime* (2013) 222.
[590] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 45.
[591] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 45; Art 10 (4) of UNECOMIC.
[592] Seitz N 'Trans-border Search: A New Perspective in Law Enforcement' 2004 7 *Yale JL & Tech* 28; Osula *Remote search and seizure of extraterritorial data* 32.
[593] Osula *Remote search and seizure of extraterritorial data* 32.
[594] Osula 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' 366–369; Osula *Remote search and seizure of extraterritorial data* 42.
[595] Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' 369–371; Osula *Remote search and seizure of extraterritorial data* 43; Art 10 (4) of UNECOMIC.

c. Using cloud computing network to conduct online criminal investigation in South Africa

An OCI can be conducted in cloud computing technology which is not a new technology. Any type of online activity or online computer operation can take place in the cloud and the function of a cloud computer is as old as the old mainframe computer in which a user stores data for a short or long period in a server owned by third-parties as to the original record keeper, including an o-mail transaction, which impacts on online privacy.[596]

The scope of cloud computing, which is still debated, range from the Internet to other forms of communications or connections.[597] Cloud computing enables a user, through some software applications, to share, store and conduct other services relating to the personal information of a person on remote servers.[598] These servers are owned or operated by third parties —such as government agencies and private, individual and legal entities— in a 'variety of flavours of private, public, internal, external, free, paid…' transactions similar to a bank transaction.[599]

The services performed by third parties who face diverse challenges in cloud computing include the sharing, storage and monitoring of the transactions of mobile cellular telephone data, general data —including activities or data in home-based desktop— and personal health record and hosting of video and photography websites, tax preparation related sites, social networking platform sites, amongst others.[600]

A foreign jurisdiction opines that it is unclear that the law that protects online privacy also protects cloud computing.[601] This impliedly means that cloud computing is not protected or adequately protected, including the encryption of cloud computing, although such data owner may find solace in European law which protects online data which does not exclude data in cloud computing while other countries are working on reviewing their law in this regard.[602]

[596] Gellman R and Dixon P *Online privacy* (2011) 37-38.
[597] Gellman and Dixon *Online privacy* 37-39.
[598] Gellman and Dixon *Online privacy* 37-39.
[599] Gellman and Dixon *Online privacy* 37-39.
[600] Gellman and Dixon *Online privacy* 38-39.
[601] Gellman and Dixon *Online privacy* 39-40.
[602] Gellman and Dixon *Online privacy* 39-40.

The position that cloud computing is not protected has the risky tendency of striping off the right to privileged data protection in an attorney-client and doctor-patient relationships if the data is shared with a third-party cloud computing vendor' as well as enabling cloud computer vendor to allow access to data by private litigants without notice to the owner of data.[603]

The further risk of non-protection of cloud computing under the general online communication regime is that the same data may not be protected in another country or server where the data is stored.[604] In some cases, some data in cloud computing may be exposed to a foreign enemy or hostile country or entity with equally weak or weaker legal framework or exposed to a foreign hacker who may not be easily tracked down.[605] However, the inadequacy of protection of cloud computing does not extend to a situation under the 'mandated disclosure' clause, which requires LEAs or LEOs to reveal criminal activities such as the whereabouts of fugitives or missing children, breach of copyright and reporting of information already discovered by LEAs or LEOs.[606]

There are two views on the true application of the technicality of cloud computing network in conducting an OCI, which bother on whether a data owner can choose a location of storage of data in cloud computing in consideration of the U.S. principle that requires a foreign country - including the RSA- to seek for and obtain consent before conducting an OCI.

Firstly, according to Koops and Goodwin, it is a weak argument in cloud computing for a foreign State to comply with the consent requirement of the U.S. before conducting an OCI in such a foreign State in instances where the data of a user is likely to be stored in decentralised servers or multi-data centres.[607] This is because servers or centres enable, at very short intervals in a random pattern,[608] technical and 'automatic dynamic data placements' at different physical

[603] Gellman and Dixon *Online privacy* 39.
[604] Gellman and Dixon *Online privacy* 39-40.
[605] Gellman and Dixon *Online privacy* 39-40.
[606] Gellman and Dixon *Online privacy* 40.
[607] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 74 and Osula *Remote search and seizure of extraterritorial data* 33 and 52; In the matter of a warrant to search a certain email account controlled and maintained by Microsoft Corporation, No 14-2985(2d. Cir 2016)2; UNODC *Study on cybercrime* (2013) 217-218; DATASTAX 'Introduction to multi-data center operations with Apache Cassandra and Datastax Enterprise- white paper' October 2013 at 1-11 http://www.datastax.com/wp-content/uploads/2012/09/WP-DataStax-MultiDC.pdf (Date of use: 7 July 2015) (DATASTAX 1-11 http://www.datastax.com/wp-content/uploads/2012/09/WP-DataStax-MultiDC.pdf (Date of use:7 July 2015).
[608] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 66.

locations, and multiple countries or jurisdictions close to the user[609] —including users in the RSA— which is one of the features in cloud computing.[610]

Given that data moves around the globe in cloud computing, it is also difficult to comply with the U.S. principle because the movement of data may also result in the *loss of knowledge of the location of data*, thereby making it difficult to hold the U.S. or any foreign State responsible for the unknown location of data or temporary location of data[611] because data may not be found in, connected to or linked with a particular State.[612] The loss of knowledge of the location of data may also imply that there is an insufficient reason for the determination of the location of the server[613] in the U.S. Invariably, the location of data at a specific server location in the U.S. has become less relevant.[614] Consequently, jurisdiction cannot be determined in favour of the U.S., which claims exclusive jurisdiction to access data on the Internet concerning the conduct of an OCI by foreign countries.

Although some foreign States still rely on the execution of an MLA in which mandate is given to the U.S. to grant consent in OCI before such foreign States conduct an OCI in their respective countries,[615] however, the recent practices show that foreign States may no longer make use of MLA since data may not be fixed in the headquarters of the server State only.[616]

---

[609] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 74 and Osula *Remote search and seizure of extraterritorial data* 33 and 52; In the matter of a warrant to search a certain email account controlled and maintained by Microsoft Corporation, No 14-2985(2d. Cir 2016)2; UNODC *Study on cybercrime* (2013) 217-218; DATASTAX_1-11 http://www.datastax.com/wp-content/uploads/2012/09/WP-DataStax-MultiDC.pdf (Date of use: 7 July 2015).

[610] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 74.

[611] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 66.

[612] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 66.

[613] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 8.

[614] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 28; UNODC *Study on cybercrime* (2013). 217-218; Osula *Remote search and seizure of extraterritorial data* 52.

[615] Art 31(1) of CoE CoCC; UNODC *Study on cybercrime* (2013) 217-218; Osula *Remote search and seizure of extraterritorial data* 52; Council of Europe 'Drafts elements of additional protocol to the Budapest convention on cybercrime regarding transborder access to data' (2013) T-CY (2013) 14; Osula A 'Accessing extraterritorially located data: Options for states' 2015 22-23 https://ccdcoe.org/sites/default/files/multimedia/pdf/Accessing%20extraterritorially%20located%20data%20options%20for%20States_Anna-Maria_Osula.pdf (Date of use: 16 February 2017 (Osula 22-23 https://ccdcoe.org/sites/default/files/multimedia/pdf/Accessing%20extraterritorially%20located%20data%20options%20for%20States_Anna-Maria_Osula.pdf (Date of use:16 February 2017); Osula *Remote search and seizure of extraterritorial data* 52; UNODC *Study on cybercrime* (2013) 217-218.

[616] *Microsoft II* supra 2; UNODC *Study on cybercrime* (2013)217-218; Council of Europe criminal justice access to evidence in the cloud https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680654221 (Date of use: 28 August 2018); Osula A 'Remote search and seizure in domestic criminal procedure: Estonian case study' 353-354; Osula *Remote search and seizure of extraterritorial data* 52.

Secondly, , though contradictory to the first proposition but arguable, it is posited that in cloud computing, there is a possibility or likelihood of identifying the location of the storage of data in cloud computing network by choosing the specific foreign State in which they want their data to be stored.[617] This is because, although agreements do not always indicate that data will be geographically located in one place, however, the service provider undertakes not to locate or relocate data from a country, jurisdiction or region without notification from the user.[618] Consequently, there is no certainty that data will always be located in the U.S. server if a user of online communication has chosen to have his or her data located outside the U.S.

Finally, notwithstanding the above views on whether a data owner can choose a foreign State to locate a data in cloud computing, a fundamental issue is raised with regards to the implementation of the provisions of CoE CoCC in the jurisdictional claim in OCI involving cloud computer network. The issue is; whether a foreign State —for example the U.S.— has a substantive connection with the crime, victim or suspect in the domestic State —RSA— where an investigation is being conducted to trigger jurisdiction in favour of the U.S.?[619]

In response, what is very clear and crucial is that there must be a 'sufficiently strong connection' or 'strong and plausible link' between the data and an investigating State —such as the U.S.— to warrant donating jurisdiction to the U.S., otherwise the RSA is not required in fact and law to seek for consent from the U.S. before conducting an OCI in the RSA.[620] Thus, no logically, reasonably, rationally and justifiably conclusive assumption can be made in favour of the U.S. to conduct an OCI where the data in question does not have 'sufficiently strong connection' or strong and plausible link'[621] to or with the U.S.

d. Using proxy technology to conduct online criminal investigation in South Africa

An OCI can be conducted in the RSA using a proxy technology, which is a technology that uses VPN or anonymous application such as Tor software.[622] Although proxy technology does

[617] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 44-45; UNODC *Study on cybercrime* (2013) 217.
[618] UNODC *Study on cybercrime* (2013) 217.
[619] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 66.
[620] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 66 and 73.
[621] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 66 and 73.
[622] National Rapporteur on Trafficking in Human Beings, 'Child Pornography – First

not disclose the location or IP address of an ostensible user but discloses that of the computer agent which may be located anywhere in the world[623] and held responsible for such communication, including the RSA.

The proxy principle is drawn on the Dutch jurisprudence, which bothers on ubiquity and non-exceptionalist principles.[624] Although subject to compliance with international law,[625] the interpretation[626] of the ubiquity[627] principle states that where an Internet proxy server[628] is employed by a user to —for example, distribute child pornography[629] in the Netherlands— whether or not the perpetrators are Dutch or in Netherland,[630] such computer is presumed to be located in the domestic State of Netherlands and not beyond its borders, unless it is proven otherwise.

Furthermore, failure to presume the location in the Netherlands would lead to the impunity of serious crime commission in the Netherlands.[631] This is because, despite the non-disclosure of the IP address of an Internet user under the proxy principle, the non-exceptionalist principle states that jurisdiction in cyberspace is 'intimately connected' to the originating or

Report of the Dutch National Rapporteur' (2011) 164 –165 http://www1.umn.edu/humanrts/research/Netherlands_child-pornography_report_2011_en.pdf. (Date of use: 12 December 2016).

623 Svanatesson D J B 'How does the accuracy of geo-location technologies affect the world' *Masaryk University Journal of Law and Technology* 2 (2007) 16-19; Kaspersen H W K 'Cybercrime and Internet jurisdiction' discussion paper (draft) 28; Muir J A and Van Oorschot P C 'Internet geo-location and evasion (2006)'; Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 43 and Osula *Remote search and seizure of extraterritorial data* 20.

624 Rijksoverheid 'Memorie van Toelichting Wetsvoorstel Computercriminaliteit III' https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/23/memorie-van-toelichting-wetsvoorstel-computercriminaliteit-iii (Date of use: 3 March 2017) (Rijksoverheid https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/23/memorie-van-toelichting-wetsvoorstel-computercriminaliteit-iii (Date of use: 3 March 2017); Osula *Remote search and seizure of extraterritorial data* 41.

625 Rijksoverheid https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/23/memorie-van-toelichting-wetsvoorstel-computercriminaliteit-iii (Date of use: 3 March 2017; Osula *Remote search and seizure of extraterritorial data* 41.

626 Art 125(j)1 of Dutch Code of Criminal Procedure; Koops B 'Cybercrime legislation in the Netherlands' December 2010 Vol. 14.3 *Electronic Journal of Comparative Law* 18 https://www.ejcl.org/143/art143-10.pdf (Date of use: 28 February 2017; Osula *Remote search and seizure of extraterritorial data* 40.

627 Thornton *Telecommunications law* 25-26

628 Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 43 and Osula *Remote search and seizure of extraterritorial data* 20.

629 See *Botha v State* A163/2014 [2015] ZAFSHC 34 (26 February 2015); *State v Kleinhans* 2014 (2) SACR 575 (WC).

630 National Rapporteur on Trafficking in Human Beings, 'Child pornography – First Report of the Dutch National Rapporteur' (2011) 164–165.

631 Vagias M *The Territorial jurisdiction of the International Criminal Court* (2014) 17-24; Osula *Remote search and seizure of extraterritorial data* 41- 42.

terminating[632] 'material space' or end, which is a physical object, real person or 'any form of data processing activity' in the 'real world'.[633]

It follows therefore that these two principles reiterate that if a computer agent can be located in the RSA via a proxy technology, consequently, an OCI can be conducted in the RSA relating to the commission of a serious offence in the RSA, which does not require any consent from the U.S. authorities.

e. Conclusion

In summary, given that the various technologies or applications examined above suggest that Internet jurisdiction is located in the RSA, it is therefore argued that consent to conduct an OCI on the Internet lies in the LEAs or LEOs in the RSA and not in the U.S. authorities.

2.8.3.4 *Impact of general and specific business and operational compliance perspective on 'no server, but law' principle*

From the general and specific business and operational compliance perspective, the implied offline enquiry by the Constitutional Court in *Kaunda v President*[634] and the international opinion and treaty suggest and posit that a foreign business entity —such as UBER software application which is used by a foreign transport company—[635] must comply with the general and specific business or operational requirements of the host country, which is the RSA in this instance.[636] The need for compliance is based on the fact that the physical object or substance

[632] Art 10 (3) & (4) of UNECOMIC.

[633] The other school of thought (*exceptionalist*) believes that 'cyberspace is a separate space', which is different from the way material space functions and which should be significantly distinguished from the real world, Goldsmith J L 'Against Cyberanarchy' *University of Chicago Law Review* 65 (19981a) 1199-250; Johnson D R and Post D G 'law and Borders-The Rise of Law in Cyberspace' 1996 48 *Stanford Law Review* 1367-402 at 1378; Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 30-31 and 43.

[634] *Kaunda v President* supra 54, 55, 66 and 57.

[635] Mabena S 'Uber operators must apply for operating licences: transport minister' https://www.timeslive.co.za/news/south-africa/2017-07-10-uber-operators-must-apply-for-operating-licences-transport-minister/ (Date of use: 10 July 2017) (Mabena https://www.timeslive.co.za/news/south-africa/2017-07-10-uber-operators-must-apply-for-operating-licences-transport-minister/ (Date of use: 10 July 2017); See Eloff D 'Unscrambling the general data protection regulation' http://www.derebus.org.za/unscrambling-the-general-data-protection-regulation/ (Date of use: accessed 18 January 2019.

[636] *Kaunda v President* supra 45; UNODC *Study on cybercrime* (2013) 217; Osula *Remote search and seizure of extraterritorial data* 52; *Rex v Buchanan* 1914 AD 509-519.

of the operation of UBER is based in the RSA, which is the passenger that patronises the transport system from one physical point to another in the RSA.

Accordingly, it is submitted that any Internet service provider that wants to operate in the RSA to which a user in the RSA wants to enter into a direct or indirect contract of Internet service provision must comply with the general and specific business and operational requirements of the business of Internet service provision in the RSA.[637] Notwithstanding the operational policy of a foreign entity —such as Google whose operations may rely on its centralised server— however, part of the operational compliance by such foreign entity in the RSA will be that it should have a decentralised server located in the RSA for obvious reasons.

One of the purposes requires that an Internet service provider must submit to the jurisdiction of the RSA —and not the U.S. authorities— in terms of the regulation of the criminal justice system, which includes the conduct of an OCI of serious offences committed in the RSA.

The general and specific business and operational perspective posts that the U.S. principle generally contradicts its ratification of and compliance with the enforcement of the CoE CoCC and the recent U.S. District Court decision in *United States v Microsoft Corporation.*[638] In this case, the court held that the U.S. authorities could not rely on the fact that since Microsoft is headquartered in the U.S., it could issue a warrant to access the o-mail content of an Irish national that is exclusively stored on the 'domestic soil' or server in Ireland or where the services are marketed in foreign states outside the U.S.[639] In finally opposing the U.S. principle, similar court decisions have been held in Belgium,[640] Canada,[641] France[642] and Ireland.[643]

[637] See chapters 2 and 3 of ECA.
[638] *Microsoft II* supra 15.
[639] *Microsoft II* supra 15.
[640] *Yahoo! Inc* [2015] supra and *Yahoo! Inc* [2013] supra*;* Osula *Remote search and seizure of extraterritorial data* 25 and 31.
[641] *eBay Canada* supra 3,17, 48 and 51.
[642] *UEJF et Licra* c. *Yahoo! Inc. et Yahoo France* 22 mai 2000 (Tribunal de Grande Instance Paris), 2000 Communication et Commerce Electronique (Comm. Com. Electr. Comm. n°92, note J-Chr. Galloux; Michaels 9-10 https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2281&context=faculty_scholarship (21 March 2016.
[643] *Microsoft II* supra; *Microsoft I* supra.

2.8.3.5 Impact of urgency, expediency or necessity perspective on 'no server, *but* law' *principle*

From the urgency, expediency or necessity (*via necessitatis*) perspective, LEAs in the RSA[644] —including the European states-are moving away from the general practice in the CoE CoCC and MLA regimes and are subscribing to *self-help* when conducting an OCI.[645] The main reason for the movement is attributed to the long response time of an estimated 90-day period of supplying information obtained from an online communication by the State having possession of the data, such as the U.S. in pursuance of their principle of 'no server, no law'.[646] *Self-help* is a coercive form of extraterritoriality, which is permissible if there is an urgent circumstance or where permission for 'hot pursuit' or roaming[647] in OCI cannot be obtained in the U.S.[648] where the server is located. Consequently, it is submitted that the RSA has the mandate to conduct an OCI in a serious offence committed in the RSA where there is an urgency, expediency or necessity to do so.

2.8.3.6 Impact of constitutional supremacy perspective on 'no server, *but* law' *principle*

The RSA generally expresses difficulty in complying with Conventions that expect the RSA to surrender its binding constitutional obligation towards the private communications of its

---

[644] Department of Justice and Constitutional Development 'Mutual Legal Assistance in Criminal Matters Treaty between the Republic of South Africa and the Argentine Republic' and RSA 'Mutual Legal Assistance in Criminal Matters in the Treaty between the United States of America and South Africa' (1999) but entered into force in 2001.

[645] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in Criminal Matters (OJ L 130, 1.5.2014) 12(4); Osula *Remote search and seizure of extraterritorial data* 21and 38; Crawford J *Brownlie Principle of public international law* 8th ed. (2012) 481 (Crawford *International law*).

[646] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 8; Reading art 25(3), 26 & 27 (8) & (9)(a) and 28 of CoE CoCC together, urgent, spontaneous or informal sharing of information gathered by a party for onward transmission (through fax or o-mail) to another party is allowed before a formal application is brought by a requesting party subject to the condition of compliance of confidentiality by the requesting state, see Miller G and Jaffe G 'Trump revealed highly classified information to Russian foreign minister and ambassador' https://www.washingtonpost.com/world/national-security/trump-revealed-highly-classified-information-to-russian-foreign-minister-and-ambassador/2017/05/15/530c172a-3960-11e7-9e48-c4f199710b69_story.html?utm_term=.6c16f1420aae (Date of use: 15 May 2017) and Adam K 'Trump calls for investigation of U.S. leaks in Manchester bombing probe' https://www.washingtonpost.com/world/british-outrage-over-alleged-us-leaks-in-the-manchester-bomb-investigation/2017/05/25/f21349e2-4b0b-4afd-ba06-333621cfa634_story.html?utm_term=.0ad53e0d07ba (Date of use: 25 May 2017); Osula 22-23 https://ccdcoe.org/sites/default/files/multimedia/pdf/Accessing%20extraterritorially%20located%20data%20options%20for%20States_Anna-Maria_Osula.pdf (Date of use:16 February 2017).

[647] Art. 30 (1) of CoE CoCC provides for roaming.

[648] Crawford *International law* 481; Osula *Remote search and seizure of extraterritorial data* 38.

citizens to a foreign State in reciprocity,[649] therefore complying with the U.S. 'no server, no law' principle, which is worse still, not a Convention,[650] is incongruous to the constitutional jurisprudence of the RSA. Even where the RSA has since 2001 been a signatory to the CoE CoCC which is a Convention on cross-border data protection, however, it has not ratified the Convention[651] let alone adopt or apply the U.S. principle which exclusively exposes the citizens of the RSA to greater risks in the U.S.

Worse still, it is ironic that the U.S. has not complied with the basic cross-border data protection reciprocal standards in the globally accepted EUDP Directive[652] and yet the U.S. requires foreign States to surrender their cyber territorial sovereignty to the former via the 'no server, no law' principle, thus, there is no legal nor moral justification for the RSA to comply with the U.S principle of 'no server, no law' but that of the principle of 'no server, but law'. Similarly, Russia has not ratified the CoE CoCC.[653]

In summary, the constitutional law perspective encompasses the reasonable justification for the various components or perspectives of the 'no server, but law' principle canvassed above which seeks to opine that the RSA does not require foreign consent from the U.S. or elsewhere that lays claim to the 'no server, no law' principle before conducting an OCI in the RSA.

2.8.3.7 Conclusion

Arguably, the imposition by the U.S. of the 'no server, no law' principle is tantamount to a state of confusion, double standard, hypocrisy and contradiction. This is because the U.S.

---

[649] Section 72 of POPIA; *Kaunda v President* supra 54, 209 and 227 and 228. Sections 231(2), (3) & (4), 232 and 233 of the Constitution. However, it is submitted that it may not be justifiable in some circumstances to protect the right in an online communication of citizens in the RSA in cases involving war crime, genocide, terrorism and war against humanity or some other universal offences, SC Resolution 1593 taken on 31 March, 2005; Du Plessis M 'International Criminal Courts' 191; Dugard J *International law: A South African perspective* 4th ed. (2013) 156 (Dugard *International law: SA*). Lately, *SAPS v Zim & Dugard* supra 74.

[650] The RSA has not ratified the CoE CoCC on international data protection, despite the fact that the RSA has been a signatory to the CoE CoCC since 2001, see CoE CoCC.

[651] CoE CoCC. Similarly, Russia has not ratified the CoE CoCC, see EDRi 'Transborder data access: Strong critics on plans to extend CoE cybercrime treaty' https://edri.org/edrigramnumber11-11transborder-data-access-cybercrime-treaty/ (Date of use: 12 May 2017) (EDRi https://edri.org/edrigramnumber11-11transborder-data-access-cybercrime-treaty/ (Date of use: 12 May 2017).

[652] Directive 95/46/EC of the European Union Data Protection (EUDP).

[653] EDRi https://edri.org/edrigramnumber11-11transborder-data-access-cybercrime-treaty/ (Date of use: 12 May 2017).

Federal Court, in one breath, assumes or shares offline jurisdiction with foreign jurisdictions in civil matters committed in any part of the world by non-nationals abroad under the Alien Torts Statute of 1789.[654] However, in another vein, the U.S. contradictorily claims the monopoly of jurisdiction to access data in Internet server, thereby excluding the RSA from conducting an OCI on the Internet over the commission of crime in the RSA.

In international law, there is no *stare decisis* rule in the administration of justice.[655] Essentially, international law is dynamic to cater for various circumstances.[656] Cyberlaw jurisprudence expects a change in the U.S. principle of 'no server, no law', which in itself is not an acceptable international principle, but a foreign law,[657] which can be contested if it contravenes international public law. The cyber-world perceives the U.S. principle as being a unilateral principle with its attendant unintended and negative consequences of less-cooperation in a general investigation.[658]

As much as international law is important in telecommunication, the significant role of domestic law cannot be over-emphasised.[659] The States view cyberspace that falls under their physical domain as being part of their territory.[660] According to Koops and Goodwin, State sovereignty or territorial integrity principle cannot be sustained amid the technological assertions if the States do not have some level of control of their cyberspace.[661]

---

[654] *Sosa v Alvarez-Machain* (US Supreme Court) (2004) 43 *ILM* 1390; *Arrest Warrant* case para 48; Dugard *International law: SA* 157.

[655] *Inter-Science Research and Development Services (Pty) v Republica Popular de Mocambique* 1980 (2) SA 111 (T) paras 119B-C, 120 and 125G-H; Dugard *International law: SA* 242; Osula *Remote search and seizure of extraterritorial data* 36-37; Art 4 (1) & (2) of TOCC.

[656] *Kaffraria Property v Government of the Republic of Zambia* 1980 (2) SA 709 (E) paras 715B-D; Dugard *International law: SA* 243; Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 20 and 73; Osula *Remote search and seizure of extraterritorial data* 24 and 36.

[657] There is nowhere in the jurisprudence of Internet law in the RSA where U.S. foreign law is recognised or acknowledged as the universal law, see Thornton *Telecommunications law* 19, 20, 28,29, 30-35, 47-48; Mokgosi *The telecommunications regulators* 101 and 107 -108; Yacoob S and Pillay K 'Licensing' in Thornton L et al (eds.) *Telecommunications law in South Africa* (2006) 135-136 and 139 (Yacoob and Pillay *Licensing*); Msimang M 'Universal service and universal access' in 'Thornton L et al (eds) *Telecommunication law in South Africa* (2006)' 219-220, 222 (Msimang *Universal service and universal access*).

[658] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 12.

[659] Thornton *Telecommunications laws* 19, 20, 21; Mokgosi *The telecommunications regulators* 110- 123; Yacoob and Pillay *Licensing* 142-143, 159 and 171.

[660] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 21.

[661] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 590.

Therefore, it is advisable that the U.S. recognises technological dynamism[662] such as the opposing and popular view of 'no server, but law' principle in favour of the RSA and other foreign States that are in the same or similar position with the RSA. Where other States — including the RSA— morally, ethically, equitably, and legally justify that they have relatively 'shared interests' in the 'open skies', oceans and waters,[663] it, suggests that all nations have a stake in the cyberspace including the increasing consensus effort by international organisations in this regard.[664]

For the U.S. authorities to successfully oppose the justification of 'no server, but law' principle, there must be a proof of material damage or harm to the 'virtual presence' of their server,[665] their cyberinfrastructure[666] or the sovereign independence and integrity[667] of the U.S., otherwise, their claim cannot be sustained based on the proof examined above. Moreover, it is possible for the U.S. authorities to create special servers for the data of each country located in the U.S servers, which can easily and only be accessed by the RSA for the purpose of conducting an OCI in the RSA.

Thus, access to data on the Internet for the conduct of OCI purposes should not be exclusively controlled and managed by the U.S. authorities, the service providers in a foreign State,[668] a 'central governing body'[669] controlled by a foreign State or patent or server owner, but must be controlled, and managed by the global public or stakeholders.[670] Therefore, it is proposed

---

[662] Regulatory authorities are advised to be awake to the development of technology to influence their decisions, Blackman and Srivastava (eds.) *Telecommunication regulation handbook* 11.

[663] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 90.

[664] Osula, 'Transborder Access and Territorial Sovereignty' 731–732; Osula *Remote search and seizure of extraterritorial data* 43 and 45- 46.

[665] It is however noted that Internet may be intercepted by LEAs by deleting some data which constitutes public nuisance or immorality, 88ter 3 of Belgium Code of Criminal Procedure; Kaspersen H W K 'Cybercrime and Internet Jurisdiction' (2009) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803042b7 (Date of use:18 February 2017); Osula *Remote search and seizure of extraterritorial data* 35 and 39 and 40; Von Heinegg 2013 89 *Int'l L. Stud.* 109; Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 9 and 61-62.

[666] Von Heinegg W H 'Legal implications of the territorial sovereignty in cyberspace' in Czosseck C, Otis R and Ziolkowski K (eds) 89 (2012) 4th ed. *International Conference on Cyber Conflict* (NATO CCD COE) 11; Osula *Remote search and seizure of extraterritorial data* 36. Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 81.

[667] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 81.

[668] Osula *Remote search and seizure of extraterritorial data* 51 and 60.

[669] Schneider B 'Anonymity and the Internet' https://www.schneier.com/blog/archives/2010/02/anonymity_and_t_3.html (Date of use:4 January 2017; Osula *Remote search and seizure of extraterritorial data* 24.

[670] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 82-83 and Osula *Remote search and seizure of extraterritorial data* 34 and 51.

that primary, secondary and tertiary rights to conduct an OCI of the serious offence will accordingly be ceded to the RSA,[671] the U.S. authorities[672] and other countries respectively based on the 'utility' and 'necessity' principles[673] formulated in this study.

Therefore, based on the points canvassed above, this study supports the principle of 'no server, but law' to ensure a possible balance between the conduct of an OCI and the right to the SOC in the RSA. However, should the determination of online interception jurisdiction on the Internet become unresolved, Mutual Legal Assistance may be resorted to in an attempt to strike a possible balance between the two divides.

2.9 CONDUCT OF ONLINE CRIMINAL INVESTIGATION IN NON-INTERNET BASED PLATFORMS

An OCI can be conducted in a non-Internet-based communication, which occurs domestically in the RSA or emanates from or comes into the RSA. It is an investigation which does not entail independent or interoperable Internet-based operating systems, technologies, software applications, services, networks, signals or servers[674] in five out of the existing six online communication devices which are a landline telephone, a facsimile machine, a two-way radio device, a mobile cellular telephone and an o-tag system.[675]

Mutually agreed upon, assigned, regulated, administered, facilitated and overseen by the Member States of the ITU,[676] non-Internet based platform bases its communication operations on the exclusive and inherent sovereign online communication frequencies, spectrums,

[671] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 43.
[672] *United States v Levin* 15-10271-WGY, 2016 WL 2596010 (D. Mass. 2016) 14; Osula *Seizure of extraterritorial data* 33; Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 8.
[673] Arts 14 and 15(3) of CoE CoCC.
[674] See CoE CoCC generally which limits its provisions to Internet-based communications.
[675] This includes 'small electronic transponders…to pay tolls at bridges and tunnels' and 'passcards and devices which allow access to protected areas; Blumberg and Eckersley *Locational privacy* 317 and 320. It can also be described as a meta or traffic tag system that is attached or imbedded to human body, object or substance which grants access to a holder, silently records an access transaction, records traffic or monitors movement of the tag holder, substance or object, etc.
[676] For example, in 2000, ITU allotted spectrum to 3G (International Mobile Telecommunication 'IMT-2000'), Blackman and Srivastava (eds) *Telecommunication regulation handbook* 87, 94, 95, 96, 101-102 and 220. One of the functions of ITU is domesticated in s 34(1)(a) & (b) and (7)(a) of ECA, which is the allotment and coordination of radio frequency spectrum.

protocols or networks, which are centralised and decentralised in the RSA. Unlike the Internet-based system, which has two contradictory principles or schools of thoughts on online interception jurisdiction, there is no published or known contradictory school of thought on non-Internet-based online interception jurisdiction.

Emphatically, subject to the grant of sovereign online communication protocol and networks to the RSA by the Member States of the ITU,[677] no principle takes away the power of the RSA in conducting an OCI in serious offences that occur in the RSA in a non-Internet based investigation. Therefore, an OCI can be effectively conducted in the RSA.

2.10 ONLINE CRIMINAL INVESTIGATION OF INCOMING AND OUTGOING CROSS-BORDER ROAMING COMMUNICATION

RICA generally makes provision for the conduct of an OCI in an incoming roaming communication of a user from outside the RSA who uses a mobile cellular telephone number in the RSA,[678] which is regulated under the privacy jurisprudence applicable in the RSA. A mobile cellular telephone is one of the devices that are capable of being easily moved from one country to another.

It is submitted that the various implications of interoperability of online communications[679] apply to such incoming roaming communication in a mobile cellular telephone such that LEAs can conduct an OCI in the other devices, technologies, networks, applications and services that are in interoperable function with a mobile cellular telephone.[680]

In an incoming roaming service provision, a Telecommunication Service Provider in the RSA shall obtain and keep the personal details of the roamer before a contract of online communication service provision is rendered to the individual or juristic roamer.[681]

[677] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 43.
[678] Sections 39(3) (a) -(c) and (4) and 40(1)(b) of RICA.
[679] Para 2.3.2 of this chapter.
[680] See para 2.3.2 of this chapter.
[681] Sections 39(1) (a) (i) (aa) & (bb), (ii) & (iii); (1) (b) (aa), (bb), (cc) & (dd), (ii) & (iii) and 1(c), 39(2), 40(2), 62 (6) and 62C of RICA.

However, there is no provision for the conduct of an OCI in an outgoing roaming communication in the legal framework of the RSA, which creates a lacuna in this regard. The outgoing roaming communication from the RSA may be an original communication emanating from the RSA or maybe a returning and outgoing communication which originally emanated from another country, which is being routed back to its country of origin.

One of the consequences of this lacuna is that the RSA may be frustrated in conducting an OCI on a person who obtained or registered a SIM card in the RSA and roams to another country to commit an offence which is not recognised as a crime in the foreign country. Recently, the RSA could not easily pursue a South African citizen, whom in the course of his trip to Australia, made hate speech by rejoicing in the fact that he did not see any black person at the beach.[682] He also referred to black people in the 'k' word, which is a derogatory word and a crime in the RSA but not a crime in Australia.[683]

Another consequence for the absence of provision for the conduct of an OCI regarding an outgoing communication is that if the LEAs or LEOs in the RSA are frustrated, prevented or sabotaged from conducting an OCI on an individual, the lacuna paves way for LEAs to conduct an unregulatory, unrestrictive and unaccountable invasion of the right in online communication of an individual. This is one of the complaints lodged against the NCC, which conducts cross-border OCI without any constitutional, statutory, regulatory or policy framework in the RSA.[684]

Additionally, there is no framework on the regulation of outgoing cross-border roaming communication in the RSA. Consequently, the conduct of an OCI on the network of a foreign or receiving State by the NCC on the communication of an outgoing traveller is arguably a breach of the foreign law of the foreign or receiving State where the device of the traveller is physically and transitorily, reasonably or permanently present or located.

---

[682] Head T "Not a k***** in sight" – SA tourist causes fury with "K-word" beach rant [video] https://city-press.news24.com/News/holidaymaker-to-face-charges-for-racist-viral-video-shot-abroad-20180822 accessed 1 November, 2018 (Head https://city-press.news24.com/News/holidaymaker-to-face-charges-for-racist-viral-video-shot-abroad-20180822 (Date of use:1 November 2018).

[683] Head https://city-press.news24.com/News/holidaymaker-to-face-charges-for-racist-viral-video-shot-abroad-20180822 (Date of use: 1 November, 2018).

[684] Swart https://mg.co.za/article/2011-10-14-secret-state/ (Date of use:12 December, 2016; See para 7.3.4 of Chapter 7 of this study where the role and management of the affairs and activities of NCC are examined.

Even if there was arguably an MLA between the NCC and the foreign or receiving State on cross-border roaming communication of an outgoing cross-border roamer from the RSA, there is no mitigation of the illegality of the breach of the right to the SOC by NCC. This is arguably because, though a bilateral agreement is a legal document, it is however not a document that has the effects of the general application[685] of constitutional, statutory, regulatory or policy effect or scrutiny to strike a balance in the conflict between the protection of the right to the SOC and the conduct of an OCI.

For example, section 16(5) (a) (iv) (aa) and (bb) of RICA has a general application which provides for the mutual assistance between the RSA and foreign States in the conduct of an OCI of some serious international offences. Accordingly, it is recommended that a legal provision be made to regulate the powers of the NCC in cross-border conduct of an OCI in the same or similar way that the domestic conduct of an OCI by LEAs is regulated. Absolute reliance in an MLA that does not have a general application or that may not be opened to public scrutiny should be discouraged to ensure an attempt in striking a balance in the conflict in the subject matters in this study.

2.11 TYPES OF ONLINE CRIMINAL INVESTIGATORS

This rubric examines the reasonableness, rationality and justifiability of the relevance and role of the types of online criminal investigators identified in this study.

2.11.1 Constitutional online criminal law enforcement agencies

The Constitution recognises three categories of law enforcement agencies —SANDF, SAPS and SSA— to control and manage the security services and maintain law and order in the RSA.[686]

It is submitted that these three categories of LEAs have some incidental powers in the performance of their constitutional functions, one of which is the power to conduct a criminal

[685] Bawa *ROICA* 306.
[686] Section 199 (1) of the Constitution.

investigation.[687] Nonetheless, section 14 of the Constitution provides a list of some objects of privacy protection and breach, which indirectly or impliedly recognise some methods of investigation of crime in the Constitution. Nevertheless, there is no express constitutional framework establishing the power of the trio to conduct an OCI despite the provision of section 159(1)(a) and (2)(b), (3), (5) and (6) of the Constitution, save the limitation clause in section 36 of the Constitution which generally makes provision for the limitation of right through reasonable and justifiable means.[688]

2.11.2 Statutory online criminal law enforcement officers

Notwithstanding the absence of express constitutional principle or provision for the conduct of an OCI, RICA provides for six categories of online LEAs and LEOs that are qualified to conduct an OCI.[689] Nevertheless, this study argues that the list of LEAs or LEOs that is qualified to conduct an OCI is inchoate because it does not guarantee the independence of Chapter Nine Institutions in the conduct of an OCI as the law only grants offline investigative power to them.

Therefore, it is submitted that the list should be extended, which should include, for example, the Chapter Nine Institutions and other independent law enforcement institutions (such as SARS, FIC and SIU and commissions of enquiries established by the Constitution (such as State of Capture Commission) in order to guarantee their independence in this regard.[690] Although the PAA Act 2018 now empowers the A-G —which is one of the Chapter Nine Institutions— to conduct criminal investigation of financial matters in government departments and parastatals, however, the A-G is still not empowered to conduct an OCI in RICA or any law.

In addition, although the OPP —a Chapter Nine Institution— revealed the location traffic data of some individuals accused of visiting the residence of the Gupta family in the State of Capture Report,[691] the OPP must have relied on section 205 of the CPA to obtain this data. This is

[687] See generally Chapter 11 of the Constitution titled 'Security Services', more particularly sections 198, 199(1) & (4) and 205 (3) of the Constitution.
[688] See Chapter 5 of this study.
[689] These are CI-SAPS, DI-SANDF, SSA, DPCI, ID-NPA and IPID.
[690] See para 4.2 of Chapter 4 of this.
[691] Office of the Public Protector *State of capture report* No. 6 of 2016/17 at 84-85, para 5.21 at 99, para 5.22 at 100, para 5.23 at 100-104, para 5.24 at 104 – 106, para 5.96 at 122, para 5.97 at 122, para 5.98 at 123, para

because the OPP is not one of the applicants directly recognised to conduct an OCI in RICA. Section 15 of RICA recognises the proviso in section 205(1) of CPA[692] and vice versa.

However, the general application of section 205 of CPA, which the Constitutional Court has declared as consistent with the Constitution to conduct a preliminary investigation according to section 35 of the Constitution,[693] is defective or inadequate to strike a balance in the conflict between online communication protection and conduct of an OCI.[694] This is because section 205(1) does not comply with the significant import of the substantive and procedural requirements in RICA, which is the main and authoritative law that regulates the conduct of an OCI in the RSA.

Chief amongst these requirements in which the provisions of CPA do not comply with RICA provisions is section 16(2)(e) and (5)(b) and (c) which requires that an OCI be conducted as an alternative method of investigation and not as a method of investigation in the first instance, save where certain exceptions apply thereto.[695] The non-compliance with the requirements of section 16(2)(e) and (5)(b) and (c) of RICA in executing section 205 of CPA makes LEOs resort to section 205 as a short-cut or an unethically preferred way of conducting an OCI.[696] Nonetheless, this study proposes that section 205 of CPA be amended[697] to the effect that its provision should comply with the provisions of RICA or section 205 be restricted to the gathering of offline evidence only.

5.100 at 123, para 5.101 at 124, 301, para (aa) at 301, paras (bb) – (cc) at 301-302 and paras (dd) - (ff) at 302-303 www.publicprotector.org (Date of use:15 October 2016) (OPP *State of capture report*).

[692] See also the application of ss 81, 82(3) and (4), 83 and Chapter XII of ECTA in relation to the conduct of OCI; Basdeo 2012 2 *SACJ* 206.

[693] *Nel v Le Roux No & Others* Case No: CCT 30/95 paras 4, 6, 7, 8, 9, 10, 11, 14, 25 and 27 (*Nel v Le Roux*); *Haysom v Additional Magistrate, Cape Town and another* 1979(3) SA 155 (C) (*Haysom*) and *State v Matisonn* supra 302.

[694] Para 6.12 of Chapter 6 of this study.

[695] Para 6.5 of Chapter 6 of this study.

[696] *State v Naidoo* supra 485 A-C, 516D-517D, 521A-J, 531C-J; *State v Agliotti* supra 135-137 and 146.1; *State v Miller* paras 15-26, 33, 34; *S v de Vries* supra 613. Parliamentary Committee No 164-2016 at 40; Swart https://www.msn.com/en-za/news/techandscience/your-cellphone-records-and-the-law-the-legal-loophole-that-lets-state-spying-run-rampant/ar-AAxyCpM?ocid=spartandhp (Date of use 20 May 2018); Hunter and Smith 4 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf(Date of use 27 November 2018).

[697] Basdeo 2012 2 *SACJ* 206.

2.11.3 Special and emergency online criminal law enforcement officers

There is no legal framework for the establishment or recognition of Special LEOs to conduct an OCI in special circumstances where the usual six LEAs are not available to conduct an OCI. However, what the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 provides for is an investigator who is not a member of SAPS but who assists SAPS members in the technical operations and execution of the functions in the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017.[698]

A special LEO is a concept borrowed from the offline concept of the duty of arrest by a private citizen in the CPA.[699] A Special LEO is a specially trained, skilled or capable law enforcement officer whose primary duty may not be related to the usual constitutional or statutory law enforcement in emergencies.[700] However, by necessity or default, a Special LEO, who doubles as a private person or someone in a public law office or in a justice of peace capacity, finds himself or herself conducting an OCI or is required to conduct an OCI in some emergency or special circumstances examined in this study.[701]

There is a distinction between Emergency LEOs who conduct emergency OCI —without an OCI direction from a court in RICA—[702] and Special LEOs, who perform some civic duty in the criminal justice system. The distinction is that the former is recognised as a statutory LEA in RICA while the latter includes both the former who may not be on duty as a LEO on the one hand but is expected to act in this regard and private persons who are capable of conducting an OCI on the other hand.

In the 'inclusive area or environment', special LEOs include human pilots, crew members or any capable person in an aircraft or airborne moving object or substance; human captains, crew members or any capable person in a ship or waterborne moving object or substance; any person or other persons underground whose life or lives is or are in actual or potential danger.

[698] See sections 29(2), 30(3) and 31(4) of CCB B6-2017 which are now replaced by sections 31(2), 32(3) and 33(4) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[699] See section 42 of CPA.
[700] Sections 7 and 8 of RICA.
[701] See paras 2.11.4 and 6.5 of this study.
[702] See sections 7 and 8 of RICA.

In the 'exclusive area or environment', special LEOs exclude drivers or riders of or any person in any moving object on surfaced land, which is not submerged by water, soil, dangerous air or any other substance or disaster that poses same or similar risk in the air, in or on the sea while in an aircraft or ship or related moving objects.

A Special LEO is allowed to conduct an OCI in the physical environment described above because the methods of investigation used in investigating offences in the 'excluded areas' described above are not proportionate to the effects of the occurrence of the type of offences envisaged to be conducted by Special LEAs in the 'inclusive environment' described above. It is important to note that the conduct of an OCI is an alternative method of investigation, which requires that at least a non-OCI method may be adopted *ab initio* to investigate an offence committed before embarking on an OCI.

However, in the 'included environment' described above, it is disproportionate, unreasonable and unjustifiable to first embark on an alternative method of investigation —such as non-OCI methods of investigation— before conducting an OCI. Accordingly, the commission of a serious offence in the 'included environment' described above is an automatic justification or proof of the existence of 'necessity' principle,[703] which is generally required to be proved by LEAs before embarking on an OCI, otherwise, LEAs will continue using non-OCI methods or revert to the use of non-OCI methods in general circumstances.

In conducting an OCI, the Special LEO does not go through the usual Four-Stage or interoperable *Popoola QOCI* protocol.[704] What the Special LEO does is to press or touch a button in a movable or an immovable underground environment or in a moving object in water or air to trigger immediate or spontaneous conduct of a mass or bulk OCI in, and outside the moving object or immovable underground environment.

In attempting to interpret the intent of the legislature, it is submitted that it seems improbable that legislature would have considered the relevance and role of Special LEOs —as conceptualised and examined in this study— to be included as applicants in the conduct of an

[703] Para 6.5 of Chapter 6 of this study.
[704] Paras 2.5.1 and 6.11 of this study where a brief introduction to and comprehensive examination of the principle are made respectively.

OCI in RICA. This is because no express or implied provision was envisaged outside the distribution of the functions of the six categories of LEAs in RICA.[705]

Finally, it is submitted that the evidence obtained from the conduct of an OCI by a Special LEO is automatically declared unlawful.[706] The unlawfulness is based on the fact that a Special LEO is not required to obtain a court direction before an OCI is conducted as it is generally required in RICA. Therefore, creates a lacuna for such evidence to be admissible without further proof of its lawfulness in terms of the necessity for the conduct of an OCI by a Special LEO. However, the admissibility of this type of evidence is subject to the admissibility principle in section 35(5) of the Constitution.

2.11.4 Robotic online criminal law investigator

2.11.4.1 Introduction

There is no constitutional or statutory principle or provision or case law recognising the use and role of Robotic Online Criminal Investigation ('ROCI') and Investigator ('ROCITOR') in conducting an OCI in the RSA. Nevertheless, to deny the technical existence of a ROCI is to deny the existence or operation, use and role of online communication in contemporary society.[707]

ROCITOR is an Automatic or Artificial LEO or an Artificial Intelligence ('AI') driven system —such as a robot or drone— that conducts an OCI without the intervention or with minimal intervention of human beings in the performance of the system that conducts an OCI.

Basically, an AI is an electronically programmed system that performs complex and multifunctional operations[708] in which a human being would ordinarily be able to perform the operations,[709] however, the operations performed by a human being are not done with the same

[705] Sections 1 and 16(3) (a) -(d) and (5)(a)(i)-(v) of RICA for the definition of applicants and distribution of power of LEAs respectively in RICA.
[706] Para 7.8 of Chapter 7 of this study.
[707] For more information on artificial intelligence, see para 6.4.9 of Chapter 6 of this study.
[708] R5Componets 'Robots race it out in Tshwane' in *Dataweek* 19 July 2017 at 8
[709] Nicholaides G 'Could artificial intelligence become our greatest enemy?' http://www.702.co.za/articles/604/could-artificial-intelligence-become-our-greatest-enemy ((Date of use 2 January 2017) (Nicholaides http://www.702.co.za/articles/604/could-artificial-intelligence-become-our-greatest-enemy (Date of use: 12 January 2017). Section 71(1) - (3) of POPIA recognises and protects the use

speed, exactitude, perfection, efficiency or volume of output with what an AI device does. An AI system in this study is triggered off to automatically conduct an OCI of the commission of crime or occurrence of an activity, event or transaction that may be relevant in the conduct of an OCI.

Given the urgency and necessity involved in conducting a ROCI where the effect of the commission of an offence is either absolutely or partially irreversible, a ROCI may be conducted in automated mobile and immobile environments, amongst other circumstances.

The way that reasonableness in wartime, hot pursuit, terrorism —such as the 9-11 attack— or other exigent circumstances do not require a warrant to intercept[710] is the same way that a ROCITOR does not require a court direction to conduct an OCI in such appropriate circumstances. A ROCI is conducted in a ship, an aircraft or movable or immovable underground environment, where there may not be any immediate or spontaneous alternative opportunity[711] of conducting an investigation.

For this reason, it is submitted that the conduct of a ROCI is an exception to the consent requirement in section 71 of the POPIA, which means that consent will not be required to conduct a ROCI. In the U.S. case of *Carroll v United States*,[712] 'the court noted that it was not practicable to obtain a warrant for evidence secreted on a ''ship, motorboat, wagon or automobile'' because the vehicle can be ''quickly moved out of the locality or jurisdiction''',[713] therefore, arguably, a ROCI is most appropriate, reasonable and justified in this circumstance.

2.11.4.2 Developing a robotic online criminal investigator from the existing sophisticated automated devices, technologies, networks, applications and services

As AI is growing exponentially in the fourth technology revolution era,[714] a ROCI is built on and goes beyond the same or similar technological nature and features described below,

of automated decision-making process which in section 71(3) entitles a data subject to make representation before a final decision is made in the process.

[710] Eastman J 'Surveillance of our enemies during wartime? I'm shocked 'in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 56-57 (Eastman *Surveillance of our enemies during wartime*). Cassilly *Geolocational Privacy and Surveillance Act* 266.

[711] See paras 2.5.1 of this study.

[712] *Carroll v United States* 267 U.S. 132 (1925) at 153.

[713] Thompson *GPS monitoring* 256.

[714] Madrigal *I'm being followed: How Google-and 104 other companies- Are tracking me on the web* 352.

amongst others.[715] This description eliminates doubt on the possibility of the creation and use of a ROCI.

Firstly, a 'Gunshot Detection Device',[716] a black box used in an aircraft and a CCTV camera used in any environment to pictorially detect, and record the occurrence of an event, activity, transaction or crime are some of the automated systems available in the RSA. Like the 'Gunshot Detection Device' is the 'Shot Spotter' which is a mobile camera placed in hot-spot crime area which captures the crime scene —including sufficient description of a vehicle— and alerts the authorities for action and prevention of future occurrence.[717]

Another illustration is in the U.S., where a digital camera in a police vehicle is installed —and triggered in seven automatic ways— which record an event the moment the door of the car from the side of the driver is opened or where the siren light is activated.[718]

Secondly, in the U.S., Britain and Italy, the LEAs experimented on the use of aircraft, helicopters and other vehicles;[719]'miniature remote-controlled drone aircraft' and Unmanned Aerial Vehicle ('UAV') 'fitted with video cameras and infra-red night vision, which have the capacity to send video back to the control room to detect ''suspicious'' behaviour in crowds.'[720] The cameras which hang about 50 metres (150) feet in the air, has a moderate lightweight, which cannot be seen or heard when it is in operation.[721] As part of the existing robotic devices, plans have been mooted 'to add a ''smart water'' device that sprays suspects in some circumstances[722] and 'infuses their skin and clothes with genetic tags', which enable LEAs to identify the suspects thereafter.[723]

[715] Vlahos *Surveillance society: New high-tech cameras are watching you* 99.
[716] eNCA 'New gunshot detection system takes aim at Cape gangsterism' (eNCA 'Gunshot detection system').
[717] Police Executive Research Forum 'Cameras' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 111 and 112 (Police Executive Research Forum *Cameras*).
[718] Police Executive Research Forum *Cameras* 117-118.
[719] Police Executive Research Forum *Cameras* 111 and 112.
[720] The Economist *Learning to live with big brother* 24. Italics mine; Police Executive Research Forum *Cameras* 111 and 1112.
[721] The Economist *Learning to live with big brother* 24.
[722] The Economist *Learning to live with big brother* 24.
[723] The Economist *Learning to live with big brother* 24.

Thirdly, another sophisticated and analytical automation is the 24\7-'Liberty Island's video cameras', anti-crime 'electronic spying eyes',[724] ''facial profiling'',[725] recognition and 'licence plate readers';[726] which are all integrated into a computer system[727] and in some cases, an 'instant video replay' application is installed with 'optical-character' 'high-speed' recognition camera, which 'puts your actions in context'.[728] These systems are fully equipped with software applications that analyse images or any suspicious package, events or behaviour.[729]

The systems detect someone who waits too long at the bus stop or someone who wants to stay after closing hours.[730] The systems also detect when people find themselves or are in positions that are too tightly positioned, which could be an indication of violence or gangsterism and this indication automatically triggers the alarm or alerts human beings who oversee the cameras.[731] The camera also spots if and when someone abandons a bag or significant item[732] or where a vehicle is repeatedly roaming around an area.[733] Some of these software applications distinguish 'between ferryboats, which are allowed to approach the islands, and private vessels, which are not'.[734]

In some cases, the software application in a camera 'automatically analyses and tags' the 'colours and locations of' vehicles and the features of the faces of individuals passing before the lens.[735] In its revelation, the software application examines 'the balance of light and dark areas of skin tone and hair and gauged the distance between [the] eyes, nose and mouth'.[736] Moreover, with accuracy, a camera 'counts the number of people at any given location' and 'sends real-time information', which enables the LEAs to determine how many LEOs are needed for deployment in the area.[737]

---

[724] Vlahos *Surveillance society: New high-tech cameras are watching you* 102.
[725] Vlahos *Surveillance society: New high-tech cameras are watching you* 104.
[726] Police Executive Research Forum *Cameras* 110; Vlahos *Surveillance society: New high-tech cameras are watching you* 101.
[727] Vlahos *Surveillance society: New high-tech cameras are watching you* 97.
[728] Vlahos *Surveillance society: New high-tech cameras are watching you* 101-102 and 106.
[729] Vlahos *Surveillance society: New high-tech cameras are watching you* 97, 101- 102 and 106.
[730] Vlahos *Surveillance society: New high-tech cameras are watching you* 101- 102 and 106.
[731] Vlahos *Surveillance society: New high-tech cameras are watching you* 97 and 102; Police Executive Research Forum *Cameras* 110 and 112.
[732] Vlahos *Surveillance society: New high-tech cameras are watching you* 97; Police Executive Research Forum *Cameras* 110.
[733] Vlahos *Surveillance society: New high-tech cameras are watching you* 102.
[734] Vlahos *Surveillance society: New high-tech cameras are watching you* 97.
[735] Vlahos *Surveillance society: New high-tech cameras are watching you* 103-104.
[736] Vlahos *Surveillance society: New high-tech cameras are watching you* 103-104.
[737] Police Executive Research Forum *Cameras* 112.

Fourthly, in the U.S., the LEAs use a device, which requires that a convicted drunkard is expected to pass an 'ignition-mounted Breathalyzer' test before his or her car starts.[738] Also, while a sweat monitoring device exists which tests the level of alcohol in a parolee, it has been strongly suggested that an upgraded device be developed to test if parolees have other substances or drugs in their body. [739]

Another example in this category is the use of a device that tests the level of alcohol, which enables the device to taste the sweat level in the human body.[740] However, it is submitted that the implantation of microchips into the human body[741] seems to be the upgrade of the above devices that have been provided in the twenty-first century.

Aside from a GPS application that is now being used to monitor the whereabouts of a parolee in ensuring the attendance and non-attendance at specific places,[742] it has been predicted that a device that pre-determines the emotional status of parolee will be developed soon.[743] However, it is submitted that a device that monitors emotional assessment does not amount to a device that proves the guilt of an individual neither does it amount to a lie detector, the use of which has been declared unconstitutional in the RSA.[744]

Fifthly, a food dispensing device which drops a portion of food to a cow when the device senses a radio-frequency tag that is fitted to the ear of a cow is another sophisticated device that indicates the possibility of the invention of a ROCI device. The system is configured in such a way that even if a cow returns to get more food, the configuration prohibits the cow from taking another ration outside the period for digestion of the initial food.[745]

Sixthly, the ATM, which is a cash payment machine system that receives and disburses money and performs other functions on request by a user, sorts out the various denominations of money on recognition is an AI device. An ATM operates instead of the conventional banking staff members in the hall who do the same functions before the invention of the machine.

[738] Wood *Prison without walls* 308.
[739] Wood *Prison without walls* 309.
[740] Wood *Prison without walls* 297.
[741] The Economist *Learning to live with big brother* 25 and 33.
[742] Wood *Prison without walls* 310.
[743] Wood *Prison without walls* 309.
[744] *FAWU v Premier Foods* supra 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54 and 55.
[745] Wood *Prison without walls* 296 – 297.

The seventh example is that an Automated Targeting System in the U.S., operated by the customs department, which 'assigns a terrorist-risk assessment score to anyone entering or leaving the United States'[746] is an AI device.

In summary, some of the common features of the sophisticated or automated devices or machines described above which have been in existence demonstrate the conscious and unconscious interactions in the online communications between the objects or substances that come in contact or friction with the devices. On the occurrence of an action, event, incident or transaction; the device reacts, responds or is triggered off for further steps to be taken by the device or a human being in complying with or fulfilling the functional requirements of the device.

It is reported that an automatic monitoring device has been developed close to certainty to achieve the desired result.[747] All these machines do not need a break for lunch or bathroom purposes, neither does it go on holidays. [748] All of this describes some of the features to be found in the function of a ROCI.

2.11.4.3 Techno-legal operation and function of a robotic online criminal investigator

Given that various sophisticated automated systems existed before 2017,[749] it is more probable that a ROCI system, which is further described below can be designed, developed and operated to conduct an effective and efficient OCI in the RSA which is titled ROCI.

In conducting an effective and efficient OCI, ROCI assists in performing some configured quasi-judicial or administrative function or decision before interception, and monitoring take place in an automated environment.

Based on the application of proportionality principle, ROCI is activated by the seriousness or severity of the outcome, observation or assessment of the cumulative or single content of an

[746] The Economist *Learning to live with big brother* 27.
[747] Wood *Prison without walls* 299.
[748] Vlahos *Surveillance society: New high-tech cameras are watching you* 97.
[749] See the various dates of publication of the references of the authorities for the examination of the devices described above.

action, event or transaction. The outcome of the content must be an excessive, a grave or a substantial confusing, frictional, chaotic, disorderly, dangerous or catastrophic lighting, heat,[750] sound, smell, touch, and movement of a living being or object or substance within the automated environment before ROCI is activated.

The facts gathered in this process in the offline world are sufficient to correspondingly form a factual matrix required for the investigation of a corresponding choice of the class of serious offence at a corresponding stage of crime commission. The formation of factual matrix triggers off the detection, recording and processing in the database of the automated OCI system from which a signal is automatically and silently triggered off without a judicial or human direction.

It is submitted that the use of ROCI is one of the exceptions to the general requirements that stipulate that a court direction must be obtained[751] to intercept online communication devices linked with, close or associated to the activity, event, transaction or crime in the automated environment.

2.11.4.4 Conclusion

Despite the statement that 'no machine currently exists that could sniff out criminal intent or schizophrenia, or sexual arousal from the armpits of' an individual, the devices monitoring the movements of an individual have been developed with a high level of accuracy —as predicted by George Orwell in his famous novel in 1984—[752] with a reliable output. Therefore, ROCI is a reality that is waiting to be configured in specialised online communication devices to ensure the effective and efficient conduct of an OCI in the RSA.

Once configured, ROCI device will be installed in the communication network of an aircraft or any airborne object or substance moving or hanging in the air; a ship or waterborne object

---

[750] Swart H 'Joburg's new hi-tech surveillance cameras: A threat to minorities that could see the law targeting thousands of innocents' https://www.dailymaverick.co.za/article/2018-09-28-joburgs-new-hi-tech-surveillance-cameras-a-threat-to-minorities-that-could-see-the-law-targeting-thousands-of-innocents/ (Date of use:12 December 2018).

[751] Search in the offline world also requires judicial consent, *Investigating Directorate v Hyundai and Smit No* supra 35. Art 16(5) of UNODC 'Model Legislative Provisions Against Organised Crime' 2012.

[752] '*United States v Pineda-Moreno*, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J, dissenting); See also *United States v Cuevas-Perez*, 640 F.3d 272, 286 (7th Cir.2011) (Wood J., dissenting); Crump *Geolocational Privacy and Surveillance Act* 280.

or substance moving or stagnant in offshore. In addition, ROCI device must also be installed in the communication network of an object or any substance underground which is or not submerged by water, soil, dangerous air or liquid or any other substance or disaster that poses a same or similar risk in the air or in or on the sea as herein described. Such communication must be secure[753]and connected to an Online Communication Service Provider, which provides the interception services for a ROCI to be conducted.

However, it has been posited that a GPS —which records the location of a user in the conduct of a ROCI— should not be used to the extent of unnecessarily gathering information about a user who is figuratively described as a 'prisoner' in online communication.[754] Similarly, ROCI device should also not be used by LEAs to unnecessarily intercept the online communication of a user[755] by creating an artificial storm or condition to trigger off Robotic conduct of an OCI.

Although the conduct of a ROCI will always result in an unlawfully obtained evidence because a ROCI is an auto controlled investigative system which does not comply with the requirement of the direction of the court, however a stage-managed storm —for example— resulting in unlawful conduct of a ROCI results in double jeopardy against a user. Consequently, the application of section 35(5) of the Constitution is more likely to be considered in favour of a user by the exclusion of the unlawfully obtained evidence because its admission will render the trial unfair given the occurrence of double jeopardy herein where a ROCI is stage-managed.[756]

2.11.5 Foreign and international online law enforcement agencies

RICA recognises the role and application of foreign and international LEAs —such as Interpol— in conducting an OCI of general serious offences in incoming roaming online communications[757] and engaging in MLA Treaty in conducting an OCI relating to organised crime and terrorism.[758] This application is made through the local LEAs in the RSA, save under

[753] Section 30(2)(e) of ECA.
[754] Vlahos *Surveillance society: New high-tech cameras are watching you* 101. See para 2.3.3.3 of this chapter.
[755] Wood *Prison without walls* 310.
[756] Para 7.8 of Chapter 7 of this study.
[757] Section 40(1)(b) of RICA; Section 28(2)(b) of Telecommunication Act states that 'The Authority shall honor present and future commitments of the Republic in terms of international agreements and standards in respect of radio communication and telecommunication matters'.
[758] Section 16(5) (iv) (aa) and (bb) of RICA.

certain circumstances in international public law,[759] one of which is where local LEAs do not cooperate in assisting the foreign or international LEAs to conduct an investigation.

For instance, the Turkish authorities may proceed to seek for an order of the court in Saudi Arabia to conduct an OCI in Saudi Arabia over the murder of an American resident journalist, Jamal Khashoggi in the consulate of the Saudi Arabia in Turkey.[760]

2.11.6 Professional and non-professional online criminal private investigators

In the conduct of non-OCI, professional[761] and non-professional private entities are empowered by law to conduct a criminal investigation within the limit of the law.[762] For example, they have the power to arrest a suspect or assist LEAs in the arrest of a suspect and immediately handover such suspect to LEAs for further investigation.[763] It is submitted that professional private entities include the registered private security companies while non-professional private entities include investigative journalists and other private individuals in the RSA who find themselves conducting an investigation.

However, similar to the rationale behind the role and importance of private prosecution recognised in the CPA in the RSA,[764] there is no legal framework for the recognition or operation of professional and non-professional private entities in the conduct of an OCI in the RSA. In resolving this lacuna, it is recommended that professional and non-professional private entities should be included amongst the categories of LEAs empowered to conduct an OCI.

This initiative should not require the same or similar procedure in securing a fiat for private prosecution because of the urgency required to conduct an OCI. However, this initiative

---

[759] Articles 18(1), (2), (3)(a), (c), (e) & (i), (4), (5), (8), (9), (10),20(1) & (2), 26, 27 (more particularly sub (1)(c)), 31 (2)(a), (7) of TOCC; Articles 4, 8(1),(2),(3),(4), (5) &(6), 10(1)(f) of Smuggling of Persons by Land, Sea and Air (SOPLSA) *Annex III* of TOCC; Art 28 of African Union Convention on Cyber Security and Personal Data Protection ('AUCCSPDA').

[760] Robertson G 'Only an international court can bring Khashoggi's killers to justice' https://www.theguardian.com/commentisfree/2018/oct/23/international-court-jamal-khashoggi-killers-un (Date of use: 21 October 2018).

[761] Section 23 of Private Security Industry Regulation Amendment Bill No 27D- 2012 (PSIRAB).

[762] Sections 23(1)(b) and (2), 24, 42, 47, 48, 49 and 50 of the CPA; Section 23 of the PSIRAB. In the U.S., a Radio Link System operates which enables 'private security guards the ability to have direct communication with police by sharing a radio channel on their hand-held radios', see Police Executive Research Forum *Cameras* 111.

[763] Sections 23(1)(b) and (2), 24, 42, 47, 48, 49 and 50 of the CPA.

[764] Sections 8 -17 of CPA.

definitely requires a court direction, additional requirements than the usual OCI application requirements by LEAs and notification to the ghost or public advocate who protects the interests of the target including the government of the RSA, which may be the target of the conduct of an OCI in appropriate cases.

An example of where professional and non-professional online private investigators may conduct an OCI relates to where some members of the executive arm of the government of the RSA allegedly conspired with a family in the RSA to economically and politically capture the State of the RSA.[765] Aside from the release of the OPP's report on this issue, which recommended further investigation by the LEAs of the alleged state of capture, private individuals and entities expressed their frustration for the refusal of the LEAs to conduct further investigation in compliance with the recommendation of the OPP.[766]

Their frustrations were aggravated when the LEAs refused or failed to take further steps on the leak of the online communication on the state of capture between some members of the executive arm of government and the suspected family in the RSA.[767] One of their frustrations was expressed in terms of their inability to secure a mandate to conduct an OCI to proceed on the private investigation based on the evidence that would be obtained in the conduct of private OCI. [768]

---

[765] Jika T, Hunter Q and Wa Afrika M 'State capture -Sink or sing for Duduzane' https://www.pressreader.com/ accessed (Date of use:12 June 2018) (Jika et. al. https://www.pressreader.com/ (Date of use:12 June 2018); Hosken G and Quintal G 'Foreign cops do SA's job as FBI, UK agencies probe Guptas' https://www.timeslive.co.za/news/south-africa/2017-10-20-foreign-cops-do-sas-job-as-fbi-uk-agencies-probe-guptas/ (Date of use:12 June 2018) (Hosken and Quintal https://www.timeslive.co.za/news/south-africa/2017-10-20-foreign-cops-do-sas-job-as-fbi-uk-agencies-probe-guptas/ (Date of use:12 June 2018); Pilling D and Cotterill J 'Captured: How Jacob Zuma 'sold' South Africa to the Guptas -One family has gained extraordinary influence over a country and its politics' https://www.irishtimes.com/news/world/africa/captured-how-jacob-zuma-sold-south-africa-to-the-guptas-1.3311139 (Date of use: 12 June 2018 (Pilling and Cotterill https://www.irishtimes.com/news/world/africa/captured-how-jacob-zuma-sold-south-africa-to-the-guptas-1.3311139 (Date of use:12 June 2018).

[766] Jika et al https://www.pressreader.com/ (12 June 2018); Hosken and Quintal https://www.timeslive.co.za/news/south-africa/2017-10-20-foreign-cops-do-sas-job-as-fbi-uk-agencies-probe-guptas/ (Date of use:12 June 2018); Pilling and Cotterill https://www.irishtimes.com/news/world/africa/captured-how-jacob-zuma-sold-south-africa-to-the-guptas-1.3311139 (Date of use:12 June 2018).

[767] Jika et al https://www.pressreader.com/ (Date of use:12 June 2018); Hosken and Quintal https://www.timeslive.co.za/news/south-africa/2017-10-20-foreign-cops-do-sas-job-as-fbi-uk-agencies-probe-guptas/ (Date of use: 12 June 2018); Pilling and Cotterill https://www.irishtimes.com/news/world/africa/captured-how-jacob-zuma-sold-south-africa-to-the-guptas-1.3311139 (Date of use:12 June, 2018).

[768] Jika et al https://www.pressreader.com/ (Date of use:12 June 2018); Hosken and Quintal https://www.timeslive.co.za/news/south-africa/2017-10-20-foreign-cops-do-sas-job-as-fbi-uk-agencies-probe-guptas/ (Date of use: 12 June 2018); Pilling and Cotterill

2.12 CONCLUSION

In the techno-legal practical operations of the nature and features of online communication, it is established that online communication is an on-demand and risk-based communication, consisting of an inherent fiduciary relationship between a service provider and a user of an online communication service.[769] The risk-based relationship in an online communication arises from the interoperable or converging, non-compartmentalised, non-passworded compartmentalised and conscriptive nature and features of online communication, which expose the use of data to high levels of risks in the *constitutionally* permissible conduct of an OCI[770] in content and non-content data, real-time and archived communication and Internet and non-Internet based online communication platforms.[771]

Specifically, the conduct of an OCI is relatively faster, more complex, exponential, delicate,[772] ubiquitous,[773] absolute, comprehensive and intrusive[774] than the conduct of an investigation in non-online communication channels, platforms or circumstances.[775] The ubiquitous,[776] absolute, comprehensive and intrusive conduct of an OCI is exacerbated in an Internet-based platform in the self-imposed U.S. principle of 'no server, no law'.[777] This principle requires that the RSA must at all times seek for consent from the U.S. authorities before conducting an OCI in the RSA simply because the Internet was invented by the U.S. authorities, with exclusive control and management mandate.[778]

However, for the effective conduct of an OCI in the RSA, objection is raised in this study by propounding the 'no server, but law' principle.[779] It advocates that primary, secondary and tertiary rights to conduct an OCI of the serious offence will accordingly be ceded to the RSA,[780]

---

https://www.irishtimes.com/news/world/africa/captured-how-jacob-zuma-sold-south-africa-to-the-guptas-1.3311139 (Date of use: 12 June 2018).

[769] Para 2.2 of this study.

[770] Paras 2.2.2.2 and 2.3.1 - 2.3.3, Chapter 3 of this study, more particularly para 3.11, Chapter 6 and Chapter 8, more importantly para 8.6 of this study.

[771] Paras 2.3 and 2.6 of this chapter.

[772] Caproni *Lawful electronic surveillance* 212.

[773] Thornton *Telecommunications law* 25-26

[774] Sections 1, 12, 13, 14, 15, 17, 18 and 19 of RICA.

[775] Paras 2.2.2.2, 2.5.2, 2.5.3 and 2.8.3.3 (d) and 3.5 of this study.

[776] Thornton *Telecommunications law* 25-26

[777] Para 2.8.3 of this study.

[778] Para 2.8.3 of this study.

[779] Para 2.8.3.7 of this study.

[780] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 43.

the U.S. authorities[781] and other countries based on the 'utility' and 'necessity' principles formulated in this study.[782]

While RICA makes provision for the regulation of in-coming online roaming communication from outside the territory of the RSA, there is no provision for the out-going online roaming communication from the territory of the RSA, which creates a defect in the effective conduct of an OCI in the RSA.[783]

Finally, this chapter establishes the existence of six categories of online criminal investigators, namely: constitutional online criminal law enforcement agencies; statutory online criminal law enforcement officers; special and emergency online criminal law enforcement officers; robotic online criminal investigators; foreign and international online criminal law enforcement agencies and professional and non-professional online criminal law private investigators.[784]

[781] *United States v Levin* 15-10271-WGY, 2016 WL 2596010 (D. Mass. 2016) 14; Osula *Seizure of extraterritorial data* 33; Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* at 8.
[782] Arts 14 and 15(3) of CoE CoCC; Para 2.8.3.7 of this study.
[783] Para 2.10 of this study.
[784] Para 2.11 of this study.

Although the utility of the air is more invisibly contentious in the contemporary *anatomic* technological era, however, the air I breathe in on earth, subjacent to the sea level or in other spaces is the innermost and most invaluable realm of my heart that I exclusively control and classify in my self-determined eternity which is the secret of my being. Anything less than worshipping it as my secret is worthless, so I am ! But please let me breathe in my dignified secrecy.

CHAPTER 3: JURISPRUDENCE OF THE TECHNO-LEGAL PROTECTION OF THE RIGHT TO THE SECRECY OF ONLINE COMMUNICATION

3.1 INTRODUCTION

One of the grounds necessitating the discourse on the techno-legal protection of the right to the SOC,[785] the first overall gravamen in this study) is premised on the adverse effect of the conduct of an OCI, the second and final overall gravamen in this study), which is generally regarded as

[785] This phrase best describes the distinction between the positive right of the general enjoyment of privacy and negative right relating to its regulation and impact when privacy is communicated. A positive right allows one to enjoy the right while the negative right prohibits others from denying one from enjoying the right, *Bernstein v Bester NO* supra 76.

a necessary 'evil',[786] but paradoxically, the supposed 'evil' is aimed at protecting 'public criminal interests'[787] in the RSA. However, regardless of whether the need to advance the debate on the protection of the right to the SOC is dependent on the conduct of an OCI, this chapter applies a multi-dimensional or holistic approach in its objectives to justify the need for the techno-legal protection of the right to the SOC in the RSA. This approach, which is different from previously applied approaches by other authors in the protection of the privacy,[788] seeks to achieve the following main substantive and non-substantive law objectives.

Firstly, this chapter introduces and summarises the broad concept of privacy[789] as well as highlights the provisions of major legislations in the RSA impacting on the techno-legal nature, components and scope of the concept of the SOC.[790] The highlight of the latter objective is in pursuance of the earlier examined techno-legal nature and features of online communication and criminal investigation.[791]

Secondly, this chapter investigates the content, activity or transaction involved in online communication which generally attracts and deserves the highest levels of risks and protection

[786] Parliament of the Republic of South Africa 'Announcement, Tablings and Committee Reports' No 164 -2016 at 27. As far back as 1977, RSA has been witnessing illegal free flow and use of bugging devices. In former Rhodesia (now Zimbabwe), it was illegal for private investigators and security guards to use or be in possession of electronic interception devices such as microphones, any form of camera etc., see McQuoid-Mason D J *The law of privacy in South Africa* (1978) 148-149 (McQuoid-Mason *Privacy I*). Right2Know 'Spooked-Surveillance of Journalists in SA' https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use:27 November, 2018) at 7 (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use:27 November, 2018).

[787] This study makes a distinction in the general use of the words between 'public interests' -which include protection of public interests against civil, ethical and social wrongdoings- and 'public criminal interests' -which include criminal wrongdoing. For example, it is in the public interest, as suggested by the Economic Freedom Fighters ('EFF'), a political party in South Africa, that ministers and members of Parliament should not be served lunch because they receive salaries like any other public or civil servants who provide their lunches. This is opposed to the 'public criminal interest' call by EFF, asking the President Cyril Ramaphosa of the RSA to refund and take responsibility for the donation of R500,000 made to his election campaign for ANC elective conference in 2017 by Bosasa, a company that has been fingered many times in State of Capture Commission of Enquiry, Hunter Q 'Cyril Ramaphosa 'give back' Gavin Watson's R500,000' https://www.timeslive.co.za/sunday-times/news/2019-02-03-cyril-ramaphosa-gives-back-gavin-watsons-r500000/ (Date of use:24 June 2019). Another related story is about money laundering allegation of R400,000,000 against Cyril Ramaphosa reported by the OPP, Mabuza E 'Claims President Cyril Ramaphosa is being investigated for money-laundering bizarre: Chauke' https://www.timeslive.co.za/politics/2019-06-24-claims-president-cyril-ramaphosa-is-being-investigated-for-money-laundering-bizarre-chauke/ (Date of use:24 June 2019).

[788] Previous works adopted different approaches and methods in examining the right to privacy, McQuoid-Mason *Privacy I* ix.

[789] Paras 3.2, 3.3, 3.4.1- 3.4.3 and 3.4.4 of this Chapter.

[790] Para 3.5.6 of this chapter.

[791] Chapter 2 of this study.

respectively than in the content, activity or transaction involved in non-online communications. Applying a thirteen-point theoretical analysis,[792] in addition to the examination of other principles or theories in this study,[793] this comparison motivates the need for the investigation of the substantive aspects[794] of the techno-legal recognition, protection and enforcement of the neglected or emerging direct and independent right to the SOC in the RSA.

This comparison is in pursuance of the unique activity or transaction involved in online communication, the contents of which are exposed to great risks since the commencement of the invention and advent of the use of digital online communication in the twentieth-century quicksilver technology era. The substantive aspects of the right to the SOC are aimed at protecting and enforcing the earlier examined invaluable treasure of privacy nature, components and scope in online 'means of communication',[795] which this study arguably recognises as a subset of the broad concept of privacy.[796]

Thirdly, in complementing the second objective, this chapter does not only investigate the adequacy of the statutory provisions on the substantive aspects of the security of online communication[797] —as opposed to the other channels of private communication with lower levels of exposure of risks in their privacy communication—[798] but examines the techno-legal diverse roles of stakeholders in the legislation in this regard.

---

[792] Para 3.5.7 of this chapter.

[793] Paras 3.4.5, 3.5, 3.6, 3.7 and 3.8 of this chapter. Although this study seeks to strike a balance in the conflict between the protection of online communication and the conduct of an OCI, however, it is submitted that the protection of the right in online communication is at the mercy of the conduct of an OCI, thus, other theories are examined and proposed in the other chapters in this study. Furthermore, any measure that regulates the conduct of an OCI –such as its administration and management- is a timeous step in the right direction for the protection of the right in online communication. Therefore, the argument for the protection of the techno-legal right to the SOC is not limited to its contents or substantive aspects but to the non-substantive aspects of the role of stakeholders in securing and protecting the right in online communication and the imposition of criminal sanction against stakeholders for breach of or non-compliance with the right in online communication, amongst others, see chapters 2 and 4-8 of this study for the argument on the protection of content and non-content aspects of the protection of the right to online communication.

[794] The third objective in this chapter examines the non-substantive aspects of the right to the SOC in the RSA.

[795] See paras 2.2, 2.3, 2.5 - 2.10 and 2.11.4 of Chapter 2 of this study. Para 3.4.4 of this chapter also deals with the application of the basic scope of privacy content in the offline world to online communication; Sloan *Law of privacy in a technological society* 61.

[796] See s 14 of the 1996 Constitution.

[797] Heyink M 'A guide to the Protection of Personal Information Act- De Stadler E and Esselaar P' http://www.derebus.org.za/guide-protection-personal-information-act/ (Date of Use:12 January 2019 (Heyink http://www.derebus.org.za/guide-protection-personal-information-act/ (Date of use:12 January 2019).

[798] The other channels of privacy communication are broadcasting, human agency, offline electronic communication and postal services, see para 2.2.1 of Chapter 2 of this study. For the distinction for risks between online and non-online communication, see para 3.5.7, more particularly paras 3.5.7.6 - 3.5.7.8 of this chapter.

Put differently, on the one hand, this chapter lays the foundation for the security of the contents of online communication, which is central and indispensable to the techno-legal recognition, protection and enforcement of the right to the SOC, which has higher cumulative risks levels as opposed to the contents of non-online communication channels, which do not have higher cumulative risks levels.[799]

On the other hand, drawing on the case of *State v Agliotti*,[800] this chapter brings to the fore the significant independent and inter-dependent techno-legal multi-dimensional responsibilities of experts[801] —and non-experts alike— in administering, managing, regulating and securing the use of the respectively indispensable, and inevitable non-compartmentalised, non-passworded compartmentalised, interoperable, conscriptive and inherently fiduciary relationship and risk-based online communication.[802]

This aspect examines the significant role of expert and non-expert stakeholders in this regard which is in partial compliance with the broad and instructive decision of the Constitutional Court in *Suzman Foundation v JSC***,** which states that all public entities and institutions are accountable for the performance of their various roles in those regards.[803] Thus, absenting the role of stakeholders in securing online communication will diminish the techno-legal protection of the right to the SOC or make the right meaningless or void. Without mincing words, the right to the SOC is premised on the integrity and security of online communication,[804] therefore cannot be overemphasised.

---

[799] See paras 3.4 -3.8 of this Chapter.

[800] *State v Agliotti* supra135, 138, 139 and 14.6.5.

[801] United Nations 'Concluding observations on the initial report of South Africa' CCPR/C/ZAF/ CO/1 para 42 at 8 https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fZAF%2fCO%2f1&Lang=en(Date of use:18 January 2019 (United Nations para 42 at 8 https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fZAF%2fCO%2f1&Lang=en (Date of use:18 January 2019); Michalson ' United Nations concerned about privacy and interception in South Africa' https://www.michalsons.com/blog/un-human-rights-committee-concerned-about-privacy-and-interc (Date of use:18 January 2019) (Michalson https://www.michalsons.com/blog/un-human-rights-committee-concerned-about-privacy-and-interc (Date of use: 18 January 2019).

[802] See para 3.9 in this chapter. Popoola *Liability of ISPs* paras 2.2, 8, 82, 83, 162-163, 175 and 182; Cassim F 'Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?' PER/PELJ 2015(18) 2 at 77; See paras 2.2, 2.3, 2.5 – 2.10 and 2.11.4 of Chapter 2 of this study.

[803] 'The foundational constitutional values of accountability, responsiveness and openness apply to the functioning of the judiciary as much as to other branches of government' see *Helen Suzman Foundation v Judicial Service Commission* [2018] ZACC 8 paras 64, 65, 66, 98, 187, 211 and 212 (*Suzman Foundation v JSC*); *Azanian People's Organization (AZAPO) v President of the Republic of South Africa* [1996] ZACC 16; 1996 (4) SA 671 (CC) (*AZAPO v President*); 1996 (8) BCLR 1015 (CC) at para 17 per Mahomed DP.

[804] Kosseff J *Cybersecurity law* (2017) xxi (Kosseff *Cybersecurity law*).

Fourthly and finally, in pursuance of the third objective and as one of the central measures in the techno-legal recognition, protection and enforcement of the right to the SOC, this chapter considers the criminalisation of, and punishment for the failure or refusal of stakeholders in their multi-dimensional roles in complying with the pre-and post-protection requirements in the right to the SOC in the RSA.[805]

3.2 INTRODUCTION TO THE CONCEPT OF PRIVACY

The definition or meaning of the nature of the right to privacy remains a broad, complex, 'amorphous and elusive' debate in privacy jurisprudence,[806] thus, it is difficult to conceptualise all instances of privacy under one umbrella.[807] However, noting one of the common law definitions, privacy is arguably defined as:

> The state or condition of being withdrawn from the society of others or from public interest; seclusion…Absence or avoidance of publicity or display…A private matter, a secret…private or personal matters or relation.[808]

Nonetheless, given the general and dynamic nature of the concept of privacy and some of its summarised features in the Constitution, the concept of privacy can be expressed from the positive and negative right perspective set out in s 14 of the Bill of Rights of the RSA[809] context

---

[805] See paras 3.5.7.11, 3.9 and 3.10 of this chapter.

[806] *Bernstein v Bester NO* supra 65; Rautenbach I M 'The conduct and interests protected by the right to privacy in section 14 of the Constitution' (2001) Vol. *TSAR* 115 (Rautenbach 2001 Vol. *TSAR* 115); Neethling J 'The Concept of Privacy in South African Law' 2005 122 *SALJ* 18-19 (Neethling 2005 122 *SALJ*); Solove D J *Understanding privacy* (2008) 102 (Solove *'Privacy'*); Solove 2002 Vol. 90 *California Law Review* 1088; Rautenbach I M 'Privacy taxonomy' (2009) 3 *TSAR* 550 and 554 (Rautenbach 2009 3 *TSAR*); Currie I 'The Concept of privacy in the South African Constitution: Reprise' 2008 3 *TSAR* 550-551; (Currie 2008 3 *TSAR*).

[807] Solove 2002 Vol. 90 *California Law Review* 1092; Ruiz *Privacy in telecommunications* 23.

[808] Onions C T (ed) *The shorter of Oxford English dictionary* (1933) 1586; McQuoid-Mason *Privacy I* 91.

[809] Bawa '*ROICA* 302; Regulation of the Interception of Communications and Provision of Communications Related Information Act No 70 of 2002 ('RICA') Scoglio S *Transforming privacy - A Transpersonal philosophy of rights* (1998) 1; Ruiz *Privacy in telecommunications* 23; McQuoid-Mason D 'Privacy' in Woolman et.al. *constitutional law of South Africa* (2013) 2nd ed. Revision Service 5 at 38-6 (McQuoid-Mason '*Privacy II*); McQuoid-Mason D 'Invasion of privacy: Common law v Constitutional Delict-Does it make a difference?' (2000) *Acta Juridica* 248 (McQuoid-Mason (2000) *Acta Juridica*); Devenish G E *A commentary on the South Africa bill of rights* (1999) 147; Roos 2012 129 *SALJ* 395; Currie I and De Waal J *The bill of rights* handbook (2014) 294-295 (Currie and De Waal *Bill of rights*); Du Plessis L and De Ville J 'Personal rights' in Van Wyk D et.al (eds.) *Rights and constitutionalism: The new South African legal order* (1994) 242 (Du Plessis and De Ville 'Personal rights'); SALRC 'Privacy and data protection,' Paper 109-Project, Chapter 2 at 10 and 14 **(**SALRC http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016); Rautenbach 2001 Vol. *TSAR* 115 115; Neethling 2005 122 *SALJ* 18; Solove *Privacy* 102 and Rautenbach 2009 3 *TSAR* 550 and 554; Currie 2008 3 *TSAR* 550-551. South Africa is a signatory to regional and international instruments such as the Universal Declaration on Human Rights (art 12), International convenant on civil and political rights (art 17) and African Charter on the rights and welfare of the child (art 10), amongst others, see

as follows:

> Everyone has the right to privacy, which *includes* the right not to have- (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) *the privacy of their communications infringed*.[810]

In case law, the negative right implies that privacy is breached in an unlawful invasion or disclosure of private facts concerning an individual.[811]

Although paragraph (d) seems to protect the privacy of communication in both offline and online world, it is however submitted that the definition is inadequate to cover the broad concept of privacy relating to the protection of the content, activity or transaction that takes place in the risky and complex interoperable, conscriptive, non-compartmentalised and non-passworded compartmentalised online communication in contemporary society.[812]

Rather, because of its unique nature and features,[813] the argument is canvassed that online communication should be protected under the concept of secrecy as a subset of or as an autonomous right in the broad concept of privacy.

To illustrate the distinction in section 14 of the Constitution using a statutory provision, section 10(3) (a) -(c) of the ISA,[814] within its scope of the object, provides for the protection of physical, computer and communication security services respectively to address the inadequacy in section 14 of the Constitution. Specifically, while section 10(3)(a) of the ISA provides for the protection of physical security, which is likened to section 14(a)-(c) of the Constitution, section 10(3)(c) of the ISA —which provides for the protection of communication security services— relates to section 14(d) of the Constitution, which is also broad to protect the unique right in online communication.

Privacy International 'State of Privacy South Africa' https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa(Date of use: 25 April, 2019.

[810] Italics mine.

[811] *Bernstein v Bester NO* supra 68.

[812] In examining the provisions of the POPIA, which commence the enforcement of the right to privacy in 2016, 20 years after the enactment of the 1996 Constitution, POPIA protects offline privacy issues but not the right in online communication, Heyink http://www.derebus.org.za/guide-protection-personal-information-act/ (Date of use:12 January 2019).

[813] Para 2.2 – 2.3 of Chapter 2 of this study.

[814] Intelligence Services Act 65 of 2002 ('ISA').

However, while section 14(d) of the Constitution relatively protects the other four channels of privacy communication,[815] it is submitted that section 14(d) is too broad to protect the unique right to the SOC, the defect of which section 10(3)(b) of the ISA —which protects computer security— largely and unequivocally seeks to cure and identify with.

3.3 THE DOCTRINE OF THE LAW OF PERSONALITY AS THE ORIGIN OF THE RIGHT TO THE SECRECY OF ONLINE COMMUNICATION

In the Roman law context, personality is usually referred to as and based on the principle of *injuria iniuria*, which comprises *corpus* (physical body or integrity), *fama* (good name) and *dignitas* (dignity),[816] which also arguably exist in online communication.

The right to privacy is identified in modern theory and practice as one of the personality rights,[817] which are 'inalienable, inherent human rights'.[818] The law of personality, which originated in Europe in 1877 is a basic, an independent and subjective private law right, which also impacts on and protects public law such as criminal law, procedure and sanction[819] as well as other aspects of the law such as insurance law, administrative law and fundamental human rights law, the general law of delict, amongst others.[820]

Accordingly, it is submitted that given that one of the personality rights is the right to privacy; and the right to the SOC is a subset of the right to privacy, then the right to the SOC is a direct, subjective, an independent, inalienable and inherent human right[821] in contemporary society, which is impacted by the conduct of an OCI in the RSA.

The law of personality regulates the 'recognition, definition and protection of the various rights to personality' of an individual and a juristic person.[822] This study seeks to examine the

[815] The five channels of privacy communications are broadcasting, human agency, offline electronic communication devices, online communication devices and postal services, see para 2.2.1 of Chapter 2 of this study.
[816] Neethling J, Potgieter J M and Visser P J *Neethling's Law of personality* (1996) 4 and 5 (Neethling, Potgieter and Visser *Neethling's Law of personality*).
[817] Neethling, Potgieter and Visser *Neethling's Law of personality* 6.
[818] Neethling, Potgieter and Visser *Neethling's Law of personality* 5.
[819] Neethling, Potgieter and Visser *Neethling's Law of personality* v, 3, 5 and 8.
[820] Neethling, Potgieter and Visser *Neethling's Law of personality* 3, 5 and 6.
[821] Neethling, Potgieter and Visser *Neethling's Law of personality* v, 3, 5 and 8; Paras 3.3, 3.4.2, 3.4.4, 3.4.5 and 3.5 of this chapter.
[822] Neethling, Potgieter and Visser *Neethling's Law of personality* 3 and 5.

recognition, definition and protection of the various rights to the personality of an individual or juristic person in online communication in contemporary society.

The most important aspects of the personality of an individual include the: 'physical integrity, freedom, honour, status (for example, by birth or profession), name, distinctive marks (such as trademark or trade name), image, undisturbed participation in the economic sphere, copyright and the right to an invention (patent)',[823] all of which arguably exists in online communication in contemporary society. For example, the monitoring of an individual via geographic traffic or geo-locus data and meta or status data impact on the physical body or integrity aspect of the personality of an individual.[824]

Some reasons account for the development of the law of personality, some of which are premised on the gravamen of this study.[825]

Firstly, because the invention and development of technology pose actual and potential threats to the breach of the personality right such as the right in photography, law of personality is protected.[826]

Secondly, as a corollary to the first, the need to protect new right such as the right to intellectual property —which was rejected as an ordinary property right— gave rise to the law of personality in this regard.[827] For example, there is an intimate relationship between an author who expresses his or her spirit, power and personality in-copyright work than an owner in a physical property.[828]

Thirdly, the need to identify the object of a right and the personality or interest involved in that

[823] Joubert W a *Grondslae van die Personoonlikheidsreg* (LL. D thesis University of Stellenbosch 1953) 20; Neethling, Potgieter and Visser *Neethling's Law of personality* 8-9 and 12- 41. Paras 3.4.5.3 of this study.
[824] See paras 2.6.2.1 and 2.6.2.2 of Chapter 2 of this study.
[825] Joubert W a *Grondslae van die Personoonlikheidsreg* (1953)15 (Joubert *Personoonlikheidsreg*); Neethling J *Die Reg op Privaatheid* (1976) 23 (Neethling *Privaatheid*); Neethling, Potgieter and Visser *Neethling's law of personality* 6.
[826] Neethling *Privaatheid* 23; Neethling, Potgieter and Visser *Neethling's law of personality* 6.
[827] Joubert *Personoonlikheidsreg*15-16; Neethling J 'Outeursreg en Persoonlikheidregte: 'n Teoretiese Analise met verwysing na Outeursregbevoegdhede in die SA Reg' 1975 *THRHR* 333 (Neethling 1975 *THRHR*); Neethling, Potgieter and Visser *Neethling's law of personality* 6-7; Ruiz *Privacy in telecommunications* 23.
[828] Joubert *Personoonlikheidsreg* 16 and 18; Neethling 1975 *THRHR* 333; Neethling, Potgieter and Visser *Neethling's law of personality* 6 - 8.

object gave rise to the development of subjective right under the law of personality.[829] Similarly, these three reasons above —amongst other reasons in this entire study— that account for the development of the law of personality square up with the reasons for the protection of the right to SOC, more particularly the development in this study of the four special reasons for the protection of the right to the SOC.[830] Therefore, the right to the SOC is traceable to the law of personality which must be protected in online communication.

3.4 APPLICATION OF THE GENERAL CONCEPT OF OFFLINE PRIVACY TO ONLINE PRIVACY

3.4.1 Introduction

Whether in the home, office, car or public place[831] — on earth, above or below the sea level— there is a legitimate personality expectation —both subjective and objective—[832] that the nature, contents, components and scope of the concept of privacy recognise and protect the biological, physical, psychological, sociological and moral aspects of the subject, object and substance of a human being.[833] Based on this expectation, the general right to privacy is broadly derived, encompassed, defined, protected and enforced in section 14 of the Constitution.

The right to privacy is protected vertically and horizontally in the RSA, which means that the right can be enforced against the State and an individual in the RSA.[834] The right to privacy is recognised by common, constitutional and statutory law in the RSA.[835]

---

[829] Joubert *Personoonlikheidsreg*16; Neethling 1975 *THRHR* 333; Neethling, Potgieter and Visser *Neethling's law of personality* 7.

[830] See paras 3.4.5.2 – 3.4.5.5 of this chapter.

[831] Currie and De Waal *Bill of rights* 296.

[832] Para 3.6 of this chapter and Currie and De Waal *Bill of rights* 298; *Bernstein v Bester NO* supra 65, 74, 75, 76, 78, 85 and 93.

[833] Para 3.6 of this chapter and Currie and De Waal *Bill of rights* 298; *Bernstein v Bester NO* supra 65, 74, 75, 76, 78, 85 and 93.

[834] *NM v Smith* supra 132 and 136.

[835] Currie 2008 3 *TSAR* 551-554 and Neethling 2005 122 *SALJ* 20; *NM v Smith* supra 120; See more particularly sections 1(a), 7(1), 10, 12, 36 and 39 of the 1996 Constitution. Currie and De Waal *Bill of Rights* 295-296. *Bernstein v Bester NO* supra 68 and 71; SALRC Chapter 2 at 4-5 http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use:27 June, 2016; See generally the provisions of the POPIA; *O' Keffe v Argus Printing and Publishing Co Ltd* 1954 (3) SA 244(C) (*O' Keffe v Argus Printing*); Roos 2012 129 *SALJ* 394; *Protea Technology Ltd v Wainer* 1997 (9) BCLR 1225 (W) 1241 or 1997 3All SA 594 (W) 608 (*Protea Technology Ltd v Wainer)*; *NM v Smith* supra 150-154; Rautenbach 2001 Vol. *TSAR* 116;McQuoid-Mason *Privacy II* at 38.2 and 38.3; Currie and De Waal *The bill of rights* 31-34, 56- 71 and 133-149 and 295-296; Roos A 'Data Protection' in D Van der Merwe et al *Information and communication*

McQuoid-Mason posits that the broad concept of privacy in the RSA is flexible to accommodate the U.S. concept of privacy,[836] which recognises and protects the concept of the secrecy of online communication.[837] Therefore, it is submitted that privacy jurisprudence in the RSA should accommodate, recognise, protect and enforce the right to the SOC as described in this introduction.

3.4.2 The religious and philosophical origins of the general concept of privacy

One of the first cases of conflict witnessed by humankind is recorded in the religious writings. These writings highlight the conflict between the protection of the right to privacy of Adam and Eve and their investigation for disobeying the commandment of God relating to the instruction by God that Adam and Eve should not eat from the 'forbidden fruit in the Garden of Eden'.[838] Upon discovering the disobedience by Adam and Eve, God decided to conduct an investigation on them, which led to their resistance to submit to the investigation, having realised that they were stark naked.[839] This scenario highlights one of the origins of the concept of privacy in contemporary society.

3.4.3 Hierarchical and non-hierarchical protection of information in the family of privacy concept

3.4.3.1 Introduction

Drawing on the general hierarchy of the protection of offline information in the family of privacy law by governments and corporate entities worldwide, it is common knowledge that, according to the levels of risks in an offline communication of privacy, communication of information or privacy is hierarchically and generally categorised as follows: a) 'public'; b) 'private'; c) 'confidential'; d) 'secret' and e) 'top secret' domains.[840]

---

technology (2008) 355 (Roos *Data Protection*). The distinction between common and constitutional law has been criticised by scholars, see Currie 2008 3 *TSAR* 2008 3 554.

[836] McQuoid-Mason *Privacy I* xl.

[837] Ruiz *Privacy in telecommunications* 1 -3 and 5.

[838] Genesis 2: 16-17 and 25 and 3:4-13 in the Holy Bible and Chapter 20: verse 120 in the Holy Quran.

[839] Genesis 2: 16-17 and 25 and 3:4-13 in the Holy Bible and Chapter 20: verse 120 in the Holy Quran.

[840] *Independent Newspaper Pty Ltd v Minister of Intelligence Services and others* [2008] ZACC para 49 (*Independent Newspaper v Minister of Intelligence Services*). See ss 60-68 of POPIA. Section 60(3) and (4) of POPIA generally recognizes the fact that there are classes of personal information to be protected.

This study draws on the above general hierarchy of protection of information to argue that the right to the SOC be placed on a unique level which is distinct from the level that non-online communication is located. Essentially, this study reconceptualises the hierarchy of information protection in some unique ways that are appropriate to give effect to the invaluability of the content of online communication in contemporary society in these interdependent approaches: a) 'general comparative hierarchical information'; b) 'specific comparative hierarchical information' and c) 'non-hierarchical online '*res ipsa loquitur*' or non-comparative hierarchical information' approaches.

3.4.3.2 General comparative hierarchical information approach

The general comparative hierarchical protection of the information approach is used in comparing the levels of risks between online and non-online communications, where the point of departure is the minimum entry-level of personality interest in privacy. This approach lays the foundation for the examination of other approaches below despite their differences.

According to the five general levels of the hierarchy of information classification listed above,[841] it is submitted that the general comparative hierarchical protection of information approach examines the justification for the general comparative hierarchical protection of the direct and independent right in the communication of information in the online world[842] at the 'secrecy' level when an online communication of information occurs as opposed to an offline 'privacy' which is at the 'confidentiality' level when the communication of information occurs.

This is because when information has not been communicated, it is generally protected at the minimum entry level of information hierarchy —which is 'privacy' level— or within the exclusive 'privacy' control and management of the data owner or subject[843] which could be in the mind of an individual, a memory stick, a document, an object et cetera.

Nevertheless, when offline information is communicated, revealed, accessed or invaded, the protection of such offline information is elevated from the 'privacy' level to the next level

[841] Para 3.4.3.1 of this chapter.
[842] Para 3.5.7 of this chapter adopts thirteen principles in the comparison of the nature, features and threshold of risks and protection between online and non-online privacy communication in the RSA.
[843] Gellman and Dixon *Online privacy* 38.

which is the 'confidentiality' level in the offline world because the risk increases to the next level as the offline private information is communicated, revealed, accessed or invaded.

However, in the case of online communication, when information is communicated from the 'privacy' level —which is the minimum level of information hierarchy— where the information is stored (in a memory stick, human mind, copied from other sources, etcetera) to the online world, the protection of such information is elevated *not* to the 'confidentiality' level but *above* the 'confidentiality' level which is the 'secrecy' level. This is because of the higher risks involved in online communication than the risks involved in offline communication.

For example, in the offline privacy, the personality interests of an individual which are exposed to higher risks in the communication process are protected at the 'confidentiality' level in offline privacy communication, such as the offline protection of HIV test report.[844] It is not surprising therefore that persons, employees or officers entrusted with official, non-official, and sensitive offline information usually sign or are usually expected to sign or are presumed to have signed or acknowledged a 'confidentiality' clause.

The signature or acknowledgement is done in a bid to elevate the level of protection of such sensitive offline information from the minimal 'privacy' level to the 'confidentiality' level of protecting personality right when such information is communicated in the offline 'privacy' concept.[845] Elevating information from the 'privacy' level to the 'confidentiality' level reduces the levels of risk that the offline information is exposed to in the 'privacy' communication process. This is because the protection level is also elevated to the 'confidentiality' level.

In online privacy, it is reasonably, rationally and justifiably appropriate to protect and give meaningful effect to the value of online communication at the 'secrecy' level,[846] which is the *next progressive level* to 'confidentiality' level in the general minimal entry of information protection. The protection of online communication at the 'secrecy' level is premised on the significance of the basic and special nature and features of online communication as opposed

[844] *NM v Smith* supra 41, 43, 56, 61, 80, 103, 137, 158 and 183; See paras 3.5.7.2 - 3.5.7.14 of this chapter.
[845] Neethling, Potgieter and Visser *Neethling's law of personality* 3.
[846] Para 3.5.7 of this chapter.

to the less risky offline privacy communication, which is located at and categorised under the 'confidentiality' level of the general hierarchy of information protection.[847]

Extending the general comparative hierarchical approach beyond the two scenarios illustrated above, the finding of this study does not have scientific evidence to show that the value of online communication of a private individual in the society is protected at the 'top secrecy' level, which is the highest level in the globally recognised hierarchy of information protection. The 'top secrecy' level, which though is not the gravamen of this study, is extremely unique in the comparative hierarchical approach, which arguably existed in the non-comparative hierarchy approach of privacy communication of critical database of government before it was replaced by the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017 which abolishes the old bill.[848]

In summary, this study adopts a thirteen-pronged principle —amongst other principles—[849] to compare the nature and features of online and non-online communication in determining the protection of right in an online communication at the secrecy level.[850]

3.4.3.3 The specific comparative hierarchical minimal information approach

Given the extent to which privacy is protected in the public domain, it is submitted that the protection of any privacy concept —be it online and non-online communications— commences at the minimum entry level of protection of the personality value, interest and right[851] of a specific instance of privacy as the point of departure to hierarchically compare the protection of online and offline privacy.

Essentially, if for instance privacy is protected in the *public place*, the minimum entry-level of personality right in online privacy in this approach is the installation of o-toll[852] cameras in

[847] Para 3.5.7 of this chapter.
[848] See paras 3.4.3.4 of this chapter respectively; See section 57 of CCB of 2017 which is now expunged by the Cybercrime Bill 2018 – Amendments Proposed to Bill B6-2017.
[849] Paras 3.4.4.2 - 3.4.4.6 of this chapter.
[850] Para 3.5.7.2 - 3.5.7.14 of this chapter.
[851] For law of personality right, see para 3.3 of this chapter; Neethling, Potgieter and Visser *Neethling's law of personality* 3.
[852] This study adopts the term 'online' communication, which seems more appropriate to describe the specific type of communication, which distinguishes it from the broad terminology of electronic communication, which

general public areas.[853] These cameras legally function to the extent of monitoring the geographic or public movement of traffic, people or object for *toll* or *fee collection only* by capturing a picture of the plate number of the vehicle and not the number of faces of the occupants in a vehicle. However, the o-toll payment system introduced in 2011 in the Province of Gauteng in the RSA impacts on the protection of the personality right at the minimal level because a bill or invoice sent by the o-toll authorities to motorists captures the pictures of occupants in the vehicle against the reasonable anticipation of some privacy while in a vehicle.

Applying the specific comparative information approach, it is argued that the capture of the picture of a pedestrian at an o-toll system is a breach of 'privacy' while the capture of the picture of the occupants in a vehicle is a breach of the right to 'confidentiality' because there is a higher risk and anticipation of greater privacy in the latter than the former. It is further submitted that the *storage* in a system of a picture captured at the o-toll system or the *dispatch* of it to an o-mail communication of the registered owner of the vehicle impacts on the right to the SOC. This is because there is higher anticipation of privacy in the vehicle where the picture was *captured*, *stored* and *sent* through an online communication to the vehicle owner.

Under this approach, until the law regarding o-toll collection is amended to broaden the scope of the cameras at the o-toll system beyond toll collection, which in any case must be lawful, reasonable, justifiable and must not be adverse to the right to the SOC as it is happening in some countries,[854] the mandate of the government does not classify the storage or dispatch of

---

comprises both offline electronic and online communications. Because the scope of this study is limited to online network communication, it seems more appropriate to adopt the term 'online' or 'o'.

[853] *Bernstein v Bester NO* supra 67; *National Media v Jooste* supra 271 (A); *Mholongo v Bailey* supra 70'; Section 22 of CPA No 51 of 1977; Sections 13(6) and 13 (7) and (8) of the Police Act No 68 of 1995; Basdeo 2009 (12) 4 *PER* 316/360- 319/360 and 326/360- 328/360. Dlulane https://ewn.co.za/2018/10/28/people-who-share-malusi-gigaba-sex-video-could-get-in-trouble-with-the-law (Date of use: 27 January 2019); Paras 3.5.7.14 of this chapter.

[854] A public camera should not be monitoring individuals on the streets with an in-built database facial recognition technology where no serious offence has been committed, see Laperruque J 'Facial recognition surveillance faces new legal limit' https://www.axios.com/facial-recognition-surveillance-faces-new-calls-legal-limits-e99794ee-5fe1-45f8-bbc8-0ef0450d93d1.html (Date of use:14 April, 2019. The Chinese model of monitoring everyone with face recognition technology which conscripts the social and family life of an individual to the extent of banning an individual from being able to buy a train ticket because such individual has not carried out family responsibility including failure to buy diapers is unlawful, unreasonable and unjustifiable, see Diamond A M 'China's surveillance State should scare everyone- The country is perfecting a vast network of digital espionage as a means of social control with implications for democracies worldwide' https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/ (Date of use: 2 March 2019); Naughton J We Have Been Harmonised: Life in China's Surveillance State by Kai Strittmatter – review - A remarkable analysis identifies 'Mao 2.0' as the west's new cold war adversary https://www.theguardian.com/books/2019/jun/30/we-have-been-harmonised-life-china-surveillance-state-kai-strittmatter-review (Date of use:2 July, 2019).

the picture of a person, object or substance in a vehicle in an o-toll system under 'public', privacy', 'confidentiality' or 'top secret' domains. Rather, the storage or dispatch of a picture captured at the tollgate can only be located at the secrecy level of personality right in privacy. Technically, an o-toll may be configured in such a way that only an invisible signal in a plate number is sent to the network at the o-toll gate, which is similar to the existing o-tag system that exists at some toll gates in the RSA that spot an o-toll registered vehicle and automatically opens the gate without capturing any picture of the car or the occupants in a vehicle.

In summary, this study refers to a four-point special reasoning[855] —amongst other forms of reasoning— in determining the specific comparative hierarchical minimal information approach in the secrecy of online communication according to the nature and features of a particular online communication, object or substance.

3.4.3.4 The non-hierarchical online 'res ipsa loguitur' or non-comparative hierarchical information approach

The non-hierarchical online *res ipsa loquitur* or non-comparative hierarchical information approach may be controversial because it may not follow the same logic, reasoning or premises applied in the other two approaches examined above.[856]

The maxim *res ipsa loquitur* is a liability principle which is commonly used in the law of delict or tort to express the occurrence of a strict liability, which requires an indiscriminately low standard of or no proof in apportioning liability to a person that is at fault. [857] It is also a situation where a party merely points to the consequence of the action or omission of another party, which translates to the saying that the 'fact of the matter speaks for itself' or '*res ipsa loguitur*', which is sufficient to show a strict liability.[858]

Accordingly, instead of embarking on a voyage of discovery of evidence to classify the right in online communication through the examination of either the 'general comparative

[855] Para 3.4.5.2 - 3.4.5.5 of this chapter.
[856] Paras 3.4.3.2 and 3.4.3.3 of this chapter.
[857] *Cecilia Goliath v Member of the Executive Council for Health, Eastern Cape* (085/2014) [2014] ZASCA 182 paras 5, 6, 9, 10, 12 and 18.
[858] *Cecilia Goliath v Member of the Executive Council for Health, Eastern Cape* (085/2014) [2014] ZASCA 182 paras 5, 6, 9, 10, 12 and 18.

hierarchical information approach' or 'specific comparative hierarchical minimal information approach',[859] all a party needs to prove is that the fact of the matter independently speaks for itself in locating an online communication at the secrecy level. This is because of the uniqueness of the non-compartmentalised, non-passworded compartmentalised, interoperable, conscriptive, inherently risk-based and fiduciary relationship-based online communication nature and features.[860]

The maxim *res ipsa loquitur* arguably lays the foundation for the subjective or societal and objective or *boni mores* beliefs[861] or expectations that online communication should be protected at the 'secrecy' level. This is because information is communicated and entrusted in a third party —i.e., Online Communication Service Provider or agent— at a highly risky quick-silver technological era which is strictly a sufficient fact that speaks for itself in contemporary society, which should independently or non-comparatively be placed at the 'secrecy' level.[862]

The inherent, obvious and undeniable fact of the existence of high risk in an online communication motivates the strict enforcement of criminal sanction against stakeholders who do not respect, observe, and comply with the various provisions of the five statutes regulating the inherently highly risky and complex online communication.[863]

According to the Supreme Court of Appeal in *Mngomezulu v NDPP*,[864]one of the reasons for regarding the information in a telephone call as a secret is because of the secrecy or covertness of the conduct of an OCI.[865] This ratio does not rely or necessarily rely on any general or specific hierarchy of information approach to arrive at this decision which is largely independent of the two approaches above, but consequentially follows that, should an investigation of this nature be conducted in online communication, it must be conducted in a secretive or covert manner. This is because of the unique nature and features of the type of channel of communication that online communication is which places its protection at the secrecy level.

[859] Paras 3.4.3.2 and 3.4.3.3 of this chapter.
[860] See paras 2.2.2 and 2.3.1 -2.3.3 of Chapter 2 and paras 3.5.7.2 - 3.5.7.14, 3.8, 3.9 and 3.10 of this chapter.
[861] *Bernstein v Bester NO* supra 68, 70 and 71 and 75.
[862] See paras 2.2.2 and 2.3.1 -2.3.3 of Chapter 2 and paras 3.5.7.2 - 3.5.7.14, 3.8, 3.9 and 3.10 of this chapter.
[863] Paras 3.5.6, 3.9 and 3.10 of this chapter.
[864] *Mngomezulu v NDPP* [2007] SCA 129 (RSA) supra 6 and 7.
[865] *Mngomezulu v NDPP* [2007] SCA 129 (RSA) supra 6 and 7.

Essentially, this precedent, without relying on the 'general comparative hierarchical information' and 'specific comparative hierarchical minimal information' approaches,[866] applies the nature and features of the conduct of an OCI as the yardstick for the recognition, classification and protection of the right to the SOC in the non-hierarchical online *res ipsa loquitur* or non-comparative hierarchical information approach.

The non-hierarchical online '*res ipsa loquitur*' information approach is used in examining a particular form or type of privacy expectation[867] on its own without necessarily relying on the comparison of the nature and features of other forms or types of privacy in contemporary society, which also describes the non-comparative hierarchical information approach in the same manner.

Put differently and specifically, to give meaning and effect to the particular nature and features of the content, activity, event and transaction in online communication, there is an expectation that privacy in an online communication is classified as the concept of the SOC[868] on its own without necessarily referencing other forms, instances or types of privacy right as the basis for the location of the right in an online communication at the 'secrecy' space.

Colloquially, from the perspective of a layman or the society, in a natural intuition or some other mysterious appreciation, the society makes a pronouncement about and protects some pieces of information at a level in the protection of personality right. For example, an individual unconsciously says that 'the information am giving you is confidential' or 'let me tell you a secret' without relying on any general or specific scientific hierarchical information approach.

Another example where a non-comparative information approach applies in the other levels of the hierarchy of information is in the nature and features of tax payment, where the society acknowledges that tax payment is placed at the 'confidentiality' level because the transaction is, in this regard, generally between two parties only, i.e., the taxpayer and the SARS.

In another related vein, the society generally knows that offline banking transaction is conventionally and independently or non-comparatively placed at the 'secrecy' level without

[866] Paras 3.4.3.2 and 3.4.3.3 of this chapter.
[867] *Bernstein v Bester NO* supra 65, 74, 75, 76, 78, 85 and 93.
[868] Paras 2.2, 2.3, 2.5- 10 and 2.11.4 of this chapter.

any comparison with other instances of privacy concept. This is because a bank acts as a third party in a transaction between a customer and a beneficiary in this regard, thus trust issues arise in the transaction and for this reason, the transaction may not be placed at the 'confidentiality' level but at the level of secrecy.

To further demonstrate the non-comparative hierarchical information approach at other levels of information hierarchy in the RSA in terms of the legislative framework, the ECTA provides for the identification and declaration of 'critical databases' as a special class of data necessary for the 'protection of national security' of the RSA or 'the economic and social well-being' of the people of the RSA,[869] which is arguably protected at 'top secrecy level'.

Furthermore, the POPIA, which is a statute that regulates both online and non-online data protection, classifies 'specialise personal information' as a unique form of personal information protection, which requires more protection than the other types of information without any comparison with other instances of privacy.[870]

In addition, before the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, the Cybercrime and Cybersecurity Bill recognised and protected different classes of data according to their 'level of sensitivity, values and criticality to the data for purposes of securing control for the protection of the data'[871] without applying any comparative hierarchical information approach to classify such data. There is no more classification of a critical database, which would have comprised public and utility data of government and non-government entities is arguably classified as 'top secret'.[872]

The rationale for the classification of a critical database at 'top secret' hierarchy stems from the fact that it involves public or utility data and if compromised, it impacts on the lives, existence and operations of the human race on earth and in other planets, where there is an online integration of data on earth and in other planets.

---

[869] Sections 53 -58 of ECTA.

[870] Section 26 of the POPIA. Moorcroft J 'POPI and the legal profession: What should you know? http://www.derebus.org.za/popi-legal-profession-know/ (Date of use: 18 January 2019).

[871] Section 57 (12) of the Cybercrime and Cybersecurity Bill (CCB) B6–2017, published in Gazette No 40487 of 9 December 2016 (CCB B6-2017). Please note that CCB B6-2017 replaces CCB B-2015. The Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017 which does not protect critical database abolishes the previous bill.

[872] Para 3.4.5.3 of this chapter.

It follows therefore that the concept of the SOC can be regarded as a standalone right in the same way that both the ECTA and POPIA classify 'critical databases' and 'special personal information'[873] without necessarily, squarely, uniformly and progressively comparing these rights in the order that it appears in the five hierarchical order above.[874] Each of these rights at their various levels of non-comparative consideration can be sub-divided into layers according to their nature, features and needs.[875]

This study also refers to a four-point special reasoning[876] —amongst other forms of reasoning—[877] in determining the non-hierarchical online 'res ipsa loguitur' or non-comparative hierarchical information approach in the secrecy of online communication according to the nature and features of a particular online communication or substance.

3.4.3.5 Conclusion

In conclusion, without conceding to the presumption for a moment that the hierarchical approach in rating the right in the risk-based online communication at the 'secret' level may be fallacious, the right and sub-rights in online communication can be independently conceptualised as a right(s) to secrecy in the Constitution with or without comparing it with other forms, types or channels of privacy communication or broad privacy concept.

This is because if one of the elements of privacy was described as 'secret' as early as 1978 when online communication was at its infancy, it follows therefore that the common law definition of privacy[878] in contemporary quick-silver technology society envisages that some unique components, contents, forms, types and scope of privacy or its communication channels will be rated at secrecy level, one of which channel is the unique online communication. Its uniqueness bothers on its non-compartmentalised, non-passworded compartmentalised, interoperable, conscriptive, inherently risk-based and fiduciary relationship-based online communication nature and features which may or may not be compared with other channels of

[873] Sections 53–58 of ECTA and section 26 of POPIA.
[874] Para 3.4.3.1 of this chapter.
[875] Paras 3.5.7 and 3.8 of this study.
[876] Para 3.4.5.2-3.4.5.5 of this chapter.
[877] Other reasoning includes all the arguments advanced in this study that directly and indirectly protect the right to the SOC.
[878] Onions CT (Ed) *The shorter of Oxford English dictionary* (1933) 1586; McQuoid-Mason *Privacy I* 91; Para 3.2 of this chapter.

privacy communication.[879]

3.4.4 Application of basic privacy principles in the protection of the techno-legal rights in online communication

3.4.4.1 Introduction

The need to protect privacy is not only common with human beings but with animals,[880] from which the reasons to protect the privacy of human beings can be drawn.

The constitutional, common and statutory[881] law provisions of the right to privacy in South Africa can, arguably, be understood from and are traceable to some interdependent and overlapping components, approaches, methods, structures, scope and contexts. The concept of 'privacy is not a value in itself', but it is recognised 'for instrumental' and protectional purposes in other personality values, which can be enforced as a set of primary interests or rights on their own.[882]

Generally, the right to privacy, arguably, protects and encompasses the scope and contents of the existing values, interests in, and rights to: a) personhood,[883] human dignity[884] and

[879] See paras 2.2.2 and 2.3.1 -2.3.3 of Chapter 2 and paras 3.5.7.2 - 3.5.7.14, 3.8, 3.9 and 3.10 of this chapter.

[880] Mills B 'Why we should consider the privacy of animals' https://www.theguardian.com/commentisfree/cif-green/2010/apr/30/animals-privacy-wildlife-ethical (Date of use:12 January, 2016.

[881] The provisions of POPIA specifically regulate personal data while the RICA protects the procedural aspects of the right to privacy. Though the Protection of State Information Bill ('PSIB') [B 6D -2010] (or 'Secrecy Bill') is still pending, it regulates the use of state information.

[882] *Bernstein v Bester NO* supra 58 and 65, *NM v Smith* supra 131-132*;* Neethling 2005 122 *SALJ* 18-19 and 22-27; Currie and De Waal *Bill of Rights* 299-300; Rautenbach 2009 3 *TSAR* 550 and 554; Sections 1(a), 7(1), 10, 12, 36(1) and 39 of the 1996 Constitution; Solove 2002 Vol. 90 *California Law Review* 1089.

[883] *State v Makwanyane and Mchunu* CCT/3/94 para 268 and 355-356 (*State v Makwanyane*); Currie 2008 3 *TSAR* 551-553; *Bernstein v Bester NO* supra 67 and 68 and *NM v Smith* supra 129- 131 and *Mistry v Medical and Dental Council* supra 25; SALRC Chapter 2 14-15 http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016; McQuoid-Mason *Privacy II* 38-3-4; McQuoid-Mason (2000) *Acta Juridica* 227 and 259 -261; Reiman J H Privacy, intimacy and personhood in Schoeman F D (ed) *Philosophical dimensions of privacy* (1984) 300 and 314 (Reimah 'Privacy, intimacy and & personhood'); Solove 2002 Vol. 90 *California Law Review* 1116.

[884] *Bernstein v Bester NO* supra 65; *National Coalition for Gay and Lesbian Equality & Others v The Minister of Home Affairs & Others* CCT 10/99 1999 1 SA paras 30, 31, 41, 42, 48 and 54 and 58 (CC) ('*Gay and Lesbian v Min of Home Affairs*'); *State v Jordan* (CCT31/01) [2002], ZACC 22, 2002(6) SA 642, 2002(11) BCLR 1117 paras 81-84; *State v Jordan* (CCT31/01) [2002], ZACC 22 paras 81-84; *The Citizen 1978 (Pty) Ltd and Another v Robert John McBride* Case CCT 23/10 [2011] ZACC 11 para 146 ('*Citizen v McBride'*); Solove 2002 Vol. 90 *California Law Review* 1116; *NM v Smith* supra 27, 48 and 50-54.

autonomy;[885] b) intimacy;[886] c) be left alone;[887] and d) limit access to the self;[888] e) control personal information and communication,[889] *inter alia*.

Although Bawa classifies these five categories of rights into two, namely, 'substantive' privacy right and 'information' privacy right. The former category of rights comprises the aforementioned first four rights on the one hand (a)-(d) and the latter category of right (e) is limited to the fifth right —privacy of communication—[890] which uniquely encompasses, protects and enforces the former rights in online communication. It is submitted that this categorisation is for purposes of examining the concept of privacy. Bawa further states that all

[885] *Mistry v Medical and Dental Council* supra 21, 23 and 25; *Bernstein v Bester NO* supra 48, 51, 65, 77, 139, 141-142,144, 147-148 and 150- 151; *NM v Smith* supra 40, 131-134, 144, 146; *F v Min of Safety* supra 104 and 106; State Security Agency: National Cybersecurity Policy Framework for South Africa No. 609 Government Gazette No 39475 4 December, 2015 at paras 1(of p 5), 1.2, 1.7, 2.1 and 8.1 ('National Cybersecurity Policy Framework No 39475 of 2015'); Sections 1(a), 7(1), 10, 12, 36(1) and 39 of the 1996 Constitution; J Q Whitman 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 *Yale LJ* 1181 (J Q Whitman 'Dignity versus Liberty'); See para 2.6 of Chapter Two of this study.

[886] *Bernstein v Bester NO* supra 77; *S v A* 1971 (2) SA 293(T) 293 and 297 (*S v A*); Solove 2002 Vol. 90 *California Law Review* 1121; *F v Min of Safety* supra 91, 95, 99, 105 and 107; *Gay and Lesbian v Min of Home Affairs* supra 6, 23, 30, 116 & 118; *State v Jordan* supra 83; *NM v Smith* supra 130 and 131; *Citizen v McBride* supra 146 and *Mistry v Medical and Dental Council* supra 25.

[887] *Bernstein v Bester NO* supra 68, 76; *S v A* supra 293 and 297; Solove 2002 Vol. 90 *California Law Review* 1100, 1101-1102; Neethling 2005 122 *SALJ* 19-20; Neethling J *Law of delict* (1995) 333 (Neethling *Delict'*); *Investigating Directorate v Hyundai and Smit No*; *Olmstead v United States* 277 U.S 438 (1928) 466 and 478 ('*Olmstead'*); *Katz v United States* 389 U.S 347 (1967) 350; *F v Min of Safety* supra 65 and 104; *NM v Smith* supra 32 and 33.

[888] *Bernstein v Bester NO* supra 68. *SABC v NDPP* Case No. CCT 58/06 supra 9, 33, 50 and 83 (*SABC v NDPP*); *NM v Smith* supra 15, 39, 41- 44, 61, 80, 105, 108-109, 127 and 136; Neethling J 'The protection of the right to privacy against fixation of private facts' 2004 121 *SALJ* 519 (`Neethling 2004 121 *SALJ*); Currie 2008 3 *TSAR* 554-557; Allen A L Uneasy access: Privacy for women in free society 7 (1988) 10; Solove 2002 Vol. 90 *California Law Review* 1102-1105; Neethling *Delict* 333.

[889] *Mistry v Medical and Dental Council* supra 21, 25, 27, 28,44, 47- 48, 51; *Investigating Directorate v Hyundai* supra 16; Roos 2012 129 *SALJ* 375 and 398-402; Neethling *Delict* 333; Neethling 2005 122 *SALJ* 20; Roos *Data Protection* 355-356; *NM v Smith* supra 40- 44, 47, 48, 59, 60, 80, 101, 108, 109, 128, 131 and 136; Currie and De Waal *Rights* 30, 294-297, 300 and 302-303; Roos A 'Data protection: Explaining the international backdrop and evaluating the South African position' 2007 124 *SALJ* 400 (Roos 2007 124 *SALJ*); Currie 2008 3 *TSAR* 553-554; POPIA, more particularly Chapter 3 titled 'Conditions for lawful processing of personal information'; Sections 50-51 or Chapter VIII of ECTA titled 'Protection of Personal Information'; Sections 52-58 or Chapter IX of ECTA titled 'Protection of critical databases'; Neethling, Potgieter and Visser *Neethling's law of personality* 291-306; SALRC Chapters 1, 2 and 5 http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016); *Bernstein v Bester NO* supra 67 and 69; *State v Miller* supra 57-58 and 72; *C v Minister of Correctional Services* 1996 (4) SA 292 (T) (*C v Minister of Correctional Services*); *State v R* 2000(1) SACR 33, 39 (W); *Klein v Attorney-General*, WLD 1995 (3) SA 848, 865 (W) (*Klein v Attorney-General*); *State v Nkanbinde* 1998(8) BCLR 996(N) (*State v Nkanbinde*); *State v Naidoo* supra 46); *Protea* supra 608; *Absa v Moller* supra 2, 13 and 18; *Web Call v Botha* supra 18 and 21; NIA 'Investigations on Mr. Macozoma' 7-18 paras 18 and 29-30; *State v Agliotti* supra 135-141 and 145 -146; Currie and De Waal *Bill of Rights* 297; *S v A* supra 293 and 297; Sections 1, 16 and 22 of RICA; See section 1 of RICA for online communications and postal communications; See ECA 36 of 2005 for the regulation of broadcasting communications.

[890] Bawa *ROICA* 302.

forms of contents or information that pass through a telecommunication device are by definition categorised as 'information' privacy.[891]

It therefore follows that without the protection of 'information' privacy right, an individual may not enjoy or fully enjoy his or her right to 'substantive' privacy in online communication, neither will the contents, expressions, activities or inactivities, events and transactions in the rights in (a)-(d) be protected in online communication. This is because these two categories of privacy rights are like Siamese twins, thus the interdependence of the two categories of privacy right is inherent.[892]

3.4.4.2 The right to personhood, human dignity and autonomy in online communication

In addition to the statement that privacy is recognised for instrumental and protectional purposes in other personality values, which constitute and can be enforced as a set of primary interests on their own,[893] the interests herein include the right to personhood, human dignity and autonomy. All these interests contribute to the understanding of the components of privacy, given the enormity of data in online communication devices.[894]

Personhood begins when life begins.[895] As soon as individual life is identified in the personhood,[896] the right to human dignity follows. Personhood, as a component of privacy, protects the interests of an individual in 'becoming, being and remaining' a person[897] and the integrity of one's personality.[898]

It is submitted that an individual —regardless of his or her age (from birth), gender, sexual orientation, race, tribe, ethnicity, class, religious belief, political ideology— expects that his or

[891] Bawa *ROICA* 302.
[892] Currie and De Waal *Bill of rights* 302 – 304.
[893] *Bernstein v Bester NO* para 58 and 65, *NM v Smith* supra 131-132*;* Neethling 2005 122 *SALJ* 18-19 and 22-27; Currie and De Waal *Bill of rights* 299-300; Rautenbach 2009 3 *TSAR* 550 and 554; Sections 1(a), 7(1), 10, 12, 36(1) and 39 of the 1996 Constitution; Solove 2002 Vol. 90 *California Law Review* 1089.
[894] See paras 2.2 and 2.3 of Chapter 2 of this study and 3.5.7.2 – 3.5.7.4, 3.5.7.6 and 3.5.7.7 of this chapter. *State v Terrence Brown* supra 5; *Riley v California* and *US v Wurie* pp 3 of the Syllabus, 4, 9, 10 and 17 of the Opinion and 4 and 5 of the minority judgments of Alito J. See also para 3.2.6(h) of this study.
[895] *State v Makwayane* supra 268 and 355-356.
[896] *State v Makwayane* paras 268 and 355.
[897] Reiman Privacy, intimacy and personhood 300 and 314.
[898] Solove 2002 Vol. 90 *California Law Review* 1116.

her personhood is protected in online communication. Therefore, a day-old baby through his or her parents, guardian or next of kin or when he or she reaches the age of majority —as an alternative to the date of cause of action— has legal recourse for the infringement of his or her right to personhood in the invasion of privacy in online communication.[899]

Human dignity is the 'individual's sense of intrinsic worth or self-worth', self-respect and an affirmation and estimation of this worth or value by the public,[900] which is expected to be protected in online communication[901] as examined in the right to personhood.

The social scientists are some of the groups of philosophers who recognise the significance of the preservation of the human dignity of an individual, which includes the 'physical, psychological and spiritual well-being' of an individual.[902] Corroborated by sociologists and psychologists, the right to privacy is recognised as a fundamental human right, valuable and more advanced aspect of personality'.[903] Essentially, in both offline and online regimes,[904] every human —commencing from birth— reserves the natural right to emotions, feelings, dignity, reputation and unhindered control of personality, all of which rights are protected under the concept of privacy.[905]

Autonomy, freedom and liberty are terms which are interchangeably used. Autonomy enables an individual to choose 'how to live his life within an overall broad framework of a broader community.'[906] Freedom is an inviolable, and intrinsic constitutional value which is indispensable for the protection of dignity and many other rights in the constitution.[907] In online

---

[899] See generally Chapter 2 of this study.

[900] *Citizen v McBride* supra 146; *NM v Smith* supra 131; *Gay and Lesbian v Min of Home Affairs* supra 30, 31, 41, 42, 48 and 54 and 58. For further understanding of this right, see Solove 2002 Vol. 90 *California Law Review* 1116; *NM v Smith* supra 27, 48 and 50-54; *Gay and Lesbian v Min of Home Affairs* supra 42.

[901] See generally Chapter 2 of this study.

[902] McQuoid-Mason *Privacy I* xxxix.

[903] Neethling, Potgieter and Visser *Neethling's law of personality* 5 and 33; SALRC iv and 2.1.1 http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016).

[904] McQuoid-Mason *Privacy I* XXXIX–XL and 7.

[905] De Villiers M *The Roman and Roman-Dutch law of injuries* (1899) 24 (De Villiers *Law of injuries*); Schiffres J 'invasion of privacy-Use of plaintiff's name or likeness for non-advertising purposes' (1970) 30 *ALR* 3d 203, 212; McQuoid-Mason *Privacy I* xxxix and 260; *Universiteit van Pretoria v Tommie Meyer Films* 1977(4) SA 376 (T) 384.

[906] *NM v Smith* supra 131, 132 and 134, *NM v Smith* supra 146 and *F & Another v The Minister of Safety & Security* CCT 20/95 106 ('*F v Min of Safety'*).

[907] *Bernstein v Bester NO* supra 77, 139 and 148 and *Mistry v Medical and Dental Council* supra 25. For further understanding of this right, see *Bernstein v Bester NO* supra 48, 51, 141 and 147; *NM v Smith* supra 40, 144, 133; *F v Min of Safety* supra 104; State Security Agency: National Cybersecurity Policy Framework for South

communication, there is an expectation[908] that users of online communication should be free to communicate without any fear of being trapped or conscripted.[909]

3.4.4.3 Right to intimacy in online communication

The right to intimacy is an inviolable right.[910] Protection of privacy entitles an individual to share or not share information about his or her actions, beliefs or emotions.[911] The right to privacy empowers an individual to take a decision in controlling personal matters relating to the human body, procreation, marriage, family relationships, contraception, childbearing, education, possession of pornography, sexual relationship, prostitution and the practice of sodomy.[912] Similarly, in this context, a user of an online communication expects the protection of the right to intimacy listed above in online communication.[913]

3.4.4.4 Right to be left alone in online communication

The right to be left alone as espoused by Warren and Brandeis[914] requires a reasonable expectation of privacy[915] that an individual is left alone by the public,[916] particularly the powerful media.[917] An individual can protect himself including his personal affairs from the scrutiny of the public and undesirable persons.[918] The Constitutional Court in *Investigating*

Africa No 609 Government Gazette No 39475 4 December, 2015 at paras 1(of p 5), 1.2, 1.7, 2.1 and 8.1 ('National Cybersecurity Policy Framework No 39475 of 2015').

[908] *Bernstein v Bester NO* supra 65, 74, 75, 76, 78, 85 and 93.

[909] See generally Chapter 2 of this study, more particularly para 2.3.

[910] *Bernstein v Bester NO* supra 77.

[911] Solove 2002 Vol. 90 *California Law Review* 1121.

[912] *F v Min of Safety* supra 91, 95, 99, 105 and 107; *Gay and Lesbian v Min of Home Affairs* supra 6, 23, 30, 116 & 118; *State v Jordan* supra 83; *Osborne v Ohio* 495 US 103,110 SCt 1691 (1990) (*Osborne v Ohio)*; McQuoid-Mason *Privacy II* 38-23. Cameron E 'Sexual orientation and constitution: A test case for human rights' (1993) 110 *SALJ* 450 and 464; Keeton W P et al. *Prosser and Keeton on the Law of torts* 5 ed. (1984) 866 - 7 (Keeton et al. *Law of torts*); McQuoid-Mason *Privacy I* 99. For further understanding of this right, see *Bernstein v Bester NO* supra 77 and *NM v Smith* supra 130 and 131; *Citizen v McBride* supra 146 and *Mistry v Medical and Dental Council* supra para 25; Solove 2002 Vol. 90 *California Law Review* 1121.

[913] Dlulane B 'Sharing sex video a violation of Malusi Gigaba's privacy' https://ewn.co.za/2018/10/28/people-who-share-malusi-gigaba-sex-video-could-get-in-trouble-with-the-law (Date of use: 27 April, 2019 (Dlulane https://ewn.co.za/2018/10/28/people-who-share-malusi-gigaba-sex-video-could-get-in-trouble-with-the-law (Date of use: 27 January 2019).

[914] Ruiz *Privacy in Telecommunication* 24.

[915] *Bernstein v Bester NO* supra 65, 74, 75, 76, 78, 85 and 93.

[916] *Bernstein v Bester NO* supra 76. Solove 2002 Vol. 90 *California Law Review* 1101.

[917] Ruiz *Privacy in telecommunications* 24.

[918] *Bernstein v Bester NO* para 68; SALRC Chapter 2 http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016); Neethling 2005 122 *SALJ* 19-20; Neethling *Delict* 333.

Directorate v Hyundai and Smit No emphasises the 'right to be left alone' in our offices, cars or when using mobile telephones.[919]

This ratio is fashioned after the decision in the America case of *Katz v United States* which overruled the majority decision in *Olmstead v United States*[920] which refused to recognise the right to be left alone in the circumstances described herein. The right enables an individual to be left alone in a peaceful state of mind, 'thoughts, sentiments and emotions' by prohibiting 'unconsented publication', works, intellectual property, image, voice or other forms of the use of an individual's personality for purposes which are not in any way related to public interests.[921]

3.4.4.5 Right to limit access to the self in online communication

The right to limit access to the self is a situation in human life which requires seclusion from the public and publicity.[922] A user of an online communication who does not want the public to have access to him or her is protected in this context.[923]

3.4.4.6 Right to control information and communication in online communication

The right to control information and communication restricts people from gaining, publishing, disclosing or using facts or information about individuals without their consent[924] which further

---

[919] *Investigating Directorate v Hyundai and Smit No* supra 16.

[920] See *Katz v United States* 389 U.S 347 (1967) 350; *Olmstead v United States* 277 U.S 438 (1928) 466 and 478 ('*Olmstead'*); *Union Pac. Ry. Co v Botsford*, 141 U.S 250, 251 (1891); Cooley T M *Law of torts* (2ed. 1888); Solove 2002 Vol. 90 *California Law Review* 1100. For further understanding of this right; *Eisenstadt v Baird*, 405 U.S 438, 454 (1972); *Stanley v Georgia*, 394 U.S 557, 564(1969); *Doe v Bolton*, 410 U.S. 179, 213(1967); *Kent v Dulles* 357 U.S 116, 126 (1958); Warren S D & Brandies L D *The right to privacy* 4 *Harv. L Rev* 193 (1890) 196, 197, 200 and 205; Solove 2002 Vol. 90 *California Law Review* 1100, 1101-1102; *F v Min of Safety* supra 104; *Union Pac. Ry. Co v Botsford*, 141 U.S 250, 251 (1891); *NM v Smith* supra 32 and 33 and *F v Min of Safety* supra 65 & 104.

[921] Ruiz *Privacy in telecommunications* 24.

[922] *Bernstein v Bester NO* supra 68). For further understanding of this right, see *SABC v NDPP* supra 9, 33, 50 and 83; *NM v Smith* supra 15, 39, 41- 44, 61, 80, 105, 108-109, 127 and 136; Neethling 2004 121 *SALJ* 519; Currie 2008 3 *TSAR* 554-557; Allen A L Uneasy access: Privacy for women in free society 7 (1988) 10; Solove 2002 Vol. 90 *California Law Review* 1102-1105; Neethling *Law of delict* 333; Godkin E L *Libel and its legal remedy* 12 *J Soc SCI* 69, 80 (1880); Godkin E L 'The Rights of the Citizen IV-To His Own Reputation' July-Dec 1890 *Scribers Magazine* at 65; Solove 2002 Vol. 90 *California Law Review* 1103.

[923] Dlulane https://ewn.co.za/2018/10/28/people-who-share-malusi-gigaba-sex-video-could-get-in-trouble-with-the-law (Date of use: 27 January 2019).

[924] *NM v Smith* supra 131 and 136; *C v Minister of Correctional Services* 292; *S v R* 2000(1) SACR 33, 39 (W); *Klein v Attorney-General* supra 865; *Mistry v Medical and Dental Council* supra 44; McQuoid-Mason *Privacy I* 99 and 158; Chapter 12; McQuoid-Mason *Privacy II* 38-26-27.

protects two aspects of privacy as identified by the Constitutional Court in the *Mistry v Medical and Dental Council*[925] namely, 'information self-determinism'[926] and privacy of communications,[927] both of which overlap. However, it is submitted that the conceptualisation of the right to the SOC in this study is categorised under the right to privacy of communication. As aforementioned,[928] the right to control information and communication, in some respect, ensures the enforcement of the four categories of the sub-rights examined above.[929]

3.4.5. Special reasons for protecting the techno-legal rights in online communication

3.4.5.1. Introduction

Although the following rights exist in non-online communications, however, this segment examines the online perspective of the following rights, which constitute the sub-sets of the right to the SOC aside from the other direct and indirect sub-rights rights which are found in the other segments of this study.

3.4.5.2 Right to access online communication

The protection of the personality right is established in the offline world as an underpinning

[925] *Mistry v Medical and Dental Council* supra 47- 48.

[926] *Investigating Directorate v Hyundai and Smit No* supra 16; *Mistry v Medical and Dental Council* supra 47-48; *NM & Others v Smith & Others* supra 40-44 and 48; Roos 2012 129 *SALJ* 375; Neethling J *Law of Delict* 333; Neethling 2005 122 *SALJ* 20; Roos 'Data Protection' 355-356; see Roos 2012 129 *SALJ* 398-402; *NM v Smith* supra 40, 41, 42, 43, 44, 47, 48, 59, 60, 80, 101, 108 and 109; Currie and De Waal *Bill of rights* 30 and 303; *Investigating Directorate v Hyundai and Smit No* supra 16; Roos 2007 124 *SALJ* 400; Currie and De Waal *Bill of rights* 296-297, 300 and 302-303; Currie 2008 3 *TSAR* 553-554; This aspect of informational privacy is regulated by an Information Regulator in South Africa by the POPIA; Neethling J 'Legal protection of personal data' in *Neethling's law of personality* 267-269 (Neethling 'Legal protection of personal data'). . The provisions of the POPIA specifically deal with personal data protection; SALRC 'Privacy and Data' Chapter 1 2 and 5; *Mistry v Medical and Dental Council* supra 51; Currie and De Waal *Bill of rights* 303; Currie 2008 3 *TSAR* 554; Neethling J 'Legal Protection of Personal Data' 267-269. *Mistry v Medical and Dental Council* supra 51; *NM v Smith* supra 80; *Bernstein v Bester* supra 67 and 69, *Mistry v Medical and Dental Council* supra 21, 27, 28 and 51; Neethling J 'Legal Protection of Personal Data' 269-270; *State v Miller* supra 57-58 and 72.

[927] *Mistry v Medical and Dental Council* supra 25, 47 and *NM v Smith* supra 128; Currie and De Waal *Bill of rights* 294-297 and 302-303; *State v Nkanbinde* supra 996; *State v Naidoo* supra 46; *Protea Technology Ltd v Wainer* supra; *Absa v Moller* supra 2, 13 and 18; *Web Call v Botha* supra 18 and 21. NIA 'Investigations on Mr. Macozoma' 17-18 paras 18 and 29-30; *State v Agliotti* supra 135-141 and 145 -146; Neethling 2004 121 *SALJ* 521; *R v Holiday* supra 395; *S v A* supra 293; See ss 1, 16 and 22 of RICA for online and postal communications; See ECA 36 of 2005 for the regulation of broadcasting communications.

[928] See para 3.4.4.1 of this chapter.

[929] Paras 3.4.4.2 – 3.4.4.5 of this chapter.

concept for the protection of privacy.[930] Similarly, the equivalence of the protection of personality right in contemporary society is the right to access an online communication, which is an incidental and indispensable right in online communication as declared by the ECA, ECTA, POPIA, United Nations and other international authorities and instruments.[931]

If the right to access an online communication –as a sub right- is not adequately and directly recognised, guaranteed or protected, it is fallacious to protect the independent and other sub-rights in the right to the SOC, particularly the indispensable rights to the integrity and security of ordinary online communication, both of which are mutually inclusive. Essentially, the right to access an online communication is premised on, gives birth to or necessitates the recognition, protection and enforcement of the other or sub-rights in the SOC as generally examined in this study, more particularly the rights below.[932]

Arguably, the right to access online communication is the online communication version of the right to control information and communication in the offline world.[933] However, the right to access online communication is different from the right to control information and communication. On the one hand, the latter right is a negative right, which prohibits the intrusion into the online communication of an individual.[934]

On the other hand, the right to access an online communication is a positive right,[935] which entitles an individual to freely, domestically and internationally communicate online with individuals and public entities without which an individual will not be able to enjoy the other or sub-rights in the SOC.

---

[930] Para 3.3 of this chapter.

[931] See Chapter 14 of the Electronics Communications Act No 36 of 2005 ('ECA'); Sections 1, 6(1)(a)-(d), 7 & 38(3)(b)& (c) of ECTA for the definition of 'universal access' and its regulation; Global campaign for free expression 'Art 19 of Global campaign for free expression–statement on the right to communicate' https://www.article19.org/data/files/pdfs/publications/right-to-communicate.pdf (Date of use: 2 December 2017) (Global campaign for free expression https://www.article19.org/data/files/pdfs/publications/right-to-communicate.pdf (2 December 2017); McLeod S 'Communication rights: fundamental human rights for all' https://www.tandfonline.com/doi/full/10.1080/17549507.2018.1428687 (Date of use: 7 June 2018); UNESCO 'UNESCO launches its publication on Internet and freedom of expression' http://www.unesco.org/new/en/member-states/single-view/news/unesco_launches_in_panama_a_publication_on_internet_and_fre/ (Date of use:17 May 2018.

[932] See paras 3.4.5.3 - 3.4.5.5 of this chapter.

[933] Para 3.4.4.6 of this chapter.

[934] Para 3.4.4.6 of this chapter.

[935] *Bernstein v Bester NO supra* 76.

Although, the scope of this study does not cover broadcasting, save for purposes of comparison;[936] in 2017, the High Court criticised the National Assembly of the RSA when the public was denied access to online communication from the live TV broadcast of the presentation of State of the Nation Address by the erstwhile President of the RSA, Mr Jacob Zuma.[937] In the other parts of the world, there are reported condemnable cases of denial of access to Internet services by the governments of such countries.[938]

For example, the government of Zimbabwe shut down its internet services during the 2018 election to prevent the unofficial announcement of the results by the public —including the opposition parties— in a bid to prevent the spread of fake news and chaos in the country.[939] Consequently, one of the leaders of the opposition party was convicted for announcing the election results before the official announcement.[940]

3.4.5.3 Right to control and protect intangible, intellectual and invaluable property in online communication

One of the components of the concept of privacy is the right to protect intangible, intellectual and invaluable property,[941] which arguably in online communication, generally and contextually comprises a treasury, wealth, galaxy, an ocean and earth of data or information in online communication.

---

[936] Paras 3.5.7.1 – 3.5.7.15 of this study.

[937] *Primemedia v Speaker, National Assembly* supra 84(1)-(4).

[938] For example, Sudan, China, Venezuela, Algeria and other countries shut down their Internet services to prevent rebellion against the State, see VOA 'China Says It Shut Down 128,000 Websites in 2017' https://www.voanews.com/a/china-says-it-shut-down-128000-websites-in-2017/4199229.html (Date of use: 23 January 2018; AT 'Activists: We're shutting down Sudan government websites' https://africatimes.com/2018/12/26/activists-were-shutting-down-sudan-government-websites/ (Date of use: 3 January, 2019; Agence France-Presse 'China has shut down 13,000 websites since 2015 – Xinhua' (Date of use: https://www.rappler.com/technology/news/192173-china-shut-down-websites-since-2015 (Date of use: 7 May 2018; Mahomed R and Bendimerad R 'Venezuela shuts down Internet amid protests' https://www.aljazeera.com/news/2019/01/venezuela-shuts-internet-protests-190124124829727.html 29 January 2019.

[939] AP 'Zim High Court rules internet shutdown illegal, orders govt to restore full internet to the country' https://www.news24.com/Africa/Zimbabwe/just-in-zim-high-court-rules-internet-shutdown-illegal-orders-govt-to-restore-full-internet-to-the-country-20190121 (Date of use: 31 January 2019)

[940] Mutsaka F 'Former Zimbabwe Fin Min Tendai Biti convicted of making false election declaration' https://www.iol.co.za/news/africa/former-zimbabwe-finmin-tendai-biti-convicted-of-making-false-election-declaration-19362547 (Date of use: 12 February, 2019).

[941] Gellman and Dixon *Online privacy* 38-39.

Construing sections 14(a)-(d) and section 25(1) and (4)(b) of the Constitution together, enormous intangible, intellectual and invaluable contents and properties can be derived, enjoyed, protected and enforced in online communication. The massive data gathered about or from the entire human race relates to, amongst others, their: a) persons and homes; b) properties; (c) possessions; and d) real-time and archived communications in the compulsory uses of non-compartmentalised, non-passworded compartmentalized, interoperable, conscriptive, 'no server, no law' and inherently fiduciary relationship and risk-based online communication.[942]

In the contemporary society, the use of these categories of property in government, economic, business, social and political transactions, activities and events in online communication has become part of human life,[943] which require a greater expectation of protection[944] in online communication than in non-online communication.

The right to protect intellectual property in an online communication consists of the complex interdependent tangible and intangible rights in online content, commerce or transaction, copyright (including databases in this context), patent, trademarks, design, performance, trade secret, traditional knowledge and biodiversity.[945]

The right to protect intangible property in an online communication comprises the right to protect stocks, shares, bonds, other forms of financial assets[946] and lately electronic money — crypto-currency— or cheque[947] and many more that will be invented in future as the way to go in an online world. The right to protect invaluable property in an online communication includes the use, control and management of data in:

---

[942] Popoola *Liability of ISPs* 8, 82, 83, 162-163, 175 and 182 and para 2.; Para 3.9 of this chapter; Cassim F 'Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?' PER/PELJ 2015(18) 2 at 77; See paras 2.2 and 2.3 of Chapter 2 of this study.

[943] Section 25 (4)(b) of the Constitution; *Riley v California* and *US v Wurie* 9, 16-17 and 28 of the Opinion and p 6 of the minority decision by Alito J; Swire and Ahmad (eds.) *Part 5: Locational tracking* 245; Thompson *GPS monitoring* 250. In the U.S., cellphone users are more than the population of the U.S., Crump *Geolocational Privacy and Surveillance Act* 274.

[944] *Bernstein v Bester NO* supra 65, 74, 75, 76, 78, 85 and 93.

[945] Bainbridge D *Intellectual property* 5th ed. (2002) 3-13 (Bainbridge *Intellectual property*).

[945] Bainbridge *Intellectual property* 3-13.

[946] Bainbridge *Intellectual property* 3-13.

[947] Corbet S et al 'Cryptocurrencies as a financial asset: A systematic analysis' https://doi.org/10.1016/j.irfa.2018.09.003Get rights and content (Date of use: 28 February 2019).

a) Databases containing personal and non-personal data belonging to domestic, foreign and international private individuals, corporate entities,[948] and governments. Although the scope of this study does not cover the protection of the right to the SOC of government data, however, in practice, private or corporate entities and individuals have legal custody or possession of government or public utility data. This means that in some instances, the invaluable property right can be enforced by all, whether private or government. Therefore, the abolished intervention of government in declaring a database as a critical information infrastructure[949] did not necessarily limit the declaration of a database to the existing government databases only. It would have also limited the declaration of databases controlled, managed, and owned by private or corporate entities and individuals on behalf of government or public, where the legal, reasonable and justifiable need arises.[950]

In the case of *SAPS v Forensic Data*,[951] the court restrained SAPS from laying claim to the copyright of the computer program and adaptation of the Firearm Permit System developed by 'Forensic Data', a private entity.[952] The court held that upon an agreement concluded between the SAPS and 'Forensic Data', the latter shall provide 'an executable, unlocked copy of the old version' of the program to SAPS,[953] which recognises, protects and enforces the invaluable property ownership right of 'Forensic Data', thus, there is general protection of the right to invaluable property belonging to private and government entities;

b) Online configuration or online programmed data[954] for: i) artificial intelligence or robotic-based functionality or operation used in logistics —including automated piloted aircraft; ii) automated captained ships and submarines and driverless vehicles and trains; iii) governance, socio-economic planning and sovereign defence —including

[948] Section 57(1), (2), (3) (i) (i) -(v) & (5)(g) of CCB 2017 is now expunged in the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017. It is noted that despite the fact that the new bill abolishes the provision in CCB 2017 does not subtract from the purpose of laying down the principle herein.
[949] See generally chapters 10, 11 and 12 of CCB B6-2017, which are abolished in the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017.
[950] Section 57(1), (2), (3) (i) (i) -(v) & (5)(g) of CCB 2017 is now expunged in the Cybercrime Bill 2018 – Amendments Proposed to Bill B6-2017.
[951] *National Commissioner of South African Police & Another v Forensic Data Analysts (Pty) Ltd & Others* (*SAPS v Forensic Data*) Case number: 24570/2018 para 86.
[952] *SAPS v Forensic Data* supra 86.
[953] *SAPS v Forensic Data* supra 86.
[954] *SAPS v Forensic Data* supra 86.

nuclear and cyber warfare; iv) commerce —IoT and ATM; v) administration and management —including microchips embedded in the human body for ingress and egress purposes;

c) Wills and codicils, amongst others.

Intangible, intellectual and invaluable property has both positive and negative rights.[955] For instance, on the one hand, a music owner has the exclusive positive right to enjoy, re-arrange, alter, reproduce, perform the music as part of the positive right.[956] On the other hand, the music owner has the negative right to prevent anyone from infringing on the right in any form recognised by law.[957]

3.4.5.4 Right to a controlled online conscription in online communication

The right of a user of online communication to controlled online conscription[958] is similar to the right an individual is entitled to in controlling information and communication under the basic reasons for protecting an online communication examined above.[959] The similarity is that both rights encompass the enforcement of the other rights in the personality right without which there will not be any value or interest to communicate offline and online respectively.

Conversely, both rights are generally negative because they are enjoyed by way of prohibiting the disclosure, access, and seizure of the information gathered in offline and online communication respectively.[960]

Given the automatic technical online conscription,[961] it is argued that the right to controlled online conscription enables an online communication user to exercise the various rights in

[955] *Bernstein v Bester NO* 76; Bainbridge *Intellectual property* 3-13.
[955] *Bernstein v Bester NO* 76; Bainbridge *Intellectual property* 3-13.
[956] *Bernstein v Bester NO* 76; Bainbridge *Intellectual property* 3-13.
[956] Bainbridge *Intellectual property* 3-13.
[957] Bainbridge *Intellectual property* 3-13.
[957] Bainbridge *Intellectual property* 3-13.
[958] Para 2.3.3 of Chapter 2 of this study. The term 'controlled' is generally used in law enforcement in this context to deal with unlawful act or omission which is necessary to achieve another positive objective, see *Jwara v State* (916)/13 [2015] ZASCA 33 para 22.
[959] See para 3.4.4.6 of this chapter above.
[960] Para 2.3.3 of Chapter 2 of this study and para 3.4.5.3 of this chapter.
[961] See para 2.3.3 of Chapter 2 of this study.

online communication. Some of these rights include the right to know why and for what purpose data is being used, how and when it is being used and who is using it in online conscription.[962]

It is noted that because online conscription is technically inevitable, it seems difficult to exercise the 'right to be forgotten'[963] in an online communication context. This is a right that requires that once information has been utilised by an authority, the information should be wiped out and not be used for other purposes, which is not the case in online conscription.[964]

3.4.5.5 Right to the integrity and security of basic online communication

The right of a user of online communication to enjoy the integrity and ensure the security of general online communication is an indispensable right that protects the general interests and values in online communication[965] in the three special rights above,[966]without which the latter rights cannot be protected.

3.5 REDEFINING THE CONCEPT OF PRIVACY AS THE RIGHT TO THE SECRECY OF ONLINE COMMUNICATION

3.5.1 Introduction

This rubric redefines the concept of privacy as the right to the SOC because of the threat of privacy by the increasing technological development and broad role of the multi-purpose mass media in contemporary society.[967]

For a fact to be a secret, it means that the fact is 'kept or meant to be kept private, unknown, or hidden from all or all but a few'.[968] Secrecy means 'the keeping of secrets as a fact, habit or

[962] Currie and De Waal *Bill of rights* 303 – 304; Sections 4, 5, 8, 9, 11, 12, 13, 14, 15, 18, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 69 and 70 of POPIA.
[963] Heyink http://www.derebus.org.za/guide-protection-personal-information-act/ (Date of use: 12 January 2019).
[964] Heyink http://www.derebus.org.za/guide-protection-personal-information-act/ (Date of use:12 January 2019).
[965] Para 3.5.7.7 of this chapter.
[966] Paras 3.4.5.2 and 3.4.5.4 of this chapter.
[967] McQuoid-Mason *Privacy I* xxxix.
[968] Fowler H W & F G Fowler F G *The concise Oxford dictionary of current English* (1995) 1249; *Dunn and Bradstreet (Pty) Ltd v SA Merchants Combined Credit Bureau (Cape) (Pty) Ltd* 1968 (1) SA 209 (C); *Meter*

faculty, a state of which all information is withheld'.[969]

Despite the open or social nature of an Internet, which is likened to a shopping mall, an Internet is accessed in the secret,[970] where people use it as a diary, to disclose secrets about fantasies, family, health, political issues and hobbies and to confess little peccadilloes.[971]

3.5.2 The concept of the secrecy of *offline* communication regime in Europe and the United States

The right to secrecy originated from the 'limited right of property' in private offline communication,[972] originally stemming from the offline conception of the protection of communication of letters and other things[973] about two centuries ago in Europe[974] and lately in the U.S.[975] from which the right to the *secrecy* of *telecommunication*[976] is derived and unequivocally protected.[977] The U.S. Fourth Amendment covers only the 'secrecy of first-class mail', that is, the secrecy of sealed packages and letters.[978]

Systems Holdings Ltd v Venter and Another 1993 (1) SA 409 (W) 428 - 430 and *Van Castricum v Theunissen and Another* 1993 (2) SA 726 (T) 731-2.

[969] Id.; Oxford University Press 'Secret' http://www.oxforddictionaries.com/definition/english-thesaurus/secret; (Date of use: 6 February 2016); *Mathias International Limited & Another v Monique Baillache &Others* Case No.23347/09 para 56. (*Mathias Int. Ltd v Baillache*).

[970] Carr N 'Tracking is an assault on liberty, with real dangers' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 366 (Carr *Tracking is an assault on liberty*).

[971] Carr N 'Tracking is an assault on liberty, with real dangers' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 366 (Carr *Tracking is an assault on liberty*).

[972] Ernst M L and Schwartz A U *Privacy-The right to be let alone* (1968) 43 and 158 (Ernst and Schwartz *Privacy-The Right To Be Let Alone*).

[973] These include postal cheques- sent by post, Ruiz *Privacy in telecommunications* 61-66.

[974] Ruiz *Privacy in telecommunications* 62.

[975] Art 8 of the European Convention on Human Rights; Art 10 of the German Basic Law; *Ex-Parte Jackson*, 96 US 727 (1877); Ruiz *Privacy in telecommunications* 1-5, 15, 19, 20-22, 59-67, 70, 81-83, 86-87, 151, 171-172, 173, 175-176, 177, 179-257; Posner R A *The economics of justice* (1981) 272-273, 315 - 323; Solove 2002 Vol. 90 *California Law Review* 1105; *Katz v U.S.* 389 supra 347; *Maryland Penitentiary v Hayden*, 387 U.S 294 (1967); Sections 2510-2520 of Chapter 119 of Title 19 U.S.C; Chapter 36 of Title 50 of U.S.C; *Gloria Bartnicki and Anthony F. Kane, Jr., v Frederick W. Vopper , et al.* Nos. 99-1687, 99-1728 72 and 76; Chapter 18 U.S.C. § 2520(b) and (c); Section 1 of the Fourteenth Amendment; Silard 1966 66 *Col L Rev* 855; Section 2511(4)(a) and 2520 of Chapter 119 of Title 18 of U.S.C.

[976] Ruiz *Privacy in telecommunications* 1-5, 15, 20-23, 45-46, 59-67, 70, 81-83, 86-87, 143, 151-159, 171-172, 175-177, 179-257, 313-318 and 322-323.

[977] Ruiz *Privacy in telecommunications* 1-5, 15, 19-23, 45-46, 59-67, 70, 81-83, 86-87, 143, 151-159,171-172,173,175-177,179-257 and 313-323; Solove 2002 Vol. 90 *California Law Review* 1105; *Riley* and *Wurie*' paras 1-4 of the Syllabus, 4, 8, 9-10 and 17-21, 24 and 25 of the Opinion and 4 and 5 of the minority judgment of Alito J.

[978] Ruiz *Privacy in telecommunications* 172. In the U.S., new terms can be created under the right to privacy to accommodate the development in technology, thus the 'The law does not object to new concepts', Ernst and Schwartz *Privacy-The right to be let alone*155 and 158.

In the concept of the secrecy of a letter, there must be an objective expectation of secrecy by ensuring that the letter or item is in a wrapped or closed form.[979] The expectation extends to the fact that until an addressee opens up a letter, the delivery of a letter in a mailbox or dropping off mail at the floor of a locked office still places the duty of care on the Post Office.[980] However, where a mail is placed on the desk of a recipient, the duty of care is taken away from the government as the agent of offline privacy communication.[981]

3.5.3 The concept of the secrecy of *offline* communication in South Africa

In the RSA, the erstwhile Post Office Act[982] and RICA lay the foundation for the protection of the right to the secrecy of an offline communication by prohibiting the invasion of privacy of the contents of a telegram or sealed letter in transit, which has always been regarded as prima facie —strict liability—[983] invasion, which constitutes a criminal offence.[984] Aside from the foregoing, strict liability is also imposed on the press for offline invasion of privacy.[985]

The Constitutional Court, Supreme Court of Appeal and High Court expressly or impliedly recognise the value of the secrecy of offline communication and other offline personality values,[986] but these courts do not expressly and unequivocally recognise the protection of the right attached to the value of the secrecy of an offline communication as described below.

Contrary to the position of South African courts on offline communication secrecy, the SALRC and scholars posit that section 14 of the Constitution may give rise to new and '*transformative*' *sets* of '*personal interests*' in privacy, the protection of which may be against the state.[987] It is

[979] Ruiz *Privacy in telecommunications* 151-154.
[980] Sloan *Law of privacy in a technological society* 52.
[981] Sloan *Law of privacy in a Technological Society* 52.
[982] Post Office Act No 44 of 1958.
[983] McQuoid-Mason *Privacy II* 38-20.
[984] Section 51 of RICA; McQuoid-Mason *Privacy I*' 143-144; *Smith* supra 153.
[985] McQuoid-Mason *Privacy I* xxxix and 260.
[986] *NM & Others v Smith & Others* 2007 7 BCLR 751 (CC) paras 136, 137, 143 and 204 (*Smith*); *Bernstein v Bester NO* supra 3; *Mistry v Medical and Dental Council* supra 45; *Powell v Van der Merwe* supra 51; *Goqwana v Minister of Safety NO & others* (20668/14) [2015] ZASCA 186 para 19(*Goqwana*); *South African National Roads Agency Limited v The City of Cape Town and others* case no. 6165/2012 paras 3 and 3; *SAA v BDFM Publishers (Pty) Ltd* Case No. 2015/33205 para 50; *SABC v Avusa Limited & Others* 2010 (1) SA 280 (GSJ) paras 3, 13 and 26; *Smith* supra 132 and 133.
[987] McQuoid-Mason *Privacy II* 38-19 to 38-20; SALRC 1.2.24, 1.2.26(b) and (d), 1.2.31, 2.1.23 -2.1.24, 2.2.8 - *2.2.10*, 2.2.14, 2.3.26 (footnote 117) http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016.

submitted that one such protection of personal interest is the protection of the right to offline secrecy, which is against the State in the conduct of an investigation.

In general terms, it is submitted that if the phrases 'strong privacy', 'personal privacy', 'highly personal' matter and 'confidential interest' may not be used to effectively describe the concept of offline secrecy, then the phrase 'wholly inviolable inner self'[988] may reasonably and justifiably describe the concept of secrecy in general terms.

Furthermore, it is alternatively argued that the former phrases may only literally be elevated to describe the concept of 'confidentiality' while the meaning of the latter phrase 'wholly inviolable inner self'[989] goes beyond the meaning of the concepts and levels of 'privacy' and 'confidentiality' in the information hierarchical approaches and proceeds into the 'secrecy' level.[990]

It is submitted that the use of the words 'strong' and 'personal' in the respective phrases 'strong privacy' and 'personal privacy' may only elevate the protection of personality right[991] in privacy from the entry-level of 'privacy' to the next level which is 'confidentiality' level.[992] The use of the word 'interest' in the phrase 'confidential interest' does not elevate the concept of 'confidentiality' to 'secrecy' or 'top secrecy'[993] but merely describes 'confidentiality' with an adjectival phrase. Confidentiality protects the 'potential harmful effect that may result from the *indiscriminate* and unauthorised disclosure' of confidential information.[994]

It is submitted that although the phrase 'wholly inviolable inner self' does not refer to 'privacy' or 'confidentiality' nor connote any meaning close to 'privacy' or 'confidentiality', the closest meaning of the phrase 'wholly inviolable inner self' is arguably the concept of 'secrecy' of information. Classifying the phrase 'wholly inviolable inner self' at the secrecy level[995] is in pursuance of the application of the principle of a subjective expectation of privacy

[988] *Bernstein v Bester No* supra 2 and 57-59; *NM v Smith* supra 40, 80, 130 and 135; *Mistry v Medical and Dental Council* supra 8, 22, 23, 25, 27 and 30.
[989] *Bernstein v Bester No* supra 2 and 57-59; *NM v Smith* supra 40, 80, 130 and 135; *Mistry v Medical and Dental Council* supra 8, 22, 23, 25, 27 and 30.
[990] See para 3.4.3 of this chapter.
[991] Para 3.3 of this chapter.
[992] See para 3.4.3 of this chapter.
[993] See para 3.4.3 of this chapter.
[994] *NM v Smith* supra 41-42. Italic mine. *Kaunda v President* supra 11. *Bernstein v Bester No* supra 17, 24 and 35.
[995] See para 3.4.3 of this chapter.

continuum.[996] This principle gives an individual the right to determine what information to disclose to the public and the right to the reasonable expectation that such disclosure is respected by society.[997] '…Individuals have very different comfort levels when it comes to revealing personal information, so a state-mandated, one-size-fits-all online privacy regime would be worse than the *status quo*'.[998]

Therefore, it is submitted that an individual is at liberty to place information at the 'wholly inviolable inner self', which may best be located at the 'secrecy' level.

Although privacy is generally and specifically protected in section 14 of the Constitution and in common law,[999] the Constitutional Court jurisprudence has always applied a generous approach to the concept of privacy,[1000] in which this study submits could be construed to mean the secrecy of offline communication if expressly pronounced below.

The Constitutional Court describes privacy as the right of an individual to choose the value of what to disclose to the public in the offline world.[1001] An individual has the power to a **'**defined' and 'closed' —or qualified— form of privacy value even where a statute compellingly requires testimony from an individual[1002] which was earlier undisclosed.[1003] In a way, this emphasises that an information value is considered secret because an individual has the right to keep such private information confidential.[1004]

The Constitutional Court in *Mistry v Medical and Dental Council* observes that anyone, who in the course of conducting an investigation, comes across a secret fact shall preserve and not

---

[996] *Investigating Directorate v Hyundai and Smit No* supra 16; *Bernstein v Bester No* para 68; Para 3.6.2 of this chapter.
[997] *Investigating Directorate v Hyundai and Smit No* supra 6; *Bernstein v Bester No* para 68; Para 3.6.2 of this chapter.
[998] The Economist *Online privacy* 357.
[999] *Mistry v Medical and Dental Council* supra 24; *Curtis v Minister of Safety and Security and Others* 1996 (3) SA 617 (CC) para 106(); Currie and De Waal *Bill of rights* 294-295; McQuoid-Mason *Privacy II* 38-19.
[1000] *Bernstein v Bester NO* supra 12, 58, 67, 68, 70, 72, 73 and 90; *Smith* supra 41, 136, 139 and 140; SALRC 2.1.20- 2.1.22 and 2.2.7 http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016); *Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others* 2008 (2) SACR 421 (CC) para 75 (*'Thint v NDPP'*); *Ferreira v Levin Others CCT* No 5/95 para 259 (*Ferreira v Levin*).
[1001] *Investigating Directorate v Hyundai and Smit No* supra 16 and *NM v Smith* supra 136. *Bernstein v Bester NO* supra 89.
[1002] *Bernstein v Bester No* supra 34. See also *SABC v NDPP* supra 50 and 51.
[1003] *Bernstein v Bester No* supra 39; *Deliwe Muriel Njongi v Member of the Executive Council, Department of Welfare, Eastern Cape* CCT 37/07 [2008] ZACC 4 para 20 (*Njongi v MEC*).
[1004] *Bernstein v Bester No* supra 39, 43 and 56.

disclose such secret fact to anyone.[1005] However, such secret fact can only be disclosed concerning the commission of an offence under the relevant Act or order of the court to five categories of officials namely: the registrar, president, council, designated professional board and OPP.[1006] This case arguably highlights the value in offline secrecy of communication, a bit short of expressing the protection of the direct and independent right to the secrecy of offline communication.

An individual has the right not to give 'blanket consent' to the disclosure of a private fact[1007] because consent to disclose should not be assumed. Privacy is measured by the number of people in possession of the knowledge of a private fact.[1008] A private fact is still a secret where a small number of people know of the existence of such fact.[1009] To take the private fact away from the private level, there must be an extensive, full, objective and genuine disclosure by an individual who controls the fact.[1010] An individual has the right and personal choice to decide under what circumstances to disclose and to whom to disclose his or her information.[1011]

A third party is expected to take sufficient steps to ascertain the 'unlimited consent' given by the individual before disclosing a private fact.[1012] It is always advisable that if a third party is unable to ascertain an unlimited consent, that third party should rather be on the side of caution by refraining to publish undisclosed information than disclosing such private facts.[1013] The caution by that third party is to prevent some damning and irreparable consequences from happening to an individual whose private facts would have been exposed to the public,[1014] thus recognises the value of secrecy but does not expressly recognise the associated and definite right to secrecy.

The concept of offline secrecy protects privacy in the public space. For example, in *SABC v NDPP*,[1015] the Constitutional Court, by agreement of parties, extended the protection of secrecy

[1005] *Mistry v Medical and Dental Council* supra 45. Italics mine.
[1006] *Mistry v Medical and Dental Council* supra 45. Italics mine.
[1007] *NM v Smith* supra 39 and 105-109.
[1008] *NM v Smith* supra 143 and 158.
[1009] *NM v Smith* supra 143 and 158.
[1010] *NM v Smith* supra 15 and 143.
[1011] *NM v Smith* supra 136.
[1012] *NM v Smith* supra 60, 61, 101 and 105. *Bernstein v Bester No* supra 39 and 43 and *Mistry v Medical and Dental Council* supra 34.
[1013] *NM v Smith* supra 60, 61, 101, 103 and 109.
[1014] *NM v Smith* supra 63, 103, 111-112 and 137-138.
[1015] *SABC v NDPP* supra 50 and 51. See also *Bernstein v Bester No* supra 34.

to the accused person in a criminal trial by holding that 'trials and parts of trials may be, and often are, held behind closed doors to protect the privacy or security of witnesses', accused persons and family members.[1016]

This type of agreement is permissible under the CPA.[1017] In America, a trial may be conducted *in camera*.[1018] Also, where a minor is involved or where grave immorality is in issue in a trial,[1019] the value in secrecy is protected.
In describing secrecy from the government perspective, it concerns itself with the exercise of its legitimate power to prohibit certain official information and secrets from being disclosed.[1020]

The concept of professional secrecy in the RSA also assists in understanding the general concept of secrecy. The professional privilege of secrecy between an attorney and a client —as opposed to the general concept of privacy— is that during and after the briefing, a lawyer is, by ethical duty —whether inside or outside a court— forbidden from voluntarily disclosing the secret and evidentiary privilege of a client to anybody or court for personal or official benefit save in circumstances permissible by law.[1021] This ethical duty extends to the clerks, stenographers and other employees of a lawyer who have the knowledge or come across such client's information.[1022] This is because the concept of offline secrecy is used in protecting risky subject matters that may suffer great harm if a breach occurs.[1023]

In applying the specific morality of the concept of the professional privilege of secrecy above[1024] —as opposed to the concept of privacy— it means that the general concept of secrecy —whether offline or online— prohibits the disclosure of communication made between parties to third parties.

[1016] *SABC v NDPP* supra 9, 50 and 51.
[1017] Sections 152-154 of CPA No. 51 of 1977.
[1018] Mathews A S 'State secrecy' in Oosthuizen G C et al (eds.) *Professional secrecy in South Africa* (1983) 44 (Mathews *State secrecy*).
[1019] *F v Min of Safety* supra 1 and 5.
[1020] *Bernstein v Bester No* supra 73; Mathews *State secrecy* 36.
[1021] Strauss S A 'Legal professional privilege' in Oosthuizen G C et al (eds.) *Professional secrecy in South Africa* (1983) 26 (Strauss *Legal professional privilege*). Italics mine; Sloan *Law of privacy in a technological society* 54.
[1022] Sloan *Law of privacy in a technological society* 79.
[1023] Mathews *State secrecy* 43.
[1024] Strauss *Legal professional privilege* 26.

In summary, even where the privacy jurisprudence in the RSA does not expressly subscribe to or precisely use the same or related term 'secrecy', there is an indication that the court may not dismiss the concept of secrecy where reasonable, rational and justifiable.

3.5.4 The concept of the secrecy of *online* communication regime in Europe and the United States

The right to the secrecy of telecommunication is a right under the general right to privacy which can be enforced against the State[1025] and private individuals or third parties including corporate entities in the U.S. as a statutory right.[1026] In Europe, the European Union instruments regard the right to the secrecy of telecommunication as an independent or autonomous right against the power of the state.[1027] However, the protected scope of the right to secrecy is not defined in ECHR and German Basic Law.[1028] The right to the SOC in Germany is seen as a participatory right which is essential for the protection for the right to participate in democracy.[1029] At the OECD Guidelines, it recognises the right to the SOC in the formulation of national cryptographic policies as opposed to the general right to privacy.[1030]

This study submits that privacy is a positive right[1031] which protects or 'deals with voluntarily supplied information' of an individual while secrecy is a negative right which prohibits the 'clandestine wiretapping, surveillance or electronic eavesdropping operations.'[1032] It is further argued that as opposed to the positive right to offline privacy which 'protects certain secrets',[1033] the right to 'secrecy' is an independent and negative right which 'guards against the disclosure' of such information.[1034]

[1025] Ruiz *Privacy in telecommunications* 62.
[1026] Ruiz *Privacy in telecommunications* 2-3, 19 and 315-323. Sections 2510-2520 of Chapter 119 of Title 19 U.S.C; Chapter 36 of Title 50 of U.S.C; *Gloria Bartnicki and Anthony F. Kane, Jr., v Frederick W. Vopper, et al.* Nos. 99-1687, 99-1728 72 and 76; Chapter 18 U.S.C. § 2520(b), (c); Section 1 of the Fourteenth Amendment; Silard 1966 66 *Col L Rev* 855; Ruiz *Privacy in telecommunications* 315-318 and 322-323.
[1027] Ruiz *Privacy in telecommunications* 62, 313- 314. See ss 201(3), 202 and 354(5) of the Germany Criminal Code.
[1028] Ruiz *Privacy in telecommunications* 179-257.
[1029] Ruiz *Privacy in telecommunications* 19.
[1030] HIPCAR *Interception of communication: 'Model policy guideline & legislative text* 2012 at 12-13 ('ITU 'HIPCAR Interception of communication').
[1031] *Bernstein v Bester NO supra* 76.
[1032] Sloan *Law of privacy in a technological society* 24.
[1033] Mathews *State secrecy* 36 and 40.
[1034] Mathews *State secrecy* 36 and 40; Strauss *Legal professional privilege* 25.

There are pros and cons to the debate the protection of the right to the secrecy of online communication in this study.

One of the arguments against the recognition and protection of the right to the SOC is found in the statement of Judge Parker of the Court of Appeal of New York who unequivocally stated that the right to privacy is not a right that should be respected.[1035] This is corroborated by some groups who regard the concept of secrecy of communication as total secrecy of information, which is meant to hide information away from the society, therefore the concept should not be legitimised.[1036] Drawing on the U.S. privacy jurisprudence, the Fourth Amendment is premised on the fact that complete secrecy is practically impossible or unachievable.[1037]

In addition, whether or not a matter remains secret to some extent or people, it is unreasonable for an individual to expect any secrecy since there is no total secrecy in the activities involving telecommunications[1038] under which online communications fall. In other words, it is believed that secrecy is an impossibility in telecommunications.[1039]

The views of these scholars oppose the need or desire to conceal or withhold discreditable and harmful facts about an individual concerning the past, present and future plans because of the individual who fears that such information may be used against him or her.[1040] Hence, in the United Kingdom and the U.S., the school of thought against the concept of secrecy of an online communication believes that where there is the public interest to disclose information, an individual should not be allowed to rely on the right against self-incrimination, which protects an individual from being compelled to answer self-incriminating questions put to an interviewee by LEAs.[1041]

[1035] Ernst and Schwartz *Privacy-The right to be let alone* 124.
[1036] Solove 2002 Vol. 90 *California Law Review* 1107-1108.
[1037] Stuntz W J Privacy's Problem and the law of criminal procedure, 93 *Mich. L. Rev* 1016, 1022 (1995); Solove 2002 Vol. 90 *California Law Review* 1107.
[1038] Ruiz *Privacy in telecommunications* 172.
[1039] Ruiz *Privacy in telecommunications* 59 and 172; Solove 2002 Vol. 90 *California Law Review* 1109.
[1040] Posner R A *Economic analysis of law* 46 5 ed. (1998) 46, 234 and 271; Jourard S M 'Some psychological aspects of privacy' 31 *Law & Contemp. Prob.* 307 (1966).
[1041] *Bernstein v Bester No* supra 26 -28 and 39, *Re Arrows Ltd (No 4) Hamilton v Naviede* [1994] 3 All ER 814 (HL), *Bishopsgate Investment Management Ltd v Maxwell* [1992] 2 All ER 856 (CA) and Solove 2002 Vol. 90 *California Law Review* 1107-1108.

In the U.S., some schools of thought believe that the right to the SOC is a private or individual interest which should not supersede the protection of the broader democratic and public interests in the society, therefore, the value in an online communication should not be protected as a right to the SOC but under the broader right to privacy.[1042]

However, one of the arguments for the protection of the right to the SOC is that given that the right to privacy is too broad to take special cognisance of the uniqueness of the nature and features of online communication —in contrast with other channels of privacy communications—[1043] the right to the SOC is in pursuance of the recognition of the right to secrecy of telecommunication in Europe and the U.S.[1044] In telecommunication, the quantitative capacity of online communication devices[1045] enables the transmission and storage of enormous data in online communication than in the analogue world.[1046]

Additionally, the quantity of data in online communication is exposed to greater risks than the information in the other channels of data communications.[1047] The higher risk levels in online communication are informed by the risky nature and features of digital data[1048] and the increasing invention of new online technologies, which pose serious harm to the protection of communications held in private and those accessible to the public.[1049]

The argument for the protection of the concept of the SOC is in pursuance of the decision of the court on the protection of information in online communication, which is by a technical default, conscripted in online communication.[1050] According to the US Supreme Court in *Riley*

[1042] Ruiz *Privacy in telecommunications* 19.
[1043] Ruiz *Privacy in telecommunications* 2-3 and 45-46.
[1044] Ruiz *Privacy in telecommunications* 1-5, 15, 20-23, 45-46, 59-67, 70, 81-83, 86-87, 143, 151-159, 171-172, 175-177, 179- 257, 313-318 and 322-323.
[1045] Ruiz *Privacy in telecommunications* 2-3 and 45-46. In *Riley v California* and *US v Wurie* supra 3 of the Syllabus and 19 of the Opinion, the court identified both *quantitative* and *qualitative* capacities of cell phone in contrast with analogue devices.
[1046] Ruiz *Privacy in telecommunications* 2-3 and 45-46. *Riley v California* and *US v Wurie* supra 3 of the Syllabus, 4, 9, 10 and 17 of the Opinion and 4 and 5 of the minority judgment of Alito J. See also para 3.5.7.2, 3.5.7.3, 3.5.7.4, 3.5.7.6 and 3.5.7.8 of this chapter.
[1047] Ruiz *Privacy in telecommunications* 2-3 and 45-46. See paras 3.5.7.2, 3.5.7.3, 3.5.7.4, 3.5.7.6, 3.5.7.8 of this chapter on the examination of these channels. See the Supreme Court of the United States consolidated cases of *Riley v California* and *US v Wurie* supra 3 of the Syllabus, 4, 9 -10, 17, of the Opinion and 4 and 5 of the minority judgment of Alito J.
[1048] See paras 3.5.7.2, 3.5.7.3, 3.5.7.4, 3.5.7.6, 3.5.7.8 of this chapter.
[1049] *Riley v California* and *US v Wurie* supra 9-12, 17-20 and 25 of the Opinion; Ruiz *Privacy in telecommunications* 2-3 and 45-46; National Cybersecurity Policy Framework No 39475 of 2015 paras 2 (of p 5), 1.3 and 1.7.
[1050] See para 2.3.3 of Chapter 2 of this study.

v California and *US v Wurie*, the court held that an offline mobile cellular telephone —which is a mini computer— collates, and collects from many distinct types of information.[1051] According to the court, a cell phone reveals a combination of information in text, audio, video, animation etc., into one form of information, which has significant 'several interrelated privacy consequences' than any previously isolated form of information in the analogue world.[1052]

The court further held that the qualitative capacity of online communication devices enables the recording, reconstruction and revelation of minute-by-minute communication, transaction, movement, location, history of online personal and behavioural interests, family, political, professional, religious, sexual and health matters, amongst others[1053] which 'can date back for years'.[1054] According to the features of the U.S. 'closed container' doctrine, an online communication device is a sealed container, which stores complex and multiple data, which is accessed by the execution of a search warrant.[1055]

Drawing on the U.S. literature on privacy, scholars support the concept of SOC in which 'privacy interest is the selective disclosure of facts'[1056] and the '*concealment of personal information or facts*'[1057] away from 'some people but not accountability to others.[1058] Besides, the concept of the SOC is also protected as the 'zone of privacy'[1059] through which the

[1051] *Riley v California* and *US v Wurie* supra 3 of the Syllabus, 4, 9 -10 and 17 of the Opinion and 4 and 5 of the minority judgment of Alito J.

[1052] *Riley v California* and *US v Wurie* supra 1-4 of the Syllabus, 4, 8, 9 -10, 17 -21, 24 and 25 of the Opinion and 4 and 5 of the minority judgment of Alito J.

[1053] *Riley v California* and *US v Wurie* supra 3 of the Syllabus and 19- 20 of the Opinion.

[1054] *Riley v California* and *US v Wurie* supra 3 of the Syllabus.

[1055] Rosen J 'The Supreme Court's cell phone case went even further than privacy advocates had hoped' http://www.newrepublic.com/article/118396/supreme-court-cellphone-case-went-further-privacy-advocates-hoped (Date of use: 30 June 2014) (Rosen http://www.newrepublic.com/article/118396/supreme-court-cellphone-case-went-further-privacy-advocates-hoped (Date of use: 30 June 2014); Van der Berg J 'Mobile phone evidence: implications for privacy in South African law' http://ohrh.law.ox.ac.uk/mobile-phone-evidence-implications-for-privacy-in-south-african-law/ (Date of use: 25 June 2013) (Van der Berg http://ohrh.law.ox.ac.uk/mobile-phone-evidence-implications-for-privacy-in-south-african-law/ (Date of use: 25 June 2013). In *People v Diaz* Cal Rptr. 3d 105, 2011, the Supreme Court of California affirmed the judgement of the Court of Appeals denying the motion to suppress evidence obtained without warrant from the cell phone of Diaz upon lawful custodial arrest. However, in the latest case of *Riley v California* 573 U.S 2014, the Supreme Court unanimously held that 'police generally may not, without a warrant, search a digital information on a cell phone seized from an individual who has been arrested.

[1056] Karst K L 'The files': Legal controls over the accuracy and accessibility of stored personal data 1966 31 *Law & Contempt Probs* 342, 344.

[1057] Italics mine; Posner *The economics of justice* 272-273; Solove 2002 Vol. 90 *California Law Review* 1105; Shils E Privacy: Its constitution and vicissitudes, 1966 31 *Law & Contemp. Probs*., 305; Solove 2002 Vol. 90 *California Law Review* 1108.

[1058] Solove 2002 Vol. 90 *California Law Review* 1108.

[1059] In Estonia, the right to secrecy of communication is guaranteed, Osula A *Remote Search and Seizure of Extraterritorial Data* 57 and 58 (PhD thesis University of Tartu, Estonia 2017). (Osula *Remote Search and*

enormous quantitative and qualitative digital data components are accessed or stored in online communication devices.[1060]

3.5.5 The common law jurisprudence on the secrecy of *online* communication regime in South Africa

The Constitutional Court has not expressly recognised or dealt with nor categorically pronounced on the concept of the SOC.[1061] However, the decision of the Constitutional Court in *NM v Smith* expresses concern and remedy over the enormous risks involved in the use of online or mechanical devices, which have the capacity of instantaneously reaching out to many people in the communication of private facts.[1062] The involvement of enormous risks implies that data online communication deserves a higher level of privacy protection than data in non-online channels of communication.[1063]

Given that this study establishes the existence of online conscription,[1064] which is one of the reasons for or features of the protection of the concept of the SOC, the Supreme Court of Appeal contradicts itself on the application of conscription in online communication, thus, denies the existence of the concept of the SOC in this regard. Although the Supreme Court of Appeal held that there was an unlawful tapping of a telephone line in *State v Pillay* in terms of the conscriptive feature in one breath,[1065] it, however, in another breath, unequivocally pronounced and contradicted itself on the non-existence of online conscription in this case[1066] as demonstrated in the following quotes.

The duo of Mpati DP and Motata AJA *State v Pillay* demonstrates the existence of online conscription as follows:

Seizure of Extraterritorial Data); Solove 2002 Vol. 90 *California Law Review* 1106; *Whalen v Roe* 429 U.S 589 (1977) 599-600.

[1060] *Riley v California* and *US v Wurie* supra 3 of the Syllabus and 19 of the Opinion.

[1061] SALRC 2.4.3 http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016).

[1062] *NM v Smith* supra 128.

[1063] See paras 3.5.7.6 and 3.5.7.8 of this chapter.

[1064] See para 2.3.3 of Chapter 2 of this study.

[1065] *State v Pillay* supra 420I.

[1066] *State v Pillay* supra 447D-F.

> ‘‘As has been mentioned above, the State conceded in the Court *a quo*, and so did counsel for the State in this Court, that *evidence of the contents of accused 10's statement that led to the discovery of the money is inadmissible* in view of the fact that accused 10 was induced by the promise that she would be used as a State witness and would not be prosecuted (for any offence, obviously) to say where the money was. [1067]…there was no doubt that the money found in the ceiling of the house of accused 10 had been found as a result of a violation, firstly, of her *constitutional right to privacy*, in that her *private communications had been illegally monitored following the unlawful tapping of her telephone line*…[1068]

The duo of Mpati DP and Motata AJA unequivocally held in *State v Pillay* that online conscription occurred via the telephone communication of accused no 10 and at the same time the court contradicted itself directly or indirectly as follows:

> ‘…….while evidence derived (real or derivative evidence) from conscriptive evidence (i. e. self-incriminating evidence obtained through a violation of a constitutional right) could be excluded on grounds of unfairness if it was found that but for the conscriptive evidence the derivative evidence would not have been discovered, *the information sourced from the illegal monitoring of accused 10's telephone line, which ultimately led to the discovery of the robbery money in her house, was not conscriptive evidence…it had not mattered whether the officers who had done the actual monitoring and who acted on the information gained from the illegal monitoring had been unaware of the fact that monitoring had been done improperly*. *That they might not have known of the illegality of the monitoring did not make the infringement less serious*. It had been conceded that other means of investigation had been available to them; surveillance of the suspects' houses being one. *To allow the impugned evidence derived as a result of a serious breach of accused 10's constitutional right to privacy might have created an incentive for law enforcement agents to disregard accused persons' constitutional rights* since, even in the case of an infringement of constitutional rights, the end result might be the admission of evidence that, ordinarily, *the State would not have been able to locate*. *That result - of creating an incentive for the police to disregard accused persons' constitutional rights - was highly undesirable and would do more harm to the administration of justice than enhance it*. *The violation of accused 10's constitutional rights had not ended with the unlawful monitoring of her private telephone communications…*’[1069]

[1067] *State v Pillay* supra 430B-C.
[1068] *State v Pillay* supra 420 H-J, 421 A and 430 E-F. Italics mine.
[1069] *State v Pillay* supra 421 A-G. Italics mine.

A further contradiction of the Supreme Court of Appeal on the existence of online conscription is as follows:

> '…The real evidence admitted by the Court *a quo* in the present case was the discovery of the money concealed in the roof. That discovery would not have been made *but for the monitoring of the telephone conversation. But the telephone conversation would have taken place whether it was monitored or not. It was not created by the infringement, nor was there any question of compulsion*…'.[1070]

The denial of the existence of online conscription in *State v Pillay*[1071] is either an express or implied way of denying the existence of the value of and right to the SOC. This is because automatic online conscription occurs immediately an online communication is activated, which exposes data to high-level risks, necessitating the protection of the right to the SOC. However, the High Court has made some useful, express, and implied pronouncements and concerns[1072] in the consideration of the endorsement of the concept of the SOC in *State v Terrence Brown,*[1073] *State v Agliotti,*[1074] *Absa v Moller,*[1075] *State v Miller*[1076] and *Web Call v Botha,*[1077] amongst others.

In support of the concept of the SOC, the High Court in summarising the evidence in the trial within a trial in *State v Terrence Brown* highlights the significant invaluability of the voluminous contents of a cell phone in an offline electronic communication device.[1078] These

[1070] *State v Pillay* supra 447 D-E. Italics mine.
[1071] *State v Pillay* para 447 D-E.
[1072] For example, *State v Terrence Brown* supra 27-31.
[1073] *State v Terrence Brown* supra 5 and 29.
[1074] *State v Agliotti* supra 135 - 141 and 145 – 146.
[1075] *Absa v Moller* supra 2, 13 and 18.
[1076] *State v Miller* supra 70 and 72.
[1077] *Web Call v Botha* supra 18 and 21. In the report on the illegal OCI procedure carried out on Mr. Macozoma, the finding condemned the outsourcing of OCI procedure as an unlawful transfer of intelligence function to a private entity, see NIA 'Investigations on Mr. Macozoma' 18 and 29-30.
[1078] *State v Terrence Brown* supra 6 and 7. In the U.S., 'Consider the amount of information stored on an individual's personal computer. A standard laptop today often holds many gigabytes of data, more than a mainframe computer held 20 years ago. If the government obtains access to an individual's personal computer, it is highly likely that the computer will reveal detailed and diverse records about the person's life. The records retained on that computer, in turn, are only a small subset of the records stored on other computers- banks, hospitals, online advertisers, data brokers, government agencies, and other record holders possess exponentially more detailed data on individuals than in the past. Although a few people to live ''off' the grid'', this is not a feasible option for the vast majority of citizens in developed countries. Once an individual, is identified as a target, the government-via lawful process- can access detailed information specific to that individual. We live in a golden age for surveillance'' because investigatory agencies have unprecedented access to information about a suspect. In addition, data mining provides unprecedented tools for identifying suspects', Swire and Ahmad *Golden age for surveillance* 240 -241; Para 2.2.1 of Chapter 2 of this study.

contents include the contact lists, videos, photographic images and SMSs, using various messaging formats.[1079] Persuasively, similar descriptive remarks were made in the US Supreme Court decision of *Riley v California* and *US v Wurie*.[1080] Given the invaluability of digital data, it is obvious that since some of the pieces of data described in *State v Terrence Brown* (such as video and SMS) are not the type of data that can be found in an analogue or paper diary, greater protection ought to be given to digital data than in non-digital data.[1081]

The greater protection of data in online privacy can only be guaranteed where data is kept or transmitted in secret in online communications as a channel of communication than in other channels of communication.[1082]

The query by the High Court in *State v Agliotti* of the careless release of 'sensitive data' in online privacy by a telecommunication fraud and risk manager to LEAs on the strength of improper and questionable documents and an ordinary witness subpoena —both of which do not entitle such release—[1083] is a strong indication that data in an online communication may only be adequately protected if considered as a right to the SOC.

In *Absa v Moller*,[1084] the court observed the high level of embarrassment and the 'obvious and far-reaching potential adverse implications' of the execution of an order to invade the privacy and dignity of Moller's and the third party's online communication devices which stored the 'most intimate details of a person's life'.[1085] The High Court added that the execution of the court order to search the online communication devices was 'an example of the 'outer-extreme' (or 'absolute extremity') of judicial power.'[1086] Further, given the nature of online communication which could be infringed secretly without notice to the affected individual, the court expresses concern over the 'highly invasive or oppressive nature' of an OCI that is conducted secretly.[1087]

[1079] *State v Terrence Brown* supra 5 and 6.
[1080] *Riley v California* and *US v Wurie* supra 3 of the Syllabus, 4, 9 -10, 17 and 25 of the Opinion and 4 and 5 of the minority judgment of Alito J.
[1081] *State v Terrence Brown* supra 6; Paras 3.5.7.2- 3.5.7.6 and 3.5.7.8 of this chapter.
[1082] See paras 3.5.7.2 – 3.5.7.6 and 3.5.7.8 of this chapter.
[1083] *State v Agliotti* supra 138-140 and 146.5.
[1084] *Absa v Moller* supra 2, 3, 13, 16 and 18.
[1085] *Absa v Moller* supra 2, 3, 13, 16 and 18.
[1086] *Absa v Moller* supra 3.
[1087] *Absa v Moller* supra 18.

In *State v Miller*, the High Court commended the LEO who was on the side of caution for not making available to the public or unrestrictively using the digital data found in the cell phones, which were voluntarily handed over to the LEO by the suspects.[1088] This level of caution by LEAs complies with the various Constitutional Court pronouncements on the secrecy of communication in the analogue world particularly in the case of *NM v Smith.*[1089] In *State v Miller*, one of the suspects voluntarily handed over the PIN of his cell phone to the LEA while the cell phone of the second suspect did not have a PIN, so there was unrestricted access to the data in the cell phones.[1090]

However, although there was unrestricted access to the data in the cell phones, the self-caution by LEA is an indication of great respect[1091] that goes beyond the conventional privacy protection, into the protection of the right to the SOC in the digital world.

In pronouncing on how investigations should be conducted, the High Court in *Web Call v Botha* held that a conventional method —or an ordinary, less invasive procedure such as discovery method— should have been used to establish evidence instead of embarking on an 'extremely or more intrusive' method of search of a laptop which infringes the right to privacy and dignity.[1092] Since 'extremely or more intrusive'[1093] invasion occurred during the search of a laptop (which was done in an offline electronic communication),[1094] it is submitted that more extreme and most intrusive invasion would occur in online communication during the conduct of an OCI because there is a higher risk in online communications than in non-online communications, therefore, the need to protect the concept of the SOC.

In summary, though the decisions of the High Court may not expressly be sufficient to sustain the conclusion in some quarters that South African privacy jurisprudence subscribes to the SOC, however, the description of privacy in the above contexts favourably opens up the discussion on the intent or interpretation of the decision of the courts in this regard. However,

[1088] *State v Miller* supra 72.
[1089] *NM v Smith* supra 61 and 103.
[1090] *State v Miller* supra 57 and 58.
[1091] *State v Miller* supra 72.
[1092] *Web Call v Botha* supra 5, 9, 15, 18-21.
[1093] *Web Call v Botha* supra 5, 9, 15, 18-21.
[1094] Para 2.2.1 of Chapter 2 of this study.

it is now established that the High Court unequivocally pronounced in favour of the protection of the right to the SOC in *AmaBhugane* case.[1095]

3.5.6 Synopsis of major statutes recognising the concept of the secrecy of online communication

3.5.6.1 Introduction

A synopsis of some legislations below describes or highlights the nature, components and scope of the pre-and post-techno-legal protective steps in the concept of the SOC.

3.5.6.2 Nature, components and scope of the concept of the secrecy of online communication in the Electronic Communications Act

The ECA broadly provides for the regulation of electronic communication services, amongst others, which include the technical aspects of electronic communication and broadcasting, licensing, infrastructure management etc.[1096]

The ECA generally recognises, protects and regulates, the nature, components and scope of personal data, privacy and national information database[1097] in online communication such as data, voice, sound, visual, text —including SMS— or a combination of these communications.[1098] It follows, therefore, that, to some extent, the right to the SOC is protected to the extent provided in the ECA since this is a special Act that caters for the various subject matters herein.

3.5.6.3 Nature, components and scope of the concept of the secrecy of online communication in the Electronic Communications and Transactions Act

As the title suggests, the ECTA is special legislation that generally regulates electronic communications and transactions. In particular, the ECTA recognises, protects and regulates

[1095] *AmaBhungane v Minister of Justice*.
[1096] See the preamble of the ECA.
[1097] Section 75(a), (b) and (h) of the ECA.
[1098] See section 1 of the ECA for the definition of 'electronic communication', See also section 2(q) and 5(3)(c) of the ECA.

the nature, components and scope of the broad meaning of personal information[1099] in online communication,[1100] online writing,[1101] data[1102] and critical databases in online communication.[1103]

The broad meaning of personal information identifies, covers and protects several aspects of an individual being in online communication, such as the information in the basic rights to the SOC examined in this study.[1104] Personal information that is protected in the ECTA includes pregnancy status, birth, conscience, belief, culture, sexual orientation, physical or mental health, criminal history, financial transactions, identification number, fingerprints, blood group, confidential correspondence[1105] and electronic signature.[1106]

However, it is inadequate to exclude the protection of information about someone who died twenty years earlier in time to the protection period.[1107] The inadequacy is based on the fact that deceased persons enjoy some basic rights to dignity —from which the rights to privacy and (now) SOC are derived— even after twenty years of being deceased.[1108] For example, the sexuality or sexual orientation of a deceased person need not be a subject of disclosure in an online communication if the deceased did not disclose in his or her lifetime or if there was no criminal investigation relating to the sexuality of the deceased against a living or another deceased person.

[1099] See the definition of personal information in section 1 of the ECTA; Paras 3.4.4.1- 3.4.4.6 and 3.4.5.2 – 3.4.5.5 of this chapter.
[1100] See the preamble and sections 38(3)(a) & (d) of the ECTA.
[1101] Section 12 of the ECTA which recognizes, protects and regulates one of the contents of online communication which is writing or text.
[1102] See section 1 of the ECTA for the definition of the following terminologies which are directly and indirectly used in regulating the protection of online communication: 'data'; 'data controller'; 'data message'; 'advance electronic signature'; 'authentication products or services'; 'automated transaction'; 'cache'; 'critical data'; 'critical data base'; 'critical database administrator'; 'cryptography product'; 'cryptography service'; 'data subject'; 'electronic agents'; 'electronic communication'; 'electronic signature'; 'email'; 'information system'; 'information system services'; 'intermediary'; 'Internet'; 'originator'; 'personal information'; 'third party'; 'transaction'; 'universal access'; 'WAP'; 'webpage' and 'World Wide Web'. See also sections 2(1)(a),(b), (c), (d), (e), (g), (h), (j), (k), (m), (n) and (r), 10(2)(b)(ii), 11(1) -(3), 12, 13, 14, 15, 20, 22, 23, 24, 25, 26, 27, 28, 31, 50, 51, 73, 74, 75, 76, 77, 82, 83, 84, 86, 87, 88 and 89 of the ECTA.
[1103] Sections 52 and 53 of the ECTA.
[1104] See the definition of personal information in section 1 of the ECTA; Paras 3.4.4.1- 3.4.4.6 and 3.4.5.2-3.4.5.5 of this chapter.
[1105] See the definition of 'personal information' in section 1 of the ECTA.
[1106] Section 13 of the ECTA.
[1107] See concluding statement of the definition of 'personal information' in section 1 of the ECTA.
[1108] See concluding statement of the definition of 'personal information' in section 1 of the ECTA.

Generally, the ECTA makes provision for the protection of the integrity and security of online communication in the following ways.

Firstly, there is adequacy in one of the key objects of the ECTA. The adequacy relates to the recognition, promotion and development of legal certainty and confidence in online communications and transactions[1109] which ensure that online transaction in the RSA complies with the highest international accepted technical and non-technical standards.[1110]

Secondly, there is adequacy in the object relating to the development of a safe, secure and effective environment for online consumers, businesses and government 'to conduct and use electronic transactions'[1111] which recognises, protects and regulates the right to the SOC.

Thirdly, , there is adequacy in the provision for government online services by a public body, which focuses on the appropriate control measures and procedures required for the protection of integrity and guarantee of security and confidentiality of online data communications or payments.[1112] Although this study focuses on the protection of private and corporate entities in the RSA as opposed to government online communication, however, private entities hold some private information in trust for government,[1113] therefore this provision also protects the online communication of a private individual or entity in this regard.

Fourthly, there is a provision for the preservation of confidential information gathered in Chapter XII of the ECTA, the contravention of which attracts a penalty of a maximum of six months imprisonment.[1114] However, it is submitted that this penalty —even though inadequate— should be generally applicable to the provisions that are contravened concerning the integrity and security of online communication.

Fifthly, it is a criminal offence for an unauthorised person to access, interfere with or intercept online communication or for anyone to attempt, aid or abet any of the listed offences.[1115] However, although the scope of this study does not extend to the examination of the adequacy

[1109] Section 2(1)(e) and Chapter 3 of the ECTA.
[1110] Section 2(1)(h) & (m) of the ECTA.
[1111] Section 2(1)(j) of the ECTA.
[1112] Section 28(1)(e) of the ECTA.
[1113] *SAPS v Forensic Data* supra 86; Para 3.4.5.3 of this chapter.
[1114] Section 84 of the ECTA.
[1115] Sections 86-89 of the ECTA.

of penology, the penalties for contravening the various provisions in the ECTA are inadequate.[1116]

One of the inadequacies is that given the fact that the provisions of RICA apply to the investigation of serious offences only, a reliance on paragraph 14 of Schedule 1 of RICA excludes the offences identified in the ECTA from being investigated under RICA provisions.[1117] This is because none of the penalties in the ECTA offences —with a maximum of which is 2 years—[1118] are up to the least period of punishment in the schedule of RICA which must exceed five years without an option of fine.[1119] Therefore, it is difficult to effectively enforce any breach of duty in the ECTA relating to the integrity and security of online communication under the ECTA.

In summary, it is submitted that in pursuance of the examination of the comparison of the nature, features and threshold of the risks and protection between online and non-online communication,[1120] the ECTA expressly recognises, protects and regulates the nature, contents, context and scope of online communication and relatively protects the right to the SOC. It does this by expressing the object of prohibiting the abuse of online communication system in the preamble of the Act, which is not expressly titled as such in the ECTA.[1121]

3.5.6.4 Nature, components and scope of the concept of the secrecy of online communication in the Regulation of Interception of Communications and Provision of Communication-related Information Act

One of the overarching objects of RICA[1122] generally protects the concept of the SOC in the nature, components and scope of online content and non-content data, real-time and archived

[1116] Para 6.3.3.3 of Chapter 6 of this study.
[1117] Para 6.3.3.3 of Chapter 6 of this study.
[1118] Section 89 of the ECTA.
[1119] Para 6.3.3.3 of Chapter 6 of this study.
[1120] Para 3.5.6 of this chapter.
[1121] See the preamble and section 1 of the ECTA for the various and relevant definitions of terminologies which are directly and indirectly used in regulating the protection of online communication and sections 2(1)(a),(b), (c), (d), (e), (g), (h), (j), (k), (m), (n) and (r), 10(2)(b)(ii), 11(1) -(3), 12, 13, 14, 15, 20, 22, 23, 24, 25, 26, 27, 28, 31, 50, 51, 52, 53, 73, 74, 75, 76, 77, 82, 83, 84, 86, 87, 88 and 89 of the ECTA.
[1122] RICA regulates the interception of online communication, amongst other channels of communication such as direct communication, postal services and non-on-demand communication, see the preamble to and ss 1 ('communication', 'communication related information', 'direct communication', 'entry warrant', 'indirect communication', 'postal service') of RICA. For the meaning of non-on-demand communication, see para 2.2.2.1 of Chapter 2 of this study.

data and Internet and non-Internet online-based platforms.[1123] This is done by prohibiting unlawful interception or unlawful attempted interception[1124] and provides a penalty for the failure or refusal to comply with the requirements therein.[1125]

Given that RICA is the main legislation examined in this study, the nature, components and scope of the techno-legal right to the SOC in RICA are generally reflected in the various chapters in this study, otherwise, a further examination or summary of the provisions of RICA herein will result in unnecessary duplication. In any case, though inadequate as examined in this study, RICA recognises, protects and regulates the concept, components and scope of the SOC.

3.5.6.5 Nature, components and scope of the concept of the secrecy of online communication in the Protection of Personal Information Act

The much-awaited data protection legislation, which is now enacted as the POPIA[1126] is expected to be executed simultaneously with RICA.[1127] The POPIA gives effect to section 14 of the Constitution[1128] concerning the domestic and cross-border[1129] protection of digital and non-digital records[1130] or personal information and special personal information.[1131]

Personal information is defined or described in many ways. Personal information is the information of a person that specifically relates to, or identifies a 'race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or

[1123] See section 1 ('archived communication-related information', 'contents', 'communication', 'communication related information', 'direct communication', 'electronic communication service', 'indirect communication', 'internet' and 'real-time communication-related information') of RICA.
[1124] Sections 2 and 3 of RICA directly protect the integrity and security of online communication as well as other provisions. Some provisions that protect online communication and interception directly and indirectly include the following sections 4-12, 16(1),(2)(d)&(e), (5)(a)(i), (b)(i), (c), (7)(b), (8)(b)(ii)-(iv), (9), (10), 17(1),(2)(d)(ii),(f),(g), (4), 18(1)(b), (2)(a) &(b)(i)-(iii), (3), (4)(a)&(b), 19(1),(3),(4)(a),(7) & (8), 20(1),(3), (4), 21(1)(a) &(b), (3),(4)(a)&(b), (5)(c)&(d), 23(1), 24, 25(1), 29(2)(a)-(c),(3)(b), (6)(a)-(b), (7)(a)-(c), (8)(a)& (b), 30(2)(a)(ii) and 49-50 of RICA where intercept is prohibited or permissible according to the various needs and circumstances as opposed to offline communication which is not regulated as online communication.
[1125] See sections 2- 21, 23-26, 29, 32, 37, 42, 43, 44, 45, 46, 49, 50, 51 and 54 of RICA and para 3.10 of this chapter.
[1126] Section 2 of the POPIA.
[1127] Bawa *ROICA* 325 and 332.
[1128] Section 2 of the POPIA.
[1129] Section 72 of the POPIA.
[1130] See the definition of 'record' in section 1 of the POPIA.
[1131] Section 26 of POPIA.

mental health, well-being, disability, religion, conscience, belief, culture, language, and the birth of the person'.[1132] It can also be defined as 'information relating to the education or the medical, financial, criminal or employment history of the person.'[1133]

Personal information includes 'any identifying number, symbol, o-mail address, physical address, telephone number, location information, online identifier or another particular assignment to the person'.[1134] Personal information consists of 'the biometric information of the person'.[1135]

Furthermore, personal information comprises 'the personal opinions, views or preferences of the person'.[1136] It is also the 'correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence'.[1137] Personal information represents 'the views or opinions of another individual about the person'.[1138] Finally, personal information is the 'the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person'.[1139]

POPIA also protects special personal information by prohibiting it from being processed.[1140] This type of information is information that relates to 'religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject' or criminal behaviour of a data subject relating to the alleged commission of an offence, proceedings or outcome of proceedings of an offence by or on a data subject.[1141]

There are exceptions or conditions in which personal information can be processed which include:[1142] where consent is given by the data subject; in pursuance of an obligation in

[1132]See para (a) of the definition of 'personal information' in section 1 of the POPIA.
[1133] See para (b) of the definition of 'personal information' in section 1 of the POPIA.
[1134] See para (c) of the definition of 'personal information' in section 1 of the POPIA.
[1135] See para (d) of the definition of 'personal information' in section 1 of the POPIA.
[1136] See para (e) of the definition of 'personal information' in section 1 of the POPIA.
[1137] See para (f) of the definition of 'personal information' in section 1 of the POPIA.
[1138] See para (g) of the definition of 'personal information' in section 1 of the POPIA.
[1139] See para (h) of the definition of 'personal information' in section 1 of the POPIA.
[1140] Section 26 of the POPIA.
[1141] Section 26 of the POPIA.
[1142] Sections 27(1)(f) and (2) and (3), 28, 29,30, 31, 32 and 33 of the POPIA.

domestic and international law; for proportionate and necessary public historical, statistical and research interests and purposes; where information has intentionally been made public by the data subject.[1143]

The regulation of personal information governs living and existing juristic persons.[1144] However, it is inadequate to exclude the protection of information about a deceased person.[1145] The inadequacy is based on the fact that deceased persons enjoy some basic rights to dignity and their estates are held liable even after death, more particularly in online communication which is expected to keep information in perpetuity in the respective sancta.[1146]
POPIA regulates the domestic and international flow and protection of personal information processed by public and private entities —both natural and artificial— and regulates the right of individuals in unsolicited online communication and automated decision-making process of personal information, amongst others,[1147] but the POPIA is not adequate to protect online communication.[1148]

The scope of protection of personal information of an individual is generally premised on eight principles that a responsible party who processes personal information must comply with, namely: accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation.[1149] Generally, the POPIA prohibits the interference of the protection of personal information, the breach of which entitles an aggrieved party to lodge a complaint before the Information Regulator who appropriately redresses the complaint, including embarking on the option of ADM and taking civil action against the responsible party on behalf of the data subject.[1150]
In summary, the provisions in the POPIA are generally inadequate to protect the right to the SOC.

[1143] Section 27(1)(a)-(f) of the POPIA.
[1144] See the definition of personal information in section1 of the POPIA.
[1145] See concluding statement of the definition of 'personal information' in section 1 of the ECTA, Para 3.5.6.3 of this chapter.
[1146] Paras 3.5.6.3 and 3.5.7.7 of this chapter.
[1147] See the Preamble and sections 1, 3(4), 69 and 72 of the POPIA.
[1148] Heyink http://www.derebus.org.za/guide-protection-personal-information-act/ (Date of use: 12 January 2019).
[1149] Sections 4 and 5 of the POPIA.
[1150] Sections 73, 74, 75, 76, 77, 78, 79, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 101 of the POPIA. See para 7.7 of Chapter 7 of this study on examination of ADM.

3.5.6.6 Nature, components and scope of the concept of the secrecy of online communication in the Cybercrime and Cybersecurity Bill

The overall objects of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 are to regulate the use of electronic communications and ensure that the integrity and security of electronic communications —which comprise both offline and online communications— are protected, by mainly prohibiting and criminalising certain acts or conducts in electronic communication.[1151]

The nature, components and scope of protection of online communication is represented in an intelligible online form such as data, computer program and computer data storage medium.[1152] The scope of protection of an online communication covers, amongst others, the prohibition of unlawful access to online communication; unlawful interception of data; unlawful and intentional uses or possession any software or hardware that is capable of compromising online communication; unlawful interference with data or computer program, system or storage medium.[1153]

In addition, the scope of protection of online communication includes unlawful and intentional acquisition, possession, provision, receipt or use of a password, access codes or similar data or devices; unlawful and intentional interference with online communication; attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring someone to commit an offence in the areas aforementioned in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.[1154] The Cybercrime Bill 2018-Amendments

[1151] See the preamble and Chapter 2 of the CCB B6-2017. See section 1 of the CCB for the nature, contents, component and scope of electronic communications in the definition of 'access', 'article', 'computer', 'computer data storage medium', 'computer system', 'data', 'data message', 'output of data', 'output of a computer program', 'public available data', 'seize' and ''traffic data. See also sections 2(1) (a)-(d) of the CCB B6-2017. These provisions are found in sections 1 and 25 of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

[1152] See section 1 of the CCB B6-2017 for the nature, contents, components and scope of online communication in the definition of 'computer system', 'data', 'data message', 'output of data', 'public available data', 'seize' and 'traffic data'. Section 2(1) (a)-(d) of CCB B6-2017. These provisions are now found in sections 1 and 25 of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

[1153] Sections 2-6 of the CCB B6-2017, which are replaced by sections 2-6 of the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017.

[1154] Sections 7, 8(b) and 12 of the CCB B6-2017, which are replaced by sections 7, 8(b) and 12 of the Cybercrime Bill 2018–Amendments Proposed to Bill B6-2017.

Proposed to Bill B6-2017 also prohibits a party from distributing data message of an intimate image in online communication.[1155]

The scope of protection of online communication in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 also covers the observance of standard operating procedures for interception and the conduct of an OCI by LEAs.[1156]

The scope of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 provides for the observance of confidentiality and restricted use of online communication in cross-border mutual assistance for criminal investigation by the RSA and foreign countries.[1157]

In all this, the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 is relatively adequate to protect the right to the SOC in this regard.

3.5.6.7 Conclusion

Save for the POPIA which substantially and discriminately protects offline privacy than online communication, the ECA, ECTA, RICA and Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 regulate the right to the SOC, though with significant lacuna in their provisions. Considering the complexity of the nature and features of online communication, it is very clear that the law recognising the concept of the SOC is scattered all over in various Acts,[1158] thus makes it difficult for proper recognition, protection and coordination of the sub-rights to the SOC, hence the purpose of this study which is to examine the existence or otherwise of this concept in the privacy jurisprudence in the RSA.

[1155] Section 18 of CCB B6-2017, which is replaced by section 19 of the Cybercrime Bill 2018–Amendments Proposed to Bill B6-2017.

[1156] Chapter 5, more particularly sections 24, 37 and 38 (amongst others) of the CCB B6-2017, which are replaced by sections 26, 39 and 40 of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

[1157] See Chapters 6 and 12 of CCB B6-2017, which are replaced by Chapters 6 and 10 of the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017.

[1158] Kosseff *Cybersecurity law* xxi.

3.5.7 Comparison of the techno-legal nature, features and threshold of risks and protection between online and non-online communication

3.5.7.1 Introduction

In privacy communication or its infringement, five channels or means of data communications are generally used, which are described and compared in this study. These channels are: 'broadcasting',[1159] 'human agency', 'offline electronic communications' device, 'online communication' device,[1160] and 'postal service'. In their various descriptions, some of these channels share the same or similar techno-legal nature, features and thresholds and in some cases, the nature and features of these channels are dissimilar.

In examining the right to the SOC as a distinct or separate component of privacy, a thirteen-point theory and reasoning —some of which are based on the risk theory— is proposed in comparing and contrasting the five channels of data communication, in addition to the earlier examination of online communication and investigation.[1161] This comparison expresses one of the multi-dimensional or holistic approaches to this study,[1162] which seeks to determine which channel of data communication has more criteria advanced in its favour with a cumulative effect of placing such a channel of communication above the others in terms of the hierarchy of risks and protection expected in privacy or data communication.

While some of these theories examined below may be overlapping, the theories generally highlight the distinctive and dissimilar complex legal, ethical, technical, operational and administrative features of the five channels of communication of data, thus resulting in different arguments, discourses and conclusions or outcomes.

[1159] Wakefield A 'SA to miss digital migration deadline, but govt. says don't worry' http://www.news24.com/SouthAfrica/News/SA-to-miss-digitial-migration-deadline-but-govt-says-dont-worry-20150616. (Date of use: 4 July 2015)

[1160] See para 2.2.1 of Chapter 2 of this study where online communication devices are identified.

[1161] See generally Chapter 2 of this study.

[1162] Para 3.1 of this chapter.

3.5.7.2 The storage capacity of digital data in online communication

The erroneous belief of the court is that the size of the content of data that is conveyed through a human agent, hard copy sources —such as a diary— and other channels of communications is the same size with the content of digital data stored in a seized mobile cellular telephone,[1163] whereas the content of the latter is enormously unimaginable,[1164] including the emerging quantum computing.

In *State v Terrence Brown*, the High Court erroneously held[1165] that since LEAs would not be precluded from opening a diary that was dropped at the scene of a crime to identify its owner or possessor and link it up with the gunman who killed the deceased, same principle applies to the physical downloading of data from a mobile cellular telephone that was found at the scene of a crime.[1166] It is noted that this comparison is specifically conducted concerning the dichotomy between offline and online data and not exclusively in relation to the seriousness of the offence committed, as this distinction is buttressed below on the need to consider the *irreversibility* of the effect of the commission of an offence as a basis to physically search a mobile cellular telephone at a crime scene without a warrant.

Similarly, the court in *State v Miller* incorrectly observed[1167] that a diary, photo album and a locked safe seized from a suspect would not require a warrant under the CPA before it is opened or searched, likewise a mobile cellular telephone seized by a LEO.[1168] Counsel for the accused argued that a cellular telephone is now regarded as a minicomputer in contemporary society,[1169] which this study unequivocally subscribes to with some qualification below.

[1163] *State v Terrence Brown* supra 29.

[1164] Pistorius T "Copyright law and IT" in Van der Merwe D et al *Information and communications technology law* (2008) 240; Rosen 1 http://www.newrepublic.com/article/118396/supreme-court-cellphone-case-went-further-privacy-advocates-hoped (Date of use: 30 June 2014); See also *United States v Jones* 565 U.S (2002) 3. It is noted that the examination of this criterion is different from the examination of criterion titled 'The risk levels involved in the indivisible digital data and divisible non-digital data' at para 6.5.7.6 of this chapter.

[1165] Section 180 (a) and (c) of the Constitution makes provision for training programmes for judicial officers and the participation of non-judicial officers in the administration of justice.

[1166] *State v Terrence Brown* supra 29-31.

[1167] Section 180 (a) and (c) of the Constitution makes provision for training programmes for judicial officers and the participation of non-judicial officers in the administration of justice.

[1168] *State v Miller* supra 38.

[1169] *State v Miller* supra 38.

Towards this end, this study emphasises that circumstances under which a warrant to search a mobile cellular telephone is not required —which though qualified in various ways in this study— include where the effect of the commission of a serious offence is *absolutely irreversible*. This this study, in a way, partially concurs with the reasoning of the court to the extent that the effect of the offence committed in *State v Terrence Brown* is a*bsolutely irreversible*.[1170]

Accordingly, it is strongly posited that a physical routine roadblock or stop and search will not entitle LEAs or LEOs to randomly, routinely, and physically search the mobile cellular telephone or other online communication devices of an individual without a warrant from the court under the guise of executing a lawful duty in sections 30-31 of the Cybercrime and Cybersecurity Bill 2017, save where there are exceptional circumstances such as the declaration of a state of emergency where certain rights are temporarily suspended including the right to the SOC.[1171]

Human-agents communicate data in non-digital format through the five natural human senses which do not seem to have large quantitative and qualitative capacities[1172] unlike digital data which can be in larger quantitative —but in a compressed format— and qualitative capacities.[1173] In *United States v Freedom of the Press*,[1174] the court held that where information is accessible as an inseparable whole, it is an invasion of privacy to have access to the other part of the information that is not needed,[1175] thus indicates a greater risk in the large storage capacity in a digital format than human agency.

[1170] *State v Terrence Brown* supra 29-31; *State v Makwanyane* supra 351; Paras 3.5.7.14, 5.3.4.2 and 6.3.3.4 of this study.
[1171] Paras 6.3.3.2(e), 6.3.3.3(e), 6.3.3.4(d), 6.3.3.5(e), 6.4.5, 6.11 and 6.13 of Chapter 6 of this study.
[1172] *Mathias Int. Ltd v Baillache* supra 60 where the High Court compared human and email memories where it was emphasised that the former does not have much memory as the latter.
[1173] Pistorius T "Copyright law and IT" 240; *Riley v California* and *US v Wurie* supra 3 of the Syllabus and 19 of the Opinion.
[1174] This case involved a request by the press in the interest of the public of some personal information concerning a family which was being investigated by the FBI which placed the record on 'a computerized summary file located in a single clearinghouse of information' of general rap-sheet covering over 24 million persons, see *United States Department of Justice v Reporters Committee for Freedom of the Press* 489 U.S 763-765 (1989) (*United States v Freedom of the Press*).
[1175] *United States v Freedom of the Press* supra 763-764; see also Chapter 2 (para 2.3.2) of this study and para 3.5.7.6 of this chapter.

Similarly, in *Web Call v Botha*, the High Court observed the difficulty in isolating digital documents identified as a whole.[1176] Borrowing from this principle, it is submitted that exposing the whole data of an individual in an online communication device when conducting an OCI is a worse intrusion of online communication because of its non-compartmentalisation and non-passworded compartmentalisation.[1177]

Therefore, a higher level of protection ought to be accorded data in online communication and other channels of communications than a human agency or hard copy. In other channels of communication other than a human agency, the digital copy may exist in broadcasting, offline electronic device and postal services -containing a memory stick, for example.

3.5.7.3 Intangibility, fluidity and ephemerality of digital data in communication

Given the risky feature and the need to maintain the integrity and security of digital data, the court in *State v Terrence Brown* highlights how careful a law enforcement officer ('LEO') was by 'purposefully or accidentally' not tampering with the data on the mobile cellular telephone that was found at the crime scene.[1178]

However, the LEAs in *State v Agliotti* were not careful to access the data in a mobile cellular telephone. It was easy for the forensic telephone experts from the Online Communication Service Providers to issue out the phone record without authorisation and an explanation for the easy 'manipulation of cellular records by unscrupulous persons' when evidence was presented to the court.[1179]

This is because, by virtue of the inherent feature of intangibility, fluidity, and ephemerality of data in digital format, a digital data is exposed to easy manipulation or alteration[1180] in all

[1176] *Web Call v Botha* supra 21; Chapter 2 (para 2.3.2) of this study.
[1177] Chapter 2 (para 2.3.2) of this study.
[1178] *State v Terrence Brown* supra 6.
[1179] *State v Agliotti* supra 136-141 and 145 -146; Van der Merwe *Unconstitutionally obtained evidence* 208.
[1180] *State v Agliotti* supra 136-141 and 145 -146. Popoola *Liability of ISPs* para 3.6.1; See s 205 of CPA and s 15 of RICA; See also *State v Naidoo* supra per McCall J 527 c-f; Van der Merwe S E 'Unconstitutionally obtained evidence' in Schwikkard P J and Van der Merwe S E *Principles of evidence* 3ed (2012) 252-253 and 410-411 (Van der Merwe '*Unconstitutionally obtained evidence*'); Sections 8, 9, 12 and 13 CCB B6-2017, which are replaced by ss 8, 9, 12 and 13 of the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017; Jurgens A and Savides M 'Revealed: SA spies scary shopping list - WikiLeaks lays bare SA Police and SARS Agents inquiries about espionage software' 2015-07-12 *Sunday Times* 1-2 (Jurgens and Savides 2015- 07-12 *Sunday Times*); Maphumulo 2016-08-30 *The Sunday Independent*; Shaikh N 'Online "Cheaters" caught in the web-

channels of data communication in this context except in human agency which does not involve digital data.[1181] Digital data is in contrast with non-digital data, which is not easily manipulated. For example, a document written by hand or which is in hard copy may not easily be manipulated.[1182]

It is noted that the planting of a microchip in a human body does not include the digital data of a micro-chip or change the natural *status quo* of a human being by incorporating a new feature into a human body whose anatomy suddenly changes to that of a being who is biologically, ethically and legally fit to integrate digital data or privacy communication as part of the natural human system. A human being referred to in this context is a human being that we are all referred to according to the nature of humanity from the religious or philosophical perspective.

If the natural anatomical *status quo* of a human being is forced to change by technology, it then takes away the natural human quantitative and qualitative capacities of a human being that is considered in this study as the basis for distinction. In other words, if the microchip is integrated as part of a human being, then such human being has been manipulated to become a robot, which is no longer a human being for the purpose that is being examined herein.

In summary, the manipulation of digital data is made possible because of the reality of the fluidity and ephemerality of the intangible digital data, more particularly where the manipulation is done in an online data communication. Thus, although an online communication should have the highest level of protection —for obvious reasons which are stated in other criteria— a higher level of protection ought to be granted to data communication in all channels of communications identified in this study than in human agency, which is the only channel that does not utilise digital data in private communication.

---

many put in compromising position by hackers' 2015-08-30 *The Sunday Independent* 3 (Shaikh 2015-08-30 *The Sunday Independent* 3'); Puren S 'Paedophiles, The web is closing in' 2015-10-29 *You* 136-137 (Puren 2015-10- 29 *You*); Maphumulo 2015-11-03 *The Star* 2.

[1181] It is however noted that technology has been developed that enables human beings have computerised device embedded in the body that would enhance and monitor human functioning senses and capacity, see Monks K 'Forget wearable tech, embeddable implants are already here' http://edition.cnn.com/2014/04/08/tech/forget-wearable-tech-embeddable-implants/ (Date of use: 12 June 2014) (Monks http://edition.cnn.com/2014/04/08/tech/forget-wearable-tech-embeddable-implants/ (Date of use: 12 June 2014). It is however noted that this new technology will still not take away the usual human nature of limited senses and capacity. Rather, the technology will constitute another form of online communication device.

[1182] Collier D W 'Electronic evidence and related matters' in Schwikkard P J and Van der Merwe S E *Principles of evidence* (2009) 410-411; Ruiz *Privacy in telecommunications* 61-66.

3.5.7.4 Access to and use of digital data in online communication

Since digital data could easily be shared and infringed in an offline electronic communication,[1183] the court commended the restrictive use of digital data gathered by the LEOs in *State v Miller*.[1184] It is advocated that in online communication, digital data is more capable of being easily copied, shared or retained[1185] and infringed within a short period by millions of people globally due to the ubiquity[1186]or accessibility of data in online communication[1187] and broadcasting, as opposed to the other channels of private communications.[1188]

Nevertheless, though contemporary broadcasting entails both real-time —podcasting or streaming— and archived communications like online communication does, however, broadcasts do not have the same risk level as that of archived communications in online communication. This is because individuals do not have the ability, and capacity to re-broadcast the archived data through the conventional broadcast equipment except through the use of online communication devices, which are not broadcasting devices in the real and conventional sense of broadcast. Online communication devices include Internet broadcast or podcast which is not the same as the conventional broadcast. Individuals have the ability and capacity to re-communicate data in online communications which can be virtually copied immediately by millions of people across the globe.

It is therefore submitted that the ability to re-communicate data ought to place data in online communication on a higher risk level than in non-online communications, consequently, data

---

[1183] *State v Terrence Brown* supra 6 and 8.
[1184] *State v Miller* supra 72.
[1185] *State v Terrence Brown* supra 6 and 8; Popoola *Liability of ISPs* 45-47, 103-105 and 148- 150.
[1186] In the U.S., information is 'quietly collected by ubiquitous devices and applications and available for analysis to many parties who can query, buy or subpoena it. Or pay a hacker to steal a copy of *everyone's* location history', Blumberg A J and Eckersley P 'On locational privacy, and how to avoid losing it forever' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 315 (Blumberg and Eckersley *Locational privacy*); Madrigal *I'm being followed: How Google-and 104 other companies- Are tracking me on the web* 342.
[1187] See criterion two above which relates to the issue being discussed; *Web Call v Botha* supra 5 and 12. The devices dealt with by the court were online communication devices. See also Rosen 1 http://www.newrepublic.com/article/118396/supreme-court-cellphone-case-went-further-privacy-advocates-hoped (Date of use: 30 June 2014. In *H v W* supra 2 and 10, the court held that social network service (SNS) is ubiquitous and observed that there are about six million users of Facebook in South Africa while there are 800 millions of users on face book globally.
[1188] For example, s 31 of CPA requires the state to return any seized item that is not used for a trial, see *Thint v NDPP* supra 217.

in an online communication deserves a higher level of privacy protection than the data in non-online communications.

3.5.7.5 Types of data end-users in online communication

The level of risk that data is exposed to in any channel of data communication is determined by whether data is in digital format[1189] and more importantly in this rubric, whether the end-user or target of data communication is the public or a private entity.[1190] If digital data is destined for the public, the level of risk that a digital data is exposed to is not as high as a situation where digital data is meant for the consumption of a private person because there is nothing or little to protect where data is meant for the public. The criterion herein is further examined as follows.

Firstly, in *broadcasting*, though data communication in a broadcast is usually in a digital format, the fact that a broadcast is usually meant for the public, sections of the public or financial subscribers to a broadcasting service[1191] —and not for a private destination— means that there is a diminished expectation of privacy in a broadcast, unlike an online communication which has a higher level of expectation of privacy. This is because, though online communication may be meant for the public too —which is disseminated at the fifth sanctum of privacy continuum,[1192] it is more often than not meant to communicate to online communication users whose expectations of privacy are between the innermost and outer sancta of online communication.[1193]

This explains the rationale of the caveat that is inserted in some online communications at the bottom of some official communications meant for a targeted person or group, which might mistakenly be delivered to an unintended person or group. Consequently, the risk that is in data

[1189] *State v Terrence Brown* supra 6 and 8 and *State v Miller* supra 72.
[1190] In *State v Terrence Brown* supra 2, 3, 27-29 and 31(more particularly para 28), because the cell phone was found at the scene of crime which was, more importantly, in a public place, the court held that there was no judicial authority needed to download data from a cell phone which was found in this circumstance.
[1191] Section 1 of ECA 36 of 2005. Stuntz W J 'Privacy's Problem and the Law of Criminal Procedure', 93 *Mich. L. Rev.* 1016, 1022 (1995); Solove 2002 Vol. 90 *California Law Review* 1107; Brierley M 'Telecommunications technologies' in Thorton L et al (eds) *Telecommunication law in South Africa* (2006) 60- 61.
[1192] See para 3.8.6 of this chapter.
[1193] Para 3.8 of this chapter.

communication is lower in a broadcast than in online communication, thus, a greater level of protection is accorded the latter than the former in the broad concept of privacy communication.

Secondly, in *human agency*, data is communicated through human senses and non-digital means to a limited number of people. This means that where there is a breach of privacy, the spread of the information is controlled or curtailed because of the limitation in the human capacity to spread the information without the aid of any public online communication system, which is unlike the ubiquitous online communication that can be used to massively communicate with the world. It therefore follows then that human agency does not bear greater risks in privacy communication than online communication, therefore, the former does not deserve a greater level of protection than the latter.

Thirdly , though the object of privacy protection in *postal services* might include both digital —such as memory stick in a physical parcel— and non-digital data and the targets of data communication might be private and public, the level of risk in postal services is not as high as that of the data communication in online communications.[1194] This is because postal services —as described herein which exclude telegraph— do not entail the use of public online communication system —such as online communication system— that will aid the widespread of information, thus, the spread of information is curtailed in the postal services. Accordingly, there is a lower expectation of privacy in postal services than in online communication that is ubiquitous in nature and feature.

Fourthly, although the object of privacy protection in an *offline electronic communication* — for example, a computer system without online connectivity— is purely digital data and the targets are both private and public, the level of risk of data communication in an offline electronic communication is not as high as that of the risk in online communications. This is because if there is an invasion of privacy of digital data in an offline electronic communication, there is no public online communication system with which data is communicated to a larger audience[1195] unlike the communication of data in online communication, which is ubiquitous in nature and feature.

[1194] *Bartnicki & others v Vopper,* et al. Nos. 99-1687, 99-1728 paras 72 and 76.
[1195] *Simataa v Magistrate of Windhoek and others* 2012 (2) NR 658 (HC) 49 (‘*Simataa v Magistrate of Windhoek’*).

Finally, in an *online communication* where digital data is the only object of privacy protection in both private and public communications, data is inherently exposed to greater risk in online communication system than other channels of data communication. This is because: firstly since data is in the virtual world, it is more susceptible to attacks by millions of online users from any part of the world.[1196] The higher risk level in online communications has prompted the proposed enactment of the Cybercrime and Cybersecurity Bill to further address cybercrime and cybersecurity issues; secondly, after the initial invasion of privacy, it is faster and effective for an infringer to subsequently distribute or reach out to millions of audiences around the globe within a short period in both private and public online communication devices.[1197]

Given the foregoing argument, it is submitted that a higher level of privacy protection is required in online communication than in non-online communications.

3.5.7.6 The risk levels involved in the indivisible digital data and divisible non-digital data

In addition to the earlier partial examination of this criterion in the first criterion —including the case of *United States v Freedom of the Press*,[1198] the courts have expressly, and impliedly acknowledged the *indivisibility of digital data*[1199] and *divisibility of non-digital data*[1200] during the investigation but failed to make a distinction in terms of the levels of risks between the two forms of data. Because LEAs have unrestricted access to the undivided digital data in online communications during the conduct of an OCI as opposed to the divisible data in 'non-electronic offline communications',[1201] data is exposed to greater risks[1202] in online communications than in the non-electronic offline communications. Thus, there ought to be a higher level of privacy protection in online communications than in non-electronic offline communications.

[1196] The New York Times 'U.S. said to find North Korea ordered cyberattack on Sony' http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0 (Date of use: May 20 2016) and Reuters 'North Korea denies cyberattacks on South Korea officials' http://www.reuters.com/article/us-northkorea-korea-cyber-idUSKCN0WF05V(Date of use: May 20 2016).

[1197] Rosen 1 http://www.newrepublic.com/article/118396/supreme-court-cellphone-case-went-further-privacy-advocates-hoped (Date of use: 30 June, 2014).

[1198] *United States v Freedom of the Press* supra 763-764.

[1199] See para 3.5.7.2 titled 'Storage capacity of digital data in online communication'; *Web Call v Botha* supra 21; *State v Terrence Brown* supra 5 and 6; *United States v Freedom of the Press* supra 763-764.

[1200] *Thint v NDPP* supra 144 and *State v Terrence Brown* supra 29.

[1201] This category excludes offline electronic devices such as computer that does not have online connectivity.

[1202] Section 57(2) of POPIA states that where there is a particular risk in an information, a particular protection is required.

In a *human agency*, communication can only be divisible in both real-time and archived communications, therefore this channel of communication has a minimal level of risk and enjoys a minimal level of privacy protection in the context herein. For example, in a real-time communication of data through human agency, the infringement of privacy involving what a couple does in the bedroom or house could be separated, qualified or prevented. This may be done by the couple in the bedroom who may give notice of their privacy before invasion occurs and by so doing, awareness is created in the minds of LEAs before the invasion into the room occurs.

Furthermore, in a real-time communication involving human beings, there is the possibility of the lowering of voices or moving away from where oral communication is being held by individuals in direct communication. Lowering of voices or moving away are unique forms of separation of data in human agency. In archived communication of data through human agency, there is a possibility of separating these items —such as documents and real evidence— before invasion occurs or during an invasion. Therefore, there is a lower level of expectation of privacy in a human agency in the above context than in online communication due to the foregoing discourse.

In *offline electronic communication devices* and *postal services* —such as a memory stick in a physical parcel, digital data is usually archived and arguably, there is usually no compartmentalisation, and passworded compartmentalisation of digital data in these two channels of data communications. Thus, same or similar level of privacy protection enjoyed in online communications is accorded to these two channels of data communications.[1203]

Nonetheless, where data is divisible during communication —in *broadcast* and *human agency*, minimal privacy protection is required during an investigation. This is because a broadcast —whether it is divisible or not— is usually meant for the general or public consumption or destination while data communication in a human agency is only divisible. Thus, in both channels, the levels of risks are low in contrast with online communication which is indivisible in nature.

[1203] *Web Call v Botha* supra 21; Ruiz *Privacy in telecommunications* 172.

In summary, there is a higher expectation of privacy in online communication than in non-online communications.

3.5.7.7 Duty and length of control and management of the security of data in online communication

In the *offline* world, there is a higher security and privacy expectation by an individual where the primary duty of control and management of the security of communication of data lies in an agent or third party[1204] than where an individual manages the data by himself or herself. This expectation is premised on the fact that where data is handed over to an agent for transmission or storage purposes, legal trust is created.

In the offline world, the Constitutional Court in *Loureiro and Others v iMvula Quality Protection (Pty) Ltd*[1205] pronounced on the legal trust principle concerning the physical security of a house, which though, does not involve data in the strict sense but the issues also bothered on the concept of privacy.[1206] Based on the legal trust principle to keep the physical property safe,[1207] the court held a private security company liable for breach of contract and negligence under the law of delict, which gives effect to the protection of constitutional rights including the right to privacy.[1208]

In offline communication, an agreement is reached in an offline communication that an employee should not breach the confidence and trust of his employer by divulging information regarding trade secret —for example— in which Ernest and Schwartz posit that 'personal secrets are inviolable'[1209] now or in the future, thus, this essentially means that agency relationship is relatively perpetual in this regard.

[1204] Chapter 2 (paras 2.2.2.2 and 2.3.3) of Chapter 2 of this study and para of 3.5.7.7 of this chapter. Generally, the law of agency requires a specific performance in the fiduciary relationship, Van Jaarsveld S R 'Agency' in CJ Commercial Law 3ed (2006) 142-166.

[1205] *Loureiro and Others v iMvula Quality Protection (Pty) Ltd* [2014] ZACC 4 paras 1, 3, 4, 5, 9, 13, 17-24, 26-30, 33, 42- 46, 48 -51, 56, 62-63 and 67 (*Loureiro v iMvula*).

[1206] *Loureiro v iMvula* supra 1, 3, 9, 21, 31, 45, 46 and 67.

[1207] *Loureiro v iMvula* supra 1, 3, 4, 5, 9, 13, 17 - 24, 26- 30, 33, 42- 46, 48 -51, 56, 62 - 63 and 67.

[1208] *Loureiro v iMvula* supra 1, 3, 4, 5, 9, 13, 17 - 24, 26- 30, 33, 42- 46, 48 -51, 56, 62 - 63 and 67; *Barkhuizen v Napier* [2007] ZACC 5; 2007 (5) SA 323 (CC); 2007 (7) BCLR 691 (CC) paras 28-30 and 35 and *Fose v Minister of Safety and Security* [1997] ZACC 6; 1997 (3) SA 786 (CC); 1997 (7) BCLR 851 (CC) para 58.

[1209] Ernst and Schwartz *Privacy- The right to be let alone* (1968) 10 and 11.

In the *online* world, since the court held a private security company liable in the physical realm where there was a choice for the house owner to hire a security company, it is advocated that there ought to be a higher level of privacy and security expectation by an individual in the compulsory use of online communication devices which have higher risks than non-online communications[1210] for the following reasons.

Firstly, if an agent generally owes a fiduciary duty or obligation[1211] to two parties in an offline communication according to Ernest and Schwartz,[1212] the duty of an online agent is greater in online communication because three parties are generally involved in an online communication save in an innermost sanctum where in most cases involves the user and Online Communication Service Provider.[1213]

Secondly, since individuals do not have any alternate choice of using online communication as business and social channel of communication in the 21st century,[1214] which is risky and 'voluntarily compulsory', greater risks abound in online communication than in the non-online communications.

Furthermore, in online communication, multiple electronic agents[1215] perpetually or continuously control and manage the security of data communication in agency, fiduciary or trust relationships,[1216] unlike other channels whose duty and management are not perpetual because the control and management of data by the agent ceases at a point in time. Every digital data in online communications —be it voice, text, picture or audio— is handed over by individuals, through the dedicated channels in an online network, to online communication agents, as system experts who keep or manage the data perpetually.[1217] Whatever information an online communication agent or its employee has access to or comes across in online

[1210] Paras 2.3 and 2.5- 2.10 and 2.11.4 of Chapter 2 of this study.
[1211] Ernst and Schwartz *Privacy-The right to be let alone* 26.
[1212] Ernst and Schwartz *Privacy-The right to be let alone* 9, 25 and 40.
[1213] Para 3.8.2 of this study.
[1214] See online conscription in Chapter 2 (para 2.3.3) of this study.
[1215] Popoola *Liability of ISPs* 8 -10.
[1216] Popoola *Liability of ISPs* 6-10 and 15-20.
[1217] Popoola *Liability of ISPs* 6-20; Alheit *Issues of civil liability arising from the use of expert systems* 522, 526 and 527.

communication, it can forever not be used for purposes or benefits other than what it was initially meant for,[1218] thus, there is a prohibition of the various non-OCI conscriptions.[1219]

In summary, a relatively higher security and privacy expectation ought to be accorded data in online communication than in non-online communications for the foregoing reasons, therefore, there is a higher duty and perpetual period of control and management of the security of data in online communication than in non-online communications.

3.5.7.8 Exposure of data to risk in the inherent, conscriptive, covert and perpetual online criminal investigation

This theory is different from the last theory examined because this theory deals with the perpetual investigation and not just the perpetual safekeeping of data examined in the last theory.[1220] Firstly, due to its inherent technical conscriptive nature, the conduct of an OCI exposes data to greater risks in the conscriptive online communication[1221] than the way data is exposed to risks in the other investigative procedures in non-online communications.[1222] For example, the use of an IMSI catcher exposes a user of online communication to great risks.

This is because the catcher unlawfully intercepts and manipulates data in online communications without the knowledge of the network service provider.[1223]

Furthermore, aside from the conscription in online communication, the exposure of data to the inherent risks in AI —such as robotic investigator—[1224] invades online communication.

Secondly, , although some covert methods are used in conducting investigations in a non-online communication world,[1225] however, the higher levels of risk that data is exposed to in the covert

---

[1218] Sloan *Law of privacy in a technological society* 54.
[1219] Para 2.3.3 of Chapter 2 of this study.
[1220] 3.5.7.7 of chis chapter.
[1221] Para 2.3.3 of Chapter 2 of this study.
[1222] See para 3.5.7.13 of this chapter.
[1223] Swart H Communication 'Surveillance by the South African Intelligence Services' 2016 at 11-13 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use: 13 August, 2016).
[1224] See para 2.11.4 of Chapter 2 of this study.
[1225] In *NDPP v Mahomed* [2007] SCA 138 (RSA) para 18, the SCA held that 'The retention by the registrar of the material, or copies of the material, even if that material is not viewed, will in my view be a continuing violation of the respondent's privacy, which is protected against violation by s 14 of the Bill of Rights. I do not think

conduct of an OCI is aggravated by the doctrine of double jeopardy against an individual who is a victim of the conduct of an OCI.[1226] The features of the conduct of an OCI in section 16(7)(a) of RICA are conscriptive.[1227] The features also prohibit an individual from having an 'opportunity to put his side of the case' across during investigation[1228] unlike an offline investigation —which in most or some and relevant instances— is conducted in a non-covert manner, and avails a victim of some level of fair hearing.[1229] Thus, data is exposed to greater risks in online communications than in the other channels of data communication when an investigation is conducted in the former than in the latter.

The exposure to risk in an online communication arises from the fact that an OCI direction is, at all times —day and night— obtained covertly via an ex-parte application, and executed covertly.[1230] The covertness thus creates some doubt on the reasonable openness and transparency of the conduct of an OCI, which has been criticised by human rights activists in the US who are advocating for a regime that allows for the security of an OCI through the controversial service of a motion on notice to the target of investigation before interception occurs.[1231]

Though the service of notice on a target before investigation may defeat the purpose of a covert online investigation, non-awareness by a target of the covert and intrusive investigation of online communication after the investigation has been concluded creates greater risks in the protection of the communication of an individual than the other channels of communication where an investigation is conducted. This is because the individual in the latter channels of communication would have directly or indirectly known of the investigation as aforesaid.

---

that privacy is violated only when private communications are viewed by or exposed to viewing by another. I think it is violated just as much merely by dispossessing a person of control over material that he or she is entitled to hold in private.' *Craig Smith & Associates v Minister of Home Affairs and Others* 12756/2014 7, 15-19, 31-32, 35 and 37-39 (*Craig v Home Affairs*). For example, a secretive a cell phone subscriber does not have a

[1226] *Absa v Moller* supra 6.

[1227] Para 2.3.3 of Chapter 2 of this study.

[1228] See s 16(7)(a) of RICA; *Web Call v Botha* supra18; *Absa v Moller* supra18.

[1229] *Thint v NDPP* supra 141, 149, 151-156, 160, 168, 182-186, 188, 192 and 208.

[1230] McQuoid-Mason *Privacy I*' 146.

[1231] Section 16(7) of RICA. There is inherent frustration in notifying a suspect or his attorney about a proposed search in the offices of the attorney, see *Thint v NDPP* supra 124-132, 142, 155, 160-161, 168 -169 and193. Electronic Frontier Foundation '13 International Principles on the Application of Human Rights to Communications Surveillance - Necessary and Proportionate' https://www.eff.org/document/13-international-principles-application-human-rights-communication-surveillance (Date of use: May 20 2016)

Furthermore, online communication devices and postal services are the only two channels of data communications that conjunctively entail the covert features of an ex-parte application and covert execution of the interception direction because of the inherently secret nature in closed-channel communications[1232] —which include letters, telegrams, and telephone conversations.[1233]

However, in the other channels of data communication —including offline electronic devices, the two conditions of obtaining an ex-parte order in intercepting communications and executing the order in secret may not always apply conjunctively.[1234]

Communication in other channels is mostly conducted through open-channel communications, which do not necessarily require secrecy protection.[1235]

It is submitted that in open communication, data is accessible, kept or made available with operational requirements that are lesser than the closed-channel communication operational requirements. Open-channel communications enable general or uninvited members of the society to have relative access to, use or record an act of communication[1236] through channels such as the manual copying of data through a memory stick, broadcasting, human agency[1237] and Bluetooth technology.[1238]

Moreover, the fact that RICA allows, in the first instance, a three-month period to conduct an OCI in an online communication[1239] regrettably creates an atmosphere of perpetuity in online communication,[1240] which is almost similar to an offline investigation, in which the law provides for general conditions, which make a search warrant perpetually effective until executed or cancelled.[1241]

[1232] Ruiz *Privacy in telecommunications* 143 and 154-157.
[1233] Ruiz *Privacy in telecommunications* 143.
[1234] *Web Call v Botha* supra 7.
[1235] Ruiz *Privacy in telecommunications* 143. 2.5
[1236] Ruiz *Privacy in telecommunications* 143.
[1237] Ruiz *Privacy in telecommunications* 143 and 148.
[1238] Popoola *Liability of ISPs* 14-15.
[1239] Sections 16(6)(d), 17(1), 20(3)(a) and (b), (4), (5) and (6) and 21(5)(e) of RICA. Para 2.5 of Chapter 2 and paras 6.9 and 6.10 of Chapter 6 of this study.
[1240] See Chapter 2 of CPA No 51 of 1997. See para 3.5.7.8 of this chapter.
[1241] Sections 17(5), 21(3)(b) and 25(2) of CPA. *Beheersmaatschappij Helling I NV and Others v Magistrate, Cape Town and Others* 2007 (1) SACR 99(C) para G at 114 (*Helling v Mag*). Para 3.5.7.8 of Chapter 3 of this study.

If there is a true, and genuine commission or attempted commission of a serious offence, which requires urgent and intrusive investigation by conducting an OCI,[1242] it is unlikely that three months would pass by without LEAs gathering sufficient evidence in the first instance of the conduct of an OCI.[1243] The evidence gathered through the conduct of an OCI will immediately give a reasonable lead —if not an unimpeachable one— to the use of other methods of investigation to complement the conduct of an OCI.[1244] In the U.S., despite the refusal by the service provider to allow LEAs have access to online communication, *a month* was used by LEAs to decode a WhatsApp communication in the investigation of a murder case without any assistance from the service provider.[1245]

In the world of online communication, it is submitted that —with or without notice to an individual— the conduct of an OCI for 24 hours in a day is arguably equivalent to conscriptively listening, monitoring, viewing or watching an individual[1246] for a month in a real-time or archived online communication. Online conscription has been described as placing a human being in a panopticon,[1247] which is certainly going to happen to any individual that uses an online communication device because the conscription is automated in some instances.

Arguably, the certainty of conscription does not indicate when and for how long an individual will be conscripted in a real-time or archived communication, which psychologically puts an individual in a naked, captured, traumatic and suspended state of liberty of mind. This is because the conduct of an OCI intrusively and comprehensively reveals both audio, and visual contents of online communication gathered, given that most online communication devices now have a camera installed and activated in them.[1248] In some instances, conscription occurs even where a camera or microphone is secretly installed in a device and where no real-time online communication occurs or even where the device is switched off.[1249]

[1242] NIA 'Investigations on Mr. Macozoma' 13, 18, 20, 24 and 26-29. Para 3.5.7.8 of Chapter 3 of this study. Para 3.5.7.8 of Chapter 3 of this study. Para 3.5.7.8 of Chapter 3 of this study.

[1243] Para 3.5.7.8 of Chapter 3 of this study.

[1244] Para 6.5 of Chapter 6 of this study.

[1245] Glover S 'Facebook's refusal to help police on murder case proves it is morally callous' http://www.dailymail.co.uk/debate/article-6132479/stephen-glover-Facebooks-refusal-help-police-murder-case-proves-morally-callous.html (Date of use: 5 September 2018). Para 3.5.7.8 of Chapter 3 of this study.

[1246] Para 2.3.3 of Chapter 2 of this study.

[1247] See para 2.3.3 (more particularly para 2.3.3.3) of Chapter 2 of this study.

[1248] Para 2.3.3 of Chapter 2 of this study.

[1249] Vaughan-Nichols S J 'How to keep your smart TV from spying on you- Opinion: You could worry about Windows 10 spying on you, or you could worry about something a bit more serious - like your TV listening in on you and passing on the information to intelligence agencies' https://www.zdnet.com/article/how-to-keep-your-smart-tv-from-spying-on-you/ (Date of use: 21 March 2018); Pagliery J 'How the NSA can 'turn

The perpetual feature of the conduct of an OCI on an individual takes away the autonomy, freedom or liberty of an individual in using online communication as a compulsory human *anatomic*, business, social and survival tool in the 21st century.[1250] This is because perpetual invasion triggers the occurrence of a serious invasion in online communication, which in real or archived time, graphically relays or reconstructs the step-by-step and second-by-second history[1251] of the breath, smell, taste, touch, sight, sound, movement, mannerism, gesture, activity, transaction or event an individual engages in within and outside his or her closet.

However, this study submits that section 15(2) of RICA, which requires that an OCI should not be conducted on a perpetual basis, seems to be a provision that is fairly applied proportionately[1252] in RICA and under other laws. Towards this end, the *three-month* duration for the conduct of an OCI is relatively reduced in the following circumstances, and durations:[1253] a) *thirty-six-hour* conduct of an OCI in the JSCI of Parliament of RSA Report;[1254] b) *two days* in *State v Naidoo*, where an employee of MTN —a telecommunication service provider in the RSA— handed over a transcript from the online communication of an individual to a captain in SAPS;[1255] c) *three-day* investigation used in Macozoma case;[1256] and d) *five-day* duration in a protection order direction in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 [1257] to proportionately conduct an OCI in relevant serious offences, the condition of which does not apply to the conduct of non-OCI methods.[1258]

It is noted that the *two* and *five days* respectively relate to archived data communications, thus it is submitted that the *two*-and *five-days* duration should not be confused with a real-time

on' your phone remotely' https://money.cnn.com/2014/06/06/technology/security/nsa-turn-on-phone/ (Date of use: 27 April 2016).

[1250] Para 2.3 of Chapter 2 of this study.

[1251] *Riley v California* and *US v Wurie* supra 3 of the Syllabus and 19-20 of the Opinion.

[1252] Paras 5.3.4 and 5.4 of Chapter 5 of this study.

[1253] Para 6.5 of Chapter 6 of this study.

[1254] JSCI Reports 2016 39.

[1255] *State v Naidoo* supra 521 B-E.

[1256] NIA 'Investigations on Mr. Macozoma' 13 and 20; *State v Terrence Brown* supra 6 and 8; *Helling v Mag* supra E at 101.

[1257] Section 20(3)(a) & (b)(i) & (ii) and (7)(a) of CCB B6-2017, which is replaced by ss 21(3)(a) &(b)(i)&(ii) and (7)(a) of the Cybercrime Bill 2018 – Amendments Proposed to Bill B6-2017; Paragraphs 89 – 97 of Section III (Explanatory Notes to Model Legislative Text on Interception of Communication) of ITU 'Interception Policy & Legislative Text' (2012).

[1258] Para 5.4.4 of Chapter 5 of this study.

communication which is regulated under different rules of *two-three minutes* periodic OCI principle as examined below.

In the U.S. and Canada, to determine whether an online communication involves criminal activities, governments instruct LEAs or LEOs to periodically, within a '…*reasonable time*, usually' between *two* to *three minutes* listen to *all calls* of an individual targeted in the instructions.[1259] This duration is sufficient and declared reasonable by several courts to make an initial judgement on the relevance of online communication to the crime commission.[1260]

Usually in the first instance, because individuals —including traffickers, amongst others— engage in a variety of topics', it is reasonable for LEAs or LEOs to conduct an OCI in 'periodic stop-checks…of minimised conversations' of *two minutes* of the real-time online communications of individuals.[1261] Any call that goes beyond two minutes is, according to instructions, re-assessed for about *two minutes* —per time— within 'intervals of at least one minute' whereby the device is turned off for one minute before continuing with the conduct of an OCI for another *two minutes* amounting to 'as much as two-thirds of a non-pertinent' communication.[1262] This is because LEAs or LEOs do not have a gift of prescience to pre-determine the direction of the issues to be discussed in online communication.[1263] Accordingly, the government should not be inherently suspected of abuse, foul play and insincerity when an OCI is conducted.[1264]

[1259] *R v Willis* (1997), 204 A.R.161 [1997] A.J. No 632 (QL) (Prov. Ct.) and *United States v Mansoori* No 99-1492 (7th Cir. 08/29/2002) para 27, see Hubbard, Brauti and Fenton *Wiretapping* at para 4.4.1 at page 4-43 to 4-44. It is noted that despite the intermittent two-minute interception, the defendant still complained, which means that lesser time could have been spent on the interception. Italics mine.

[1260] United States v Ozar 50 F.3d 1440, 1448(8th Cir.), see Hubbard, Brauti and Fenton *Wiretapping* at para 4.4.1 at page 4-44.

[1261] *United States v Ozar* 50 F.3d 1440, 1448(8th Cir.), see Hubbard, Brauti and Fenton *Wiretapping* at para 4.4.1 at page 4-44; *R v Willis* (1997), 204 A.R.161 [1997] A.J. No 632 (QL) (Prov. Ct.) and *United States v Mansoori* No 99-1492 (7th Cir. 08/29/2002) para 27, see Hubbard, Brauti and Fenton *Wiretapping* at para 4.4.1 at page 4-43 to 4-44. Italics mine.

[1262] *R v Willis* (1997), 204 A.R.161 [1997] A.J. No 632 (QL) (Prov. Ct.) and *United States v Mansoori* No 99-1492 (7th Cir. 08/29/2002) para 27, see Hubbard, Brauti and Fenton *Wiretapping* at para 4.4.1 at page 4-43 to 4-44. It is noted that despite the intermittent two-minute interception, the defendant still complained, which means that lesser time could have *United States v Quintana*, 508 F. 2d 867, 874 (7th Cir. 1975), see Hubbard, Brauti and Fenton *Wiretapping* at para 4.4.1 at page 4-44. Italics mine.

[1263] *United States v Quintana*, 508 F. 2d 867, 874 (7th Cir. 1975), see Hubbard, Brauti and Fenton *Wiretapping* at para 4.4.1 at page 4-44.

[1264] *R v Steel* (1995), 34 Alta. L.R. (3d) 440 and *United States v Mansoori* supra 29; see Hubbard, Brauti and Fenton *Wiretapping* at para 4.4.1 at page 4-44. This aspect of the quote basically means that LEAs should be granted the leeway to determine whether an online communication is relevant.

Despite the reasonableness of the practice in Canada and U.S., the defendant complained of lack of 'real minimisation' of the intrusion of online communication, which is believed should have been terminated at an earlier time where the evidence obtained is not relevant to the crime committed.[1265]

Finally, a fairly and reasonably open and transparent OCI ought to be in place to ensure that a higher level of protection is accorded online communication than in non-online communications. Given that non-content archived online communication[1266] is readily available to be accessed by LEAs or LEOs with a direction of the court to conduct an OCI which enables LEAs or LEOs to follow the lead from the information gathered or comply with the requirements of alternative methods,[1267] it is proposed that the *two-three-minute* periodic OCI should proportionately be conducted in the *first* to *third* classes of serious offences *only*[1268] *without a direction* of the court.

It is arguably advocated that while a *once-off or terminal three-minute* OCI is conducted in a real-time communication in a *first-class* serious offence *without a direction* of the court, *a minute* of OCI is conducted in a real-time communication in a *third-class* serious offence *without a direction* of the court in pursuance of the proportionality principle.[1269]

The need to conduct an OCI without a direction of the court is meant to partially and arguably borrow from sections 32-33 of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017. These sections prescribe that a LEO may carry out an investigation on an offline electronic communication device *without a direction* of court because of the expediency or urgency required with the expectation that a direction will be successful when applied for.[1270]

[1265] *United States v Quintana*, 508 F. 2d 867, 874 (7th Cir. 1975), see Hubbard, Brauti and Fenton *Wiretapping* at para 4.4.1 at page 4-44; *R v Willis* (1997), 204 A.R.161 [1997] A.J. No 632 (QL) (Prov. Ct.) and *United States v Mansoori* No 99-1492 (7th Cir. 08/29/2002) para 27, see Hubbard, Brauti and Fenton *Wiretapping* at para 4.4.1 at page 4-43 to 4-44. *United States v Quintana*, 508 F. 2d 867, 874 (7th Cir. 1975), see Hubbard, Brauti and Fenton *Wiretapping* at para 4.4.1 at page 4-44.

[1266] Para 2.6.2 of Chapter 2 of this study.

[1267] Para 6.5 of Chapter 6 of this study.

[1268] Paras 6.3.3.2(e), 6.3.3.3(e), 6.3.3.4(d) and 6.3.3.5(e) of Chapter 6 of this study.

[1269] Paras 6.3.3.2- 6.3.3.5 and 6.4.5 – 6.4.8 of Chapter 6 of this study.

[1270] Para 3.5.7.14 of this chapter.

3.5.7.9 Decent and orderly manner of investigation in offline communication

Given that great caution is exercised in the protection of offline privacy by ensuring that investigations are conducted in a decent and orderly manner[1271] and that the search is conducted in the presence of the suspect —if the suspect is available— while the LEA departs thereafter,[1272] there ought to be stricter protection for an online communication than offline privacy based on the high sensitivity and risky features of the former.[1273]

It is submitted that in interpreting the entire provisions of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, more particularly the broad meaning of an 'article',[1274] section 36(1)(a) and (b) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 applies to the conduct of an OCI which means that the conduct of an OCI must be done in a decent and orderly manner and proportionately too,[1275] otherwise, a LEO will be held liable for knowingly carrying out an unlawful order.[1276]

3.5.7.10 Exposure of online privacy to a limited number of law enforcement agencies and officers in online criminal investigation

Some of the government departments and agencies are empowered to conduct offline criminal investigations[1277] given the low level of risk in non-online communications. Nonetheless, due to the higher levels of risks and protection involved in online communication than the non-online communication, the provisions of RICA permit only six categories of LEAs to conduct

[1271] Section 29 of CPA, section 29(2)(a)-(c) of NPA Act, section 34(1)(a) of the CCB B6-2017 which is replaced by section 36(1)(a) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, Chapter 4 of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 and preambles of RICA and the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017; *Investigating Directorate v Hyundai and Smit No* supra 19, 40 and 51 and *Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others* (CCT 89/07, CCT 91/07) [2008] ZACC 13; 2008 (2) SACR 421 (CC) 86, 138, 139 and 148.(*Thint v NDPP*); Section 105 (1) and (2) of the Consumer Protection Act 68 of 2008('COPA'); Section 84(7) of the POPIA.

[1272] McQuoid-Mason *Privacy I* 146.

[1273] See paras 3.5.7.6 and 3.5.7.8 of this chapter.

[1274] See the definition of 'article' in section 1 of CCB B6-2017, which is replaced by section 1 of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

[1275] Section 34(1)(a) of the CCB B6-2017, which is replaced by section 36(1)(a) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

[1276] Right2Know 'Spooked- Surveillance of Journalists in SA' at 13-14 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018 (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[1277] See section 1 of RICA and para 2.11 of Chapter 2 of this study.

an OCI to control its use or abuse[1278] which, arguably, is a strong indication of the greater risks involved in the conduct of an OCI than in non-OCI.

However, although this study advocates for the inclusion of more statutory authorities and private entities such as the Chapter Nine Institutions[1279] and robotic investigators[1280] to further guarantee their independence and enforcement respectively in the conduct of an OCI, the list of LEAs qualified to conduct an OCI should not be endless, subject to condition.[1281] Although there is a greater expectation of privacy in online communication in terms of the number of authorities qualified to conduct an OCI than in non-OCI, however, this study does not advocate for a flood gate for all authorities or entities to conduct an OCI in the RSA.

3.5.7.11 Severity of sanctions against law enforcement officers for non-compliance in online criminal investigation

Although there may not be any imposition of a criminal sanction in the unlawful infringement of privacy in some instances in both online and offline communications due to the grant of indemnity,[1282] however, there is a specific and general criminal sanction for the wrongful

[1278] The LEAs that are permitted to use OCI are the CI-SAPS, DPCI-'Hawks', IPID, ID-NPA, SSA and DI-SANDF. See section 1 of RICA and para 2.11 of Chapter 2 of this study. It is noted that section 24 of the CCB B6-2017 broadly identifies SAPS and any other person or agency who or which is empowered in other laws to conduct an OCI. For the disqualification of NPA as a LEA in OCI, see para 5.3.1 of this study, see also *Hugh Glenister v President of the Republic of South Africa & Others* [CCT 48/10] 2011 ZACC 6.

[1279] Para 4.2 of Chapter 4 of this study.

[1280] Para 2.11 of Chapter 2 of this study.

[1281] Para 4.2 of Chapter 4 of this study.

[1282] See the concluding part of para 3.10 of this chapter. Section 204 of the CPA is a general law that empowers the court to indemnify a witness from prosecution if the witness is found to be complacent in the case but is saying the truth as a witness. It is noted that the power of the court in indemnifying a witness from prosecution if the provisions of RICA are infringed under section 204 of the CPA —by virtue of section 51(7) of RICA— may encourage the infringement of the right to privacy in online communications by LEAs. This is because it will be seen as an escape route for LEAs to easily rely on if there is an unlawful interception which will ultimately defeat the purpose of the provision for criminal sanction in the infringement of the right to the SOC. While SABC reports that there was a decrease in the number of OCI application brought before the designated judge in 2017/2018 financial year report by the designated judge, this does not necessarily mean that there was a drop in the conduct of an OCI because the designated judge admitted that since the nature of scope of the function of an interception judge ends in the office and not in any technical intervention due to the loopholes in the provisions of RICA. It is therefore not surprising to note that the Daily Maverick report in 2018 says that 95 % of interception that takes place are never directed by the court in the RSA, which suggests that the reduction in the official application of an OCI is as result of the loopholes in RICA which continue to trigger unlawful conduct of an OCI, see Phillip B 'Interception of communication applications decrease' http://www.sabcnews.com/sabcnews/interception-of-communication-applications-decrease/ (Date of use:12 January 2019) (Phillip B http://www.sabcnews.com/sabcnews/interception-of-communication-applications-decrease/ (Date of use:12 January 2019) and Swart H 'Your cell phone records and the law: The legal loophole that lets state spying run rampant' https://www.dailymaverick.co.za/article/2018-05-20-your-cellphone-records-and-the-law-the-legal-loophole-that-lets-state-spying-run-rampant/ (Date of use:_12 January 2019)

conduct of an OCI[1283] which is effectively and cumulatively greater than the sanction for the wrongful invasion of non-online channels of data communication.[1284]

This is because while both RICA —substantially cater for online communication— and the POPIA (which does not substantially cater for online communication) provide for 10 years maximum imprisonment for non-compliance and that plea bargain is generally lawful in the RSA. However, reading together sections 107(a), 108 and 109(2)(c),(d)(i)-(iii) and (e) and (4) -(8) of the POPIA, it is clear that the criminal provisions in the POPIA are alternatives, quasi or far less criminal and almost elastically negotiable in nature and practice.

This is based on the presumption that where an infringer has the right to negotiate in section 109 (2)(d)(iii) and (4)-(8) of the POPIA, it is an indication that the Magistrate Court may not impose the maximum penalty as opposed to the general punishment in the CPA which does not make provision for same or similar negotiable criminal sanction. The criminal provisions in RICA are characterised by the usual criminal punishment which does not provide for negotiation of punishment to the extent that the POPIA does, therefore the distinction indicates the higher risks observed and protection accorded in online communication in RICA than an offline communication in the POPIA.

It is important to note that although section 14 of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 makes provision for 15-year imprisonment, this provision should not be mistaken for the imposition of a sanction for non-compliance with the investigative procedure or provision in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017. Rather, section 14 provides for the breach of substantive law in the commission of cybercrime which is not the yardstick for comparison under this rubric 'severity of sanctions against LEOs in conducting an OCI'.[1285]

(Swart H https://www.dailymaverick.co.za/article/2018-05-20-your-cellphone-records-and-the-law-the-legal-loophole-that-lets-state-spying-run-rampant/ (Date of use:12 January 2019).

[1283] Para 3.10 of this chapter; Section 28(1) of CPA; Section 51(1)(a) and (b) of RICA; See generally, amongst others, chapters 2, 3 and 4 of the CCB B6-2017, more particularly sections 14 and 22 which impose 15 years for the commission of an offence; Section 84 of the ECTA; Sections 49-51 of RICA.

[1284] See Chapter 11 of the POPIA. See also para 3.10 of this chapter for the description of the severe sanctions for non-compliance with the rights in online communication.

[1285] Sections 2-13 of the CCB.

Put differently, this study does not, at all costs, create an impression that section 14 nullifies the submission in the immediate paragraph about the maximum punishment which is generally and cumulatively higher in RICA than in the POPIA to build false or unmerited support for greater sanction in the breach of online communication than in non-online communications. The comparison of RICA and the POPIA in this rubric above relates to the non-compliance with the adjectival or procedural aspects of these Acts in conducting an investigation and not concerning the non-compliance with the substantive aspects of RICA and the POPIA.

Therefore, from the foregoing analysis, the 15-year imprisonment in section 14 of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 is irrelevant to use as the basis for the conclusion that there is a severe punishment against LEOs for non-compliance in the conduct of an OCI than in the conduct of a non-OCI.

Nonetheless, concerning the imposition of a fine for non-compliance, section 109(c) of the POPIA imposes a fine of not more than R10 million for non-compliance with the POPIA, which is higher than the penalties in the ECTA, RICA and Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017. However, the fine in the POPIA is an administrative, civil and non-mandatory fine because the fine in the POPIA is not imposed as a criminal committal neither is the fine imposed in addition to a custodial sentence[1286] as opposed to the ECA, ECTA, RICA and Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 which have compelling custodial punishment.

Moreover, given that the POPIA provides for the regulation of both offline and online privacy —though there is more protection for the former, it is submitted that it is unlikely that an administrative fine only will be sufficiently imposed for the breach of online communication in the POPIA. This is because there are higher risk levels in online communication[1287] than in offline privacy and the greater intent of penalties which specifically cater for online communication in the ECA, ECTA RICA and Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 than in the POPIA.

[1286] Section 109(2) (d) (i) -(iii), (e) and (4) -(8) of the POPIA
[1287] See generally Chapter 2 of this study, more particularly paras 2.3, 2.5- 2.10 and 2.11.4.

Furthermore, though RICA has been in existence since 2002, in which the Act should have recorded more prosecuted cases than expected thus far,[1288] however, no prosecuted case whatsoever has been reported in favour of the POPIA to demonstrate the enforcement of the Act,[1289] which shows that there is more enforcement of the penalty in RICA —no matter how little penalties have been recorded— than in the POPIA. The enforcement of the provisions in RICA is arguably an indication that there is the tendency to regard infringement of online communication on a higher level than the infringement in offline privacy which is mainly regulated by the POPIA. In an unreported case of the first successful prosecution of a LEO for non-compliance with RICA, a former CI-SAPS was convicted in August 2017 for unlawfully spying on the online communication of an individual.[1290]

Consequently, in the overall analysis, there is a strong indication that there are general and cumulative severe sanctions against LEOs for non-compliance in the conduct of an OCI in online communication than the sanctions against LEOs for non-compliance in the conduct of non-OCI in non-online communications because of the higher levels of risks in the right in online communication than in non-online communications.

3.5.7.12 Lack of protection of third-party interest in online criminal investigation

The privacy of a third party who is not a target of search and seizure in offline privacy is more often than not, observed, respected, and protected[1291] but not the privacy of a third party in an online communication where every third party that an individual —or a target— communicates with[1292] is intercepted or monitored in the non-compartmentalisation and non-passworded online communications.[1293]

[1288] Defenceweb 'Former police crime intelligence officer guilty of phone spying https://www.defenceweb.co.za/security/national-security/former-police-crime-intelligence-officer-guilty-of-phone-spying/ (Date of use: 27 September 2018).

[1289] United Nations para 42 at 8 https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fZAF%2fCO%2f1&Lang=en (Date of use:18 January 2019); Michalson https://www.michalsons.com/blog/un-human-rights-committee-concerned-about-privacy-and-interc (Date of use:18 January, 2019).

[1290] Defenceweb https://www.defenceweb.co.za/security/national-security/former-police-crime-intelligence-officer-guilty-of-phone-spying/ (Date of use: 27 September, 2018).

[1291] *Fikizolo Norman Khosana and Another v The Minister of Safety & Security N.O. & Others* Case No.: 2512/08 paras 11, 12, 13, 14, 16 and 40 (*Khosana v Min of Safety*). Offline privacy is protected in privilege communication between an attorney and client even where the client is a third party in the investigation involving one of the clients of the attorney, see *Thint v NDPP* supra 145, 196 and 208.

[1292] *Absa v Moller* supra 3; Para 6.14 of Chapter 6 of this study. *AmaBhungane v Minister of Justice* supra 26, 40, 109, 110, 130, 133 and 135.

[1293] Para 2.3.1 of Chapter 2 of this study.

Despite the provision for the legal protection of third-party rights[1294] and legitimate interests in section 36(1)(b) the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017,[1295] the natural technical operations of online communication are not capable of protecting third party rights. For example, the prayers in *AmaBhugane* in the High Court[1296] sought to, amongst others, protect third-party rights in an online communication regarding the privileged communication between an investigative journalist and a whistle-blower.[1297] Therefore, there ought to be a higher technical level of privacy protection in online communication than in the offline world.

It is however noted that section 57 of the CCB —which is expunged in the Cybercrime Bill 2018- Amendments Proposed to Bill B6-2017— proactively provided that the government of the RSA had the power to control, and manage the configuration and maintenance of equipment, software, hardware and cyberinfrastructure of government which has public interests only.[1298] However, section 57 omitted the provision for the configuration of online communication devices concerning ordinary private individuals whose communications are not declared as a critical information infrastructure.[1299] It is important to note that few commercial and expensive compartmentalised and passworded compartmentalised o-mail services exist which are not within the reach of an average user of online communication devices in the RSA.

However, in practical terms, section 57 does seem to be an unenforceable and ineffective provision because it domestically cedes into the South African government the technical power and rights to configure or reconfigure internetworking of computers which lie in the US authorities, though subject to the submissions that the U.S. authorities still do not have right or power to grant consent for the conduct of an OCI in an Internet-based platform of serious

[1294] See the definition of 'third party' in s 1 of ECTA.
[1295] Section 34(1)(b) of CCB B6-2017.
[1296] *AmaBhungane v Minister of Justice* supra 168.
[1297] *AmaBhungane v Minister of Justice* supra 26, 40, 109, 110, 129, 130, 133, 135, 137 and 168. See para 6.14 of this study on the examination of the general protection of privileged communication between a professional trustee and a party.
[1298] Section 57 of CCB B6-2017; Minnaar 2016 29(2) *Acta Criminologica*: *Southern African Journal of Criminology* at 123. The infrastructure includes a lifesaving medical equipment that substantially operates on computerised equipment, Rooyen H J N *Investigate corruption* (2013) 265.
[1299] Section 57(1), (2), (3) (i) (i) -(v) of CCB B6-2017; Minnaar 2016 29(2) *Acta Criminologica*: *Southern African Journal of Criminology* at 135.

offences committed in the RSA.[1300] Therefore, it is concluded that there is lack of protection of third party interest or right who is not a target in the conduct of an OCI against an identified target.

In summary, aside from the other recommendations under similar rubrics,[1301] it is proposed that the *2-3 minutes* periodic conduct of an OCI be adopted which entitles the LEAs or LEOs conduct a re-assessment of whether to commence or continue with the conduct of an OCI against a third party.[1302]

3.5.7.13 Specific statutory and uniform online method of investigation of serious offences

On the one hand, save in rare cases of some serious offences that require specific offline methods to investigate,[1303] no statutory and uniform or specific provision generally limits the use of offline methods to investigate serious offences only.[1304] This is arguably a strong

[1300] Para 2.18 of Chapter 2 of this study; Lehman BA "Intellectual property and the national and global information infrastructure", WIPO Worldwide Symposium on Copyright in the Global Information Infrastructure, Mexico City (22–24 May 1995) 76; Hance O *Business and law on the Internet* trans (1996) 39-40; Gringras C *The laws of the Internet* (1997) 2; Downing, Covington and Covington *Dictionary of computer and Internet terms* 243; Popoola *Liability of ISPs* para 2.2; See Ax J 'U.S. judge orders Microsoft to submit customer's emails from abroad' 1-2; Rosenblatt B 'Principles of Jurisdiction' 1 - 9 http://cyber.law.harvard.edu/property99/domain/Betsy.html (Date of use: 2 July 2015) (Rosenblatt 1 - 9 http://cyber.law.harvard.edu/property99/domain/Betsy.html (Date of use: 2 July 2015); Cajani F 'Communication interception regarding Google, Microsoft and Yahoo! Tools and electronic data retention on foreign server: a legal perspective from the state which is conducting an investigation' 1-7 www.iisfa.eu (Date of use: 8 June 2013) (Cajani 1-7 www.iisfa.eu (Date of use: 8 June 2013) (Cajani 'Communication interception: electronic data retention on foreign server'); Kravets D 'Obama administration says that the world's servers are ours: US says' https://www.google.co.za/?gws_rd=ssl#q=Obama+administration+says+the+world%E2%80%99s+servers+are+ours (Date of use: 2 July 2015) Kravets https://www.google.co.za/?gws_rd=ssl#q=Obama+administration+says+the+world%E2%80%99s+servers+are+ours (Date of use: 2 July 2015); Kravets D 'Microsoft tells US: The world's servers are not yours' 1-2 http://arstechnica.com/tech-policy/2014/12/microsoft-tells-us-the-worlds-servers-are-not-yours-for-the-taking/ (Date of use: 2 July 2015) Kravets http://arstechnica.com/tech-policy/2014/12/microsoft-tells-us-the-worlds-servers-are-not-yours-for-the-taking/ (Date of use: 2 July 2015).

[1301] Paras 3.5.7.8 and 6.14 of this study.

[1302] Para 3.5.7.8 of this chapter.

[1303] Section 13(8)(d)(i) and (g) of SAPS Act; Schedule 1 to CPA. Section 13 (6) of SAPS Act section 25 of CPA; Basdeo 2009 *PER* (12)4 311, 319, and 325- 327/360. Section 28(13) and 28(14) of the NPA Act 32 of 1998; see *Investigating Directorate v Hyundai and Smit No* supra 1, 2, 3, 44, 45, 46, 47, 48, 49, 51 and 53 and *Thint v NDPP* supra 50, 74, 115, 124, 140, 142, 151-155, 160, 161, 167 and 221, Section 28 and 29 NPA Act. Other specific methods of investigations of some offences include sections 36B(1)(a) and (c), 36C(1)(a), 36D and 36E(1)(a) of CPA.

[1304] The law provides for the general use of offline warrant and warrantless searches and seizures for the investigation of all categories of offences, see Chapter 2 of the CPA; *Minister of Safety & Security v Antus Van Niekerk* [2007] ZACC 15 paras 2, 8, 11, 17 and 19 (*Min of Safety v Van Nierkerk*); See para 2.11 of Chapter Two of this study. The general use of warrantless searches for all offences has been condemned by the Constitutional Court in *Estate Board v Auction Alliance* supra 33, 37, 40, 41 and 43; Basdeo 2009 (12)4 *PER* 2009 308/360. See para 5.3.6 of Chapter 5 of this study on the proportionality of the limiting measure in

indication that offline investigative methods are used for all categories of offences —including less serious offences— because of the relatively low risks involved in the protection of offline communication which accommodates an offline investigation.

On the other hand, given that RICA excludes the conduct of an OCI of less serious offences but specifies that it is used for the investigation of serious offences *only* as defined in RICA and conceptualised in this study[1305] is arguably a very strong indication that an OCI is a unique, risky and complex method that should not be used to investigate all categories of offences including less serious offences. This is because doing so would unreasonably and unjustifiably further[1306] expose online communication to the inherent and higher risks involved in the protection of online communication than in non-online communications,[1307] given the high frequency at which the conduct of an OCI for every category of the offence will unnecessarily, unreasonably and unjustifiably enable a consequential intrusion into online communication.

Furthermore, assuming —though without conceding— that there are specific or uniform offline methods to investigate serious offences, there is an 'absence of strict requirement, as precondition'[1308] to engage in such offline search, unlike the use of an OCI which requires strict conditions before interception occurs[1309] because of the higher risks and protection of online privacy than offline privacy.

---

privacy matters. Basdeo *PER* 2009 (12) 4 325- 327/360. The power to search must not be overbroad, see *Gaertner v Min of Finance* supra 65 and *Mistry v Medical and Dental Council* supra 30; *Thint v NDPP* supra 124, 131 and 132 and *Isaac Metsing Magajane v The Chairperson, North West Gambling Board and Others* Case CCT 49/05 para 50 (*Magajane v North West Gambling Board*); *Patrick Lorenz Martin Gaertner & others v Minister of Finance & Others* [2013] ZACC 38 para 65 (*Gaertner v Min of Finance*); *Min of Safety v Van Nierkerk* supra 14, 15, 17, 18 and 20. See para 5.3 of Chapters 5 and 6 of this study. See *Mistry v Medical and Dental Council* supra 30; *F v Min of Safety* supra 146; Section 40 of the CPA and *Minister of Safety and Security v Luiters* [2006] ZACC 21; 2007 (2) SA 106 (CC); 2007 (3) BCLR 287 (CC) para 35. Section 36 of the Constitution; *Bernstein v Bester No* supra 30, 31, 39, 60, 61, 90 and 94. *Mistry v Medical and Dental Council* supra 29 and 30 and *Estate Board v Auction Alliance* supra 40-42, 62 and 64-65 made a distinction between the two searches. *Bernstein v Bester No* supra 3, 7, 9, 12, 13, 15, 16 (c), (f) - (h), (j), (k), 17-20, 23, 24, 25, 26, 27, 30, 31, 33, 34, 35, 36, 38, 40, 46, 47, 50, 55, 60, 89, 94, 102, 111, 112 and 121 and *Investigating Directorate v Hyundai and Smit No* supra 44; See also the following for other principles guiding the choice and proportionality of method of investigation for an offence: *Thint v NDPP* paras 75, 86, 271 and 380-381; *Helling v Mag* supra 110; *Gaertner v Min of Finance* supra 50-54, 65 and 78; *Min of Safety v Van Nierkerk* supra 11, 14, 15, 17, 18 and 20. In *Bernstein v Bester No* supra 23 - 27, the Constitutional Court in referring to some foreign cases held that an intrusive measure can be used for a serious offence or 'an exceptionally pernicious form of crime'.

[1305] Para 6.3.2 of Chapter 6 of this study.

[1306] Paras 2.2.2.2, 2.3.1 -2.3.3, 2.5, 2.6, 2.7, 2.8, 3.4.5, 3.5.7.2 - 3.5.7.12 of this study.

[1307] Paras 2.2.2, 2.3.1 – 2.3.3, 2.5, 2.6, 2.7, 2.8, 3.4.5 and 6.3 of this study.

[1308] *Simataa v Magistrate of Windhoek* supra 20. Sections 1 and 16 and Schedule 1 of RICA. *Estate Board v Auction Alliance* supra 34; Para 6.5 of Chapter 6 of this study.

[1309] See section 1 of the Schedule to RICA; Paras 6.4 and 6.5 of Chapter 6 of this study.

Based on the foregoing discussion, it is concluded that because an OCI is a specific and uniform method of investigation of serious offences *only*, whereas other methods of investigations are used for the investigation of all categories of offences strongly indicate that there are higher risks involved in the conduct of the former than the latter.

3.5.7.14 Mandatory direction of the court for online criminal investigation

The law is that in offline privacy, there is a general 'absence of strict requirement, as precondition'[1310] to engage in such offline search. However, the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 —which is a bill— has in its definition of the term 'article' broadened the scope of search without a warrant which includes the conduct of an OCI, which contradicts the object of RICA —as the main law in this regard.[1311] RICA requires that court direction must be obtained before an interception occurs[1312] save in some exceptional circumstances[1313] and as canvassed in this study.[1314]

The Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 implies that a search warrant is not mandatory to be issued in some circumstances before a LEA searches an article.[1315] The search, according to the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, arguably includes the controversial search of an offline mobile cellular telephone[1316] or premises based on the reasonable ground to believe[1317] that a warrant would be issued but not

[1310] *Simataa v Magistrate of Windhoek* supra 20. Sections 1 and 16 and Schedule 1 of RICA. *Estate Board v Auction Alliance* supra 34.

[1311] This is in furtherance of sections 29 -31 of CCB B6-2017, which controversially allow the search of any article which is in direct control of an arrested person. These provisions are replaced by sections 3-33 of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017. See *State v Miller* supra 72 and *State v Terrence Brown* supra 5 and 6. See the preamble of RICA.

[1312] Court direction is also required in oral interception and preservative order applications in s 23 of RICA and Sections 40-43 of CCB B6-2017 (which are replaced by sections 42-45 of the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017); Articles 29(3), (4) & (5), 31(3)(a) of Council of Europe 'Chart of Signatures and Ratifications of Treaty 185-*Convention on Cyber Crime* -Status as at 02/06/2017 (CoE CoCC).

[1313] See sections 4-11 of RICA.

[1314] Paras 2.11.3, 2.11.4 and 6.2.2-6.2.6 of this study.

[1315] This is in furtherance of sections 29-31 of the CCB B6-2017, which controversially allow the search of any article which is in direct control of an arrested person. These provisions are replaced with sections 31-33 of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017. See *State v Miller* supra 72 and *State v Terrence Brown* supra 5 and 6. See the preamble of RICA.

[1316] This is in furtherance of sections 29-31 of CCB B6-2017, which controversially allow the search of any article which is in direct control of an arrested person. These provisions are replaced by sections 31-33 of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017. See *State v Miller* supra 72 and *State v Terrence Brown* supra 5.

[1317] Para 6.4 of Chapter 6 of this chapter.

applied for due to envisaged delay of issuance of a warrant or where the person concerned consents to the search.[1318] However, in South Africa, support is being canvassed for the position that a warrant ought to be obtained before an offline cell phone is searched.[1319]

This support is strengthened by the US Supreme Court consolidated cases of *Riley v California* and *US v Wurie*,[1320] which prohibit the search of an offline mobile cellular telephone without a search warrant when a suspect is arrested.[1321]

The scope of this study does not cover the search of an offline mobile cellular telephone. However, it is submitted that the non-requirement of a search warrant in an offline mobile cellular telephone should generally be applied proportionately concerning, amongst other exceptional circumstances or factors,[1322] the *absolutely irreversibility* of the effect of the commission of a serious offence as espoused in this study subject to the *strict* proof of the relevant standards of proof.[1323]

Given the higher risk levels in online communication,[1324] the requirement of mandatory interception order ought to be considered in favour of a higher level of protection for data in online communication than the data in non-online communication. This is notwithstanding the use of the word 'may' in the provision for the conduct of an OCI,[1325] which still does not make the application for the conduct of an OCI discretionary, keeping in mind the overall object of RICA as opposed to the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, which is a bill. The use of the word 'may' is not a blanket provision but only applies to sections 4 - 11 of RICA[1326] and other circumstances, which arguably include where an AI is used to intercept automated substances.[1327]

[1318] Section 22(a) and (b) and 40 of CPA.
[1319] Van der Berg 1 http://ohrh.law.ox.ac.uk/mobile-phone-evidence-implications-for-privacy-in-south-african-law/ (Date of use: 25 June 2013).
[1320] Supreme Court of the United States consolidated cases of *Riley v California* and *US v Wurie* supra 3 of the Syllabus and 19-20 of the Opinion.
[1321] Sections 22 and 25(3) of CPA; Rosen http://www.newrepublic.com/article/118396/supreme-court-cellphone-case-went-further-privacy-advocates-hoped (Date of use: 30 June, 2014).
[1322] Other circumstances include the 'Necessity' principle, see para 6.5 of Chapter 6 of this study.
[1323] Paras 3.5.7.2, 5.3.4, 5.3.6, 5.4, 6.3.3.4, 6.4, 6.5 and 6.6 of this study.
[1324] See generally Chapter 2, more particularly paras 2.2, 2.3 and 2.8.
[1325] Section 16(1) of RICA.
[1326] Para 6.2 of Chapter 6 of this study.
[1327] Chapter 2 (paras 2.11.3 and 2.11.4) of this study.

3.5.7.15 Conclusion

In the examination of the thirteen-point criterion,[1328] all of which is cumulatively in favour of higher levels of risks and protection of data in online communication than in non-online communications, it is submitted that the scale thereof tilts in favour of the right to the SOC than in other channels of data communication.[1329]

While the right to the secrecy of telecommunication is expressly and unequivocally recognised in the European Union instruments, the right is not expressly protected under the South African and American Constitutions but impliedly or unintentionally interpreted and acknowledged by the courts and scholars in diverse ways in both countries.[1330] Above all, whatever interpretation that the RSA may subscribe to in terms of the applicable law on the protection of online communication, it is trite that the interpretation or conceptualisation of cyberlaw as coded in the European Union instruments ought to globally and uniformly apply in the same regard in the RSA because of the global and uniform features of the operations of online communication devices, technologies, networks, applications and services.

The right to the SOC is a complex one, which entails and gives meaningful effect to the techno-legal issues dealt with in this study, namely the non-compartmentalised, non-passworded compartmentalised, interoperable, conscriptive, inherently risk-based and fiduciary relationship-based online communication issues.[1331] In attempting to give effect to the right to the SOC, it is expressed in two distinct ways.

First, it is a right to the protection of online communication which is independent of the conduct of an OCI. Second, it is the right to the protection against unlawful conduct of an OCI. In the latter right, because of the existence of the infringement of online communication at the pre-OCI, actual OCI, post-OCI and distribution stages,[1332] a LEA must observe the right of a user of online communication, which should not be less than the right to the SOC.

[1328] Paras 3.5.7.2 - 3.5.7.14 of this chapter.

[1329] See amongst others, chapters 2, 3, 7, 9, 10 and 11 of CCB B6-2017 where the proposed legislation places emphasis on the high level of risk in online communications.

[1330] *Absa v Moller* supra 2, 3, 13 and 18; *Katz v U.S*. 347; *Maryland Penitentiary v Hayden*, 387 U.S 294 (1967); Ruiz *Privacy in telecommunications* 22, 59, 61-62, 70, 86-87 and 175-176; *Riley v California* and *US v Wurie* supra 1-4 of the Syllabus and 4, 8-12, 17-21, 24 and 25 of the Opinion and 4 and 5 of the minority judgment of Alito J.

[1331] See paras 2.2.2 and 2.3.1 -2.3.3 of Chapter 2 and paras 3.5.7.2-3.5.7.14 of this chapter.

[1332] Para 5.2.2 of Chapter 5 of this study.

3.6 LEGITIMATE EXPECTATION OF THE SECRECY OF OFFLINE AND ONLINE COMMUNICATION

3.6.1 Introduction

A legitimate or reasonable expectation of privacy is a concept identified in the meaning of the concept of privacy by the Constitutional Court in *Bernstein v Bester NO*,[1333] comprising two components that an individual must establish which make up the meaning of the concept. Firstly, an individual must have *a subjective expectation of privacy'*. Secondly, society recognizes the individual '*expectation as objectively reasonable*'.[1334]

One of the important issues in the examination of the concept of the expectation of privacy is the protection of 'private facts'.[1335] According to the Constitutional Court, private facts are 'those matters, the disclosure of which will cause mental distress and injury to anyone possessed of ordinary feelings and intelligence in the same circumstances and in respect of which is a will to keep them private'.[1336]

Borrowing from the US jurisprudence in online communication, the disclosure of the enormous quantitative and qualitative data in online communication —which is irreparable— is stressful for any individual who expects that an online agent will keep his 'private facts'[1337] secret in the inherent risk-based, non-compartmentalised, non-passworded compartmentalised, interoperable, conscriptive and ubiquitous online communication networks.[1338]

It has been held that the scope of protection of the right to privacy falls within the ambit of what a legitimate expectation of privacy can accommodate.[1339] Similarly, it is submitted that the scope of the right to the SOC falls within the scope of what a legitimate expectation of secrecy can be accommodated in online communication. The scope of the legitimate

---

[1333] The second component is the 'reasonable continuum of privacy interest', see para 3.8 of this chapter; *Bernstein v Bester NO* supra 65, 74, 75, 76, 78, 85 and 93.
[1334] *Bernstein v Bester NO* supra 75- 76; Currie 2008 3 *TSAR* 551-552; Currie and De Waal *Bill of Rights* 297-298.
[1335] *Bernstein v Bester NO* supra 69.
[1336] *NM v Smith* supra 34 and 142-143.
[1337] *Riley v California* and *US v Wurie* supra 3 of the Syllabus and 19 of the Opinion. *Bernstein v Bester NO* supra 75 and 77. Currie 2008 3 *TSAR* 552.
[1338] See paras 2.2.2 and 2.3.1 - 2.3.3 of Chapter 2 of this study.
[1339] *Bernstein v Bester NO* supra 75 and *Mistry v Medical and Dental Council* supra 27.

expectation of secrecy of an online communication covers the sub-rights, interests and values examined in this chapter.

These are the sub-rights, interests and values to: personhood, human dignity and autonomy; intimacy; to be left alone; limit access to the self; access to control online communication; control and protect the intangible, intellectual and invaluable property or treasure; controlled online conscription and ultimately, the integrity and security of basic online communication, all of which should be included or considered for inclusion in the Constitution.[1340]

3.6.2 The subjective expectation of the secrecy of online communication

According to the Constitutional Court in *Investigating Directorate v Hyundai and Smit No*, 'Wherever a person has the ability to decide what he or she wishes to disclose to the public and the expectation that such a decision will be respected is reasonable, the right to privacy will come into play'.[1341] There is no contemplation of any reasonable expectation of privacy in what an individual physically exposes to the public on a daily basis.[1342]

Therefore, drawing on the foregoing analysis, it is submitted that given the inherent fiduciary relationship in the risk-based online communication between an online communication agent and user, an individual has the right to determine his or her expectation by way of choosing what and where to disclose in the five levels of the continuum of secrecy interests in online communication which must be respected by the society.[1343]

3.6.3 The objective reasonableness of the secrecy of online communication

The subjective expectation component of the legitimate expectation of privacy is regulated by the component of the objective reasonableness of the society, (*boni mores*) and the legal conviction of the community as perceived by the court.[1344] Reasonableness is determined by a set of values that one attaches to the 'empty standard of reasonableness'[1345] or attaches to the

[1340] Paras 3.4.4.2 – 3.4.4.6, 3.4.5.2 – 3.4.5.5 and 3.11 of this chapter.
[1341] *Investigating Directorate v Hyundai and Smit No* supra 16. *Bernstein v Bester NO para 68;* Ruiz *Privacy in telecommunications* 39.
[1342] *Bernstein v Bester NO* supra 68; *US v Dionisio* 410 US 1 (1975) and *US v Mara* 410 US 19 (1973) 21.
[1343] See para 3.8 of this chapter.
[1344] *Bernstein v Bester NO* supra 68, 70 and 71 and 75.
[1345] Currie and De Waal *Bill of Rights* 298.

dynamic, and robust concept of reasonableness. A court must not only consider the reasonableness of the current mood of the community but also the 'long-term community values.[1346]

Nonetheless, the fact that technology is fast developing globally, it is submitted that the concept of online communication is elastic in nature and features and reasonably accommodates the current and future standards and values of the community. However, it is regrettable that this global development was not favourably taken into consideration by the courts in the erroneous decisions in *State v Terrence Brown*[1347] and *State v Miller*.[1348]

In summarising the facts and ratio of these cases according to the global uniform and unique features and nature of online communication and without making any reference to any foreign jurisdiction, the courts regard the risks and protection levels of offline and online privacy to be the same.[1349] The finding of the courts contradicts the gravamen of this study by not taking into consideration the dynamic, delicate and complex unique nature and features of online communication which would have made the court to hold otherwise, which is to the extent that online privacy has a heightened risk and protection than offline privacy.[1350]

3.7 THE REASONABLE CONTINUUM OF SECRECY OF OFFLINE COMMUNICATION INTERESTS

3.7.1 Introduction

A reasonable continuum of privacy interest is the second component identified in the meaning of privacy by the Constitutional Court in the *Bernstein v Bester NO* which holds that privacy lies along a continuum of interests.[1351] In *Thint v NDPP*, the Constitutional Court emphasises the fact that the level or continuum of protection of privacy must be understood according to

[1346] *R v Collins* supra 136; Schwikkard P J 'Arrested, detained and accused persons' in Currie I and De Waal J *The bill of rights handbook* (2014) 809-810 (Schwikkard *Arrested, detained and accused persons*).
[1347] *State v Terrence Brown* supra 29-31. Section 180 (a) and (c) of the Constitution.
[1348] *State v Miller* supra 38.
[1349] *State v Terrence Brown* supra 29-31. Section 180 (a) and (c) of the Constitution; *State v Miller* supra 38.
[1350] See Chapter 2 (more particularly paras 2.2, 2.3 and 2.8) of this study.
[1351] *Bernstein v Bester NO* supra 67 and 77, *Gay and Lesbian v Min of Home Affairs* supra 29 – 32, *Mistry v Medical and Dental Council* supra 22-23, 25, 27 – 30; *F v Min of Safety* supra 91 and *Investigating Directorate v Hyundai and Smit No* supra 15.

the different stages of the investigation and trial of serious and complex offences.[1352] The axiom that no right is absolute implies that every right is already limited by the adverse rights belonging to other individuals in the continuum of privacy interests.[1353] The three levels of sanctum identified by the courts are examined in the offline continuum of privacy interests.[1354]

3.7.2 Inner sanctum

In *Bernstein v Bester No,* the Constitutional Court identifies the 'most intimate core', inner sanctum or the truly personal realm of an individual, which is narrowly construed[1355] and enjoys the highest level of protection.[1356] This sanctum is the deepest part of an individual from which the conflicting right of the society is shielded.[1357] Privacy is intense when it shifts into the inner realm of a person.[1358] This sanctum is regarded as the situation of 'relatively impervious sanctum of the home and personal life.'[1359] It is an inviolable right of an individual in which no justifiable limitation can be allowed.[1360] The inner sanctum comprises the family life, sexual preference and home environment,[1361] whereas a corporate entity does not enjoy this deep level of privacy.[1362]

However, it is argued that though romance issues are not part of the legal corporate identity, the equivalence of this right is the legal, ethical and moral right to keep a business secret or intellectual property in this sanctum. In online communication, this sanctum is classified or identified as the innermost sanctum.[1363]

[1352] *Thint v NDPP* supra 80; *Estate Board v Auction Alliance* supra 63 where the Constitutional Court states that the legislature should be given the 'latitude to formulate the inner and outer reaches of the search power'.
[1353] *Bernstein v Bester NO* supra 67 and 77.
[1354] *Bernstein v Bester NO* supra 67 and 77, *Gay and Lesbian v Min of Home Affairs* supra 29–32, *Mistry v Medical and Dental Council* supra 22-23, 25, 27–30; *F v Min of Safety* supra 91 and *Investigating Directorate v Hyundai and Smit No* supra 15.
[1355] *Bernstein v Bester NO* supra 67 and 83; *NM v Smith* supra 33 and 135 and *Mistry v Medical and Dental Council* supra 27.
[1356] *Investigating Directorate v Hyundai and Smit No* supra 15.
[1357] *Bernstein v Bester NO* supra 67 and *NM v Smith* supra 130 and 131.
[1358] *Mistry v Medical and Dental Council* supra 27; *Bernstein v Bester NO* supra 18, 65 and 85; *F v Min of Safety* supra 91.
[1359] *Mistry v Medical and Dental Council* supra 27.
[1360] *Bernstein v Bester NO* supra 67 and 77.
[1361] *Bernstein v Bester NO* supra 67 and 77.
[1362] *Bernstein v Bester NO* supra 69 and 83.
[1363] See para 3.8 of this chapter for the examination of the five levels of continuum of online privacy interests. In *H v W* supra 19, three levels of continuum of privacy interests are also identified in Facebook namely 'Everyone-Public', 'Friends of Friends' and 'Friends Only'.

3.7.3 Middle sanctum

According to the Constitutional Court, this sanctum also contains private information such as medical information of an individual.[1364] The distinction between inner and middle sancta is the extent to which such information is objectively and genuinely disclosed in the public that it can no longer be regarded as being private in the inner sanctum.[1365] It is inconclusive to rely on the number of people that may have obtained knowledge of the private fact as the yardstick for disclosure of private fact to the public, thus, the disclosure must be objectively and genuinely done.[1366]

In this study, the middle sanctum exists, which is arguably regarded as the third level of the continuum of privacy interests in online communication.[1367] The first two levels in the continuum in online communications are the innermost and inner sancta,[1368] thus emphasises the broad needs, interests and values in the online communication sanctum and consequently, the inadequacy in the offline principle.

3.7.4 Communal sanctum

The Constitutional Court identifies the communal or outer sanctum or peripheral level in which the 'scope of personal space shrinks' as an individual moves away from the personal realm unto a space that is available to or accessible by the public, business —or artificial person— and societal relations and activities.[1369] The same court in *Bernstein v Bester No* also held that there is accordingly no reasonable expectation of privacy in the public sphere.[1370]

It is however important to arguably note that the court in *Bernstein v Bester No* did not hold that there is no privacy in the public sphere at all, it only impliedly held that there is a higher level of privacy protection in the private sphere than in the public realm.[1371] For example, firstly, publishing someone's photograph who is in a public place or private facts without their

[1364] *NM v Smith* supra 143.
[1365] *NM v Smith* supra 143.
[1366] *NM v Smith* supra 143.
[1367] Para 3.8.4 of this chapter.
[1368] Para 3.8.2 and 3.8.3 of this chapter.
[1369] *Bernstein v Bester NO* supra 67, 77, 83 and 85 and *NM & Others v Smith & Others* paras 135-136.
[1370] *Bernstein v Bester NO* supra 85.
[1371] *Bernstein v Bester NO* supra 67.

consent remains an invasion of privacy.[1372] Secondly, although LEAs have the right to search an individual on the street under section 22 of the CPA and sections 13(6) and 13 (7) and (8) of the SAPSA but the power does not extend to making such individual naked in the search process because of the various privacy implications,[1373] amongst other illustrations.[1374]

3.8 REASONABLE CONTINUUM OF SECRECY OF ONLINE COMMUNICATION INTERESTS

3.8.1 Introduction

In offline privacy, the Constitutional Court identifies three levels of the continuum of offline privacy interests,[1375] which are considered at different stages of crime investigation.[1376] These stages are classified by the Constitutional Court of offline privacy into *inner*,[1377] *middle*[1378] and *communal*[1379] *sancta* of *privacy interests.*[1380]

Nevertheless, the three levels of the continuum of offline privacy interests are too narrow to protect the high risks, volume and type of data in the interoperable, non-compartmentalised, non-passworded compartmentalised and conscriptive online communications[1381] when conducting an OCI. The three-level classification does not cater to the dynamic and multi-

[1372] *National Media v Jooste* supra 271 (A); *Mholongo v Bailey* supra 70.
[1373] Section 22 of CPA 51 of 1977; Sections 13(6) and 13 (7) and (8) of the SAPSA 68 of 1995; Basdeo 2009 (12) 4 *PER* 316/360- 319/360 and 326/360-328/360. Dlulane https://ewn.co.za/2018/10/28/people-who-share-malusi-gigaba-sex-video-could-get-in-trouble-with-the-law (Date of use: 27 January 2019); Paras 3.5.7.14 of this chapter.
[1374] Para 3.4.3.3 of this chapter.
[1375] See para 3.7.2–3.7.4 of this chapter. In the US, the continuum of privacy interests indicates what type of information requires greater or lesser privacy protection when conducting OCI procedure, Justice Information Sharing 'Electronic Communication Privacy Act 1986 (ECPA), 18 U.S.C s 2510-22' https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (Date of use: April 2 2016.
[1376] *Thint v NDPP* para 80.
[1377] *Bernstein v Bester NO* supra 18, 65, 67, 69, 77, 83 and 85; *Smith* supra 33, 130, 131 and 135 and *Mistry v Medical and Dental Council* supra 27; *Investigating Directorate v Hyundai and Smit No* supra 15, 18; *F v Min of Safety* supra 91.
[1378] *Smith* supra 143.
[1379] *Bernstein v Bester NO* supra 67, 77, 83 and 85 and *Smith* supra 135-136; *National Media v Jooste* supra 271; Section 22 of the CPA; Sections 13(6) and 13 (7) and (8) of SAPSA; Basdeo 2009 (12)4 *PER* 316/360-319/360 and 326/360-328/360.
[1380] *Smith* supra 33,130,131,143 and 135; *Mistry v Medical and Dental Council* supra 27; Sections 13(6) and 13 (7) and (8) of the SAPSA; Basdeo 2009(12)4 *PER* 316/360-319/360 and 326/360-328/360. The offline communication in government circle in the RSA and elsewhere is generally classified into *five* levels of privacy interests which are *public notice*, *private*, *confidential*, *secret* and *top secret*, Chapter XXVI Para 2(1) (a), (b) & (c) of Regulation 7797 Notice No. 1505 Gazette No 25592.
[1381] See para 2.3.1 of Chapter 2 of this study.

faceted, racial and cultural needs[1382] of the South African contemporary society.

Therefore, in pursuance of the combined effect of the spirit, purport and object of section 14(d),[1383] this study generally identifies and examines some guiding principles in five levels of the continuum of the SOC interests. Besides, these guiding principles can be specifically and relatively applied as a model —on a case-by-case basis— in the various content and meta or traffic data[1384] to address the above needs in pursuance of the protection of the right to the SOC. The levels identified and examined in this study are the *innermost, inner, middle* and *outer sancta* and *public domain levels*, in which LEAs or LEOs proportionately conduct an investigation based on the seriousness of an offence.[1385]

The Constitutional Court warns that the protection of the continuum of online privacy should not be allowed to hamper the investigation and prosecution of serious and complex offences.[1386]

The gravity of an offence committed[1387] determines how deep LEAs would conduct their investigation in the continuum of the SOC interests.[1388] Put differently, the deeper the level of invasion of continuum of the SOC interest or the deeper the reasonable expectation of privacy by an individual, the higher the threshold for the conduct of an OCI by LEAs or LEOs,[1389] the requirement of which is determined by the seriousness of an offence committed.[1390] This illustration emphasises the proportionality principle.[1391]

Arguably, subject to the type of data that is targeted for investigation —whether it is content or non-content data and in some cases, whether the data is real-time or archived

[1382] Reed *Internet law: Text and materials* 106.
[1383] Currie and De Waal *Bill of rights* 29-71 and 133-149.
[1384] See the types of data in Chapter 2 (para 2.6) of this study.
[1385] *Thint v NDPP* supra 80.
[1386] *Thint v NDPP* para 80.
[1387] Du Plessis M 'International criminal courts, the International Criminal Court, and South Africa's implementation of the Rome Statute' in Dugard J *International Law: A South African Perspective* 4th ed. (2013) 191 (Du Plessis 'International Criminal Courts').
[1388] See paras 5.3.4, 5.3.6 and 5.4 of Chapter 5 of this study.
[1389] Hubbard, Brauti and Fenton *Wiretapping* paras 3-3 to 3-5 and 3-6.2 to 3-6.3.
[1390] See paras 6.3.3.2–6.3.3.5 of this chapter.
[1391] See paras 5.3.4, 5.3.6 and 5.4 of Chapter 5 of this study.

communication;[1392] the decision on the type of device,[1393] technology, application, service, and network[1394] to be employed by LEAs may arguably, proportionately and appropriately be conducted as follows.[1395]

Firstly, , LEAs or LEOs may conduct an OCI at the 'innermost sanctum' concerning the state of emergency offences and offences that pose 'actual and potential threat' to national security, public health or safety or compelling national economic interests.[1396] Secondly, LEAs or LEOs may conduct an OCI at the 'inner sanctum' relating to 'most serious offences'.[1397] Thirdly, LEAs or LEOs may conduct an OCI at the 'middle sanctum' regarding 'more serious offences'.[1398] Fourthly, , LEAs or LEOs may conduct an OCI at the 'outer sanctum' for 'general serious offences'.[1399] Finally, LEAs or LEOs are at liberty to conduct an OCI in the 'public domain' for any offence —whether serious or not serious.

Before proceeding to the examination of the five levels of the continuum of the SOC sancta, it is submitted that three criteria, amongst others, are considered in the examination of the classification of the five levels of the continuum of the SOC interests.

Firstly, the degree of compartmentalisation and security of compartmentalisation of online communication devices, technologies, applications, services and networks determine the classification of layers of the continuum of the SOC interests. It is submitted that the compartmentalisation of online communication devices, technologies, applications, services and networks into five layers should require the use of different encryption and decryption keys or PIN at each layers of continuum of the SOC interests.[1400]

[1392] Hubbard, Brauti and Fenton *Wiretapping* 4-20 and 4-20.10; Koops B and Goodwin M 'Cyberspace, the cloud and cross-border criminal investigation- Limits and possibilities of international law' 23 www.tilburguniversity.edu/tilt (Date of use: 14 December 2016) (Koops and Goodwin www.tilburguniversity.edu/tilt (Date of use: 14 December 2016).

[1393] The devices are telephone landline, fax machine, two-way radio communication, Internet, mobile cellular telephone and e-tag system.

[1394] Para 5.4.6 of Chapter 6 of this study.

[1395] Paras 6.4.2.3 and 6.4.3 of Chapter 6 of this study.

[1396] Paras 6.3.3.2 – 6.3.3.5, 6.4.5 and 6.4.6 of Chapter 6 of this study; *Kaunda v President* supra 104, 105 and 127; Du Plessis 'International Criminal Courts' 191; Cajani at 9 https://rm.coe.int/09000016802f241b (Date of use: 21 March 2016).

[1397] Paras 6.3.3.2-6.3.3.5 and 6.4.7.1 of Chapter 6 of this study.

[1398] Paras 6.3.3.2-6.3.3.5 and 7.4.7.2 of Chapter 6 of this study.

[1399] Paras 6.3.3.2-6.3.3.5 and 6.4.8 of Chapter 6 of this study.

[1400] For example, a user or service provider or both can encrypt the data that is kept at different layers which indicate the layers in which a user wants to keep a data, Koops and Goodwin at 23 www.tilburguniversity.edu/tilt (Date of use: 14 December 2016). For the conceptualization in this study of a

The key or PIN may be configured to secure the peculiar needs of the level of the sanctum of secrecy interest.[1401] For example, micro-chip implantation in the body,[1402] the iris,[1403] fingerprint,[1404] voice recognition[1405] and ordinary or combination of alphabets, symbols, and number may relatively be used to compartmentalise or secure the innermost, inner, middle and outer sancta of the SOC interests respectively since these access codes are ranked according to their level of security or efficiency.[1406]

Secondly, the *number of people or the level of interactivity*[1407]involved in communication determines the level of continuum of SOC interests.[1408] The larger the number of recipients in online communication, the lesser the expectation of the SOC of the recipients.

Thirdly, further to the effect of the concept of a subjective expectation of online communication,[1409] the societal attachment of value to some online communication matters determines the level of continuum of the SOC interests. For example, in South Africa, although some individuals in the society openly declare their HIV status, it is still regarded as a confidential matter if an individual chooses not to disclose it to the public.[1410] Therefore, if an individual places this type of information into the innermost sanctum, it is reasonable that the

---

modern approach to this issue, see para 6.11 of Chapter 6 of this study titled '*Popoola QOCI*' application process.

[1401] Para 6.11 of Chapter 6 of this study.

[1402] Friggieri A, Michael K and Michael M G 'The legal ramifications of microchipping people in the United States of America - a state legislative comparison' file:///f:/li-us-%20art%20-%20legal%20aspects%20of%20implanting%20micro%20chips%20in%20us%20fulltext.pdf (Date of use: 12 June 2016.

[1403] Brocklin V V 'Legal, privacy concerns to consider before implementing iris-scanning technology looking at some public concerns and legal issues can help law enforcement plan its use of the evolving technology' https://www.policeone.com/police-products/police-technology/biometrics-identification/articles/430150006-Legal-privacy-concerns-to-consider-before-implementing-iris-scanning-technology/ (Date of use: 15 July 2018).

[1404] Fingerprint can be cloned, Vlok M 'The vultures preying on your social network- Criminals can exploit even the most innocent pictures or posts on social media-Here's how to protect yourself' 2017-02-23 *You* 24- 25.

[1405] Popov A 'Legal aspects of deploying voice biometrics and other speech technologies in connection with GDPR enforcement' https://www.linkedin.com/pulse/legal-aspects-deploying-voice-biometrics-other-speech-alexey-popov (Date of use: 15 July 2018)

[1406] Paras 5.3.4, 5.3.6 and 5.4.6 of Chapter 5 of this study.

[1407] Internet is one of the devices that entails widespread interactivity Spencer A B 'Jurisdiction and the Internet: Returning to traditional principles to analyse networked-mediated contacts' 2006 *University of Illinois Law Review* No 1 at 79, 81, 85, 86, 87, 89, 91, 93, 94, 97, 98 and 105.

[1408] Paras 5.3.2- 5.3.6 of Chapter 5 of this study.

[1409] See para 3.6.2 of this chapter.

[1410] *NM v Smith* supra 41, 43, 56, 61, 80, 103, 137, 158 and 183.

society must respect that decision.[1411]

Moreover, national security issues and trade secrets —or economic, commercial, industrial, financial or technical matters— are not allowed to be disclosed in an extraterritorial jurisdictional arrangement,[1412] therefore, the choice to place this type of data in the innermost sanctum by a government must be reasonably respected.[1413] This is in pursuance of the powers vested in a government to hierarchically classify information into: 'public domain', 'private', 'confidential', 'secret' and 'top secret'.[1414]

3.8.2 The inner-most sanctum in online communication secrecy interest

The innermost sanctum is the deepest part in online communication devices, technologies, networks, applications and services which require the highest level of expectation of secrecy and exclude everyone from having knowledge of or access to the archived, motion and motionless data in online communications.

Based on the features of content and non-content data,[1415] content data generally falls under the inner-most sanctum because content data may reveal undeniable and impeccable information, unlike non-content data which may be construed differently or inconclusively. The content data in this sanctum has the highest value as perceived by the owner who has the power to decide what to exclude from public or publicity[1416] or has the absolute power on whether to give consent as opposed to other sancta, which have multiple parties who may give consent.[1417]

Interestingly, having data in an innermost sanctum occurs when an individual engages in a proxy transaction, initiates or sends content data into the network for safekeeping, storage or for personal archival purposes and he or she is the only person who has knowledge or access to the information.[1418]

[1411] Para 3.6.2 of this chapter.
[1412] Koops and Goodwin 54 www.tilburguniversity.edu/tilt (Date of use: 14 December 2016).
[1413] Para 3.6.2 of this chapter.
[1414] *Independent Newspaper v Minister of Intelligence Services* supra 49.
[1415] See para 2.6 of Chapter 2 of this study on the features of content and traffic data.
[1416] Paras 3.4.4.4 and 3.4.4.5 of this chapter.
[1417] Hubbard, Brauti and Fenton *Wiretapping* 1-6.3.
[1418] *Bernstein v Bester NO* supra 67; Roos 'Data Protection' 353; Snail and Papadoulos *Privacy and data protection* 277-278; Chigoma W, Robertson B & Mimbi L 'Synchronised smart phones' 32.

From different approaches or perspectives, it is submitted that the following illustrations may further assist in describing the concept of inner-most sanctum:

(i) an individual may send a text from an o-mail address on the Internet to the same email address or 'mydropbox.com' or from a mobile cellular telephone to the same mobile cellular telephone for storage and safety purposes. The data in this sanctum may include a will, business or trade secret, password(s) of other electronic devices, the secret of an individual not known to anyone including the person that the secret relates to or any data that an individual places a high value on. This category may also include the activity of an individual who quietly sends data or expresses an opinion anonymously.

(ii) an individual who anonymously accesses the Internet through a proxy or firewall to prevent the identity of an individual from being disclosed in the communication may place data in the innermost sanctum;[1419]

(iii) an electronic chip containing some bio-data —including the status of organ donation— embedded in the human body to carry out sophisticated biological, physiological or general medical examination, diagnosis, function, monitoring of, and balancing of deficiencies in the human body is a form of data that may be placed in the innermost sanctum;

(iv) data in an indoor or domestic audio-visual robot or Internet of Things used for personal operational activities at home;

It is however important to note that it is difficult, if not impossible to place a real-time voice communication at the inner-most sanctum because it is at the moment impossible to make a voice call to one's self on a landline, mobile cellular telephone, two-way radio communication or Internet device which enable voice or audio-visual calls such as 'Skype' audio-visual call. It is also impossible to send a fax message to one's self from the same fax number or line in the olden day fax machine.

[1419] Gratton *Internet and wireless privacy* 13; Roos 'Data Protection' 327.

Despite the foregoing submissions, in the Canadian case of *R v Telus Communications Co*, archived text messages do not attract a higher level of protection unlike text a message in transit which attracts higher protection.[1420]

3.8.3 The inner sanctum in online communication secrecy interests

Having dealt with the innermost sanctum, the inner sanctum is arguably the deepest level of secrecy protection for ordinary, usual or minimal communications in online communication devices between *two parties only*,[1421] which require a higher expectation of secrecy and threshold when conducting an OCI. This sanctum arguably accommodates real-time and archived motion and motionless content[1422] data only -whether voice, audio-visual or text- in the devices.

According to Roos, online processing of personal information —that is, content data only— by online traders or by social network site operators falls under this sanctum.[1423] In order to protect inner-sanctum communications, a caveat or disclaimer is inserted by a sender to prevent the infringement of secrecy if an o-mail communication erroneously gets into the hands of unintended persons.[1424]

In some special non-content or traffic data communications, secrecy may arguably be protected at the inner sanctum. For example, where an individual conceals his number when a call is made from a mobile cellular telephone, there is a great level of secrecy required even if the call goes or does not go to voicemail.

[1420] *R v Telus Communication Co.* (2011) 105 O.R (3d) 411, 93 W.C.B. (2d) 292 paras 41-43(S.C.J); Hubbard, Brauti and Fenton *Wiretapping* 1-5 to 1-6.

[1421] Roos 2012 129 *SALJ* 397; Gratton *Internet and wireless privacy* 6; Hubbard, Brauti and Fenton *Wiretapping* para 1-6.2.

[1422] See paras 2.6 and 2.7 of Chapter 2 of this study. The content data includes voice and non-voice communications but, in this regard, excludes traffic data since the latter cannot be protected at the inner sanctum.

[1423] This view corroborates the opinion of Rautenbach and Neethling who believe that data protection does not fall under the inner-most sanctum. Their belief is in contradiction of judgment of Ackerman J in *Bernstein v Bester* supra 788-789 and 795 who categorized some examples of privacy into the inner-most sanctum of a person or his truly personal realm, see Rautenbach 2001 Vol. *TSAR* 117; Neethling 2005 122 *SALJ* 20. Further, Langa DP supports the view of the duo in *Investigating Directorate v Smit NO* supra 16 that privacy is not limited to the 'intimate space' but went further to say that privacy extends to OCI environment in which people act.

[1424] Snail and Papadoulos *Privacy and data protection* 286.

Other non-content or traffic data can only be arguably protected at the middle or outer levels of the sanctum of online communication interests.

3.8.4 The middle sanctum in online communication secrecy interests

One of the features of the middle sanctum is that it is a communication between a *determinable* and *limited number of parties* in both SNSs such as Facebook[1425] and arguably non-social network communications involving real-time and archived motion and motionless content and non-content data —whether voice, audio-visual or text. It requires medium expectation privacy for the content and non-content data and medium threshold requirement when conducting an OCI.

In content data, to some extent, an individual arguably waives his right to secrecy to accommodate more than two parties by including *a determinable* and *limited number of parties* in online communication. The communication in the middle sanctum is narrow and manageable in terms of the number of participants. The communication occurs within a circle, entity, group or association with a closed or common interest or purpose.

In the case of non-content data, the first general or deepest level of protection of secrecy for non-content is at the middle sanctum in online communications. Privacy in this regard may include the following data, and activities: data concerning the calculation of a bill for the use of a utility (e.g., vehicular o-toll system);[1426] data containing physical access control of an individual; data containing the attendance of an employee at the workplace; communication of all traffic data in all devices between an online communication agent and an individual who subscribes to a service —such as a car tracker.[1427]

Lately, the content data —i.e., pictures of passengers of a moving vehicle— gathered from a vehicular o-toll device[1428] and an o-toll bill —i.e., non-content data—[1429] which otherwise comprehensively show the motion, and motionless pictorial or graphic representation of an

[1425] Id.; Ellison N B et al 'Privacy and SNS: An overview' in Trepte S and Reinecke L (eds) *Privacy online-perspectives on privacy and self-disclosure in the social web* (2011) 22 (Ellison et al *Privacy and SNS*).
[1426] Hubbard, Brauti and Fenton *Wiretapping* 3-75.
[1427] Hubbard, Brauti and Fenton *Wiretapping* 3-75.
[1428] Hubbard, Brauti and Fenton *Wiretapping* 3-75.
[1429] See para 2.6.2 of Chapter 2 of this study where non-content data is examined which includes o-toll bill, which is short of content data.

individual in a vehicle while passing through an o-toll device arguably fall under the middle sanctum.

It is argued that the reason for grouping both content and non-content data of o-toll system under the middle sanctum —and not grouping the content data under inner sanctum— is that the passengers are already exposed to the public place by being on the road which may be or is now being monitored by CCTV cameras which are ubiquitous in recent time.[1430] Therefore, the level of secrecy in the public place is arguably, to some extent, diminished, drawing on the Canadian jurisprudence that believes that there is no reasonable expectation of privacy where there is a movement of an individual from one place to another.[1431]

Nevertheless, this study opposes the position that there is 'diminished' privacy when a driver is plying public roads based on the erroneous belief that because it is a public thoroughfare, therefore it does not protect the privacy of an individual in that regard.[1432] This is because, relying on the aforementioned o-toll system,[1433] the basis of this opposition is that it is an invasion of privacy where an o-toll payment system records the appearance or takes a photograph of occupants in a vehicle which is legally meant to be tagged for payment system of a vehicle only and not based the number of passengers in the vehicle.[1434]

3.8.5 Outer sanctum in online communication secrecy interests

Content data may fall under the outer sanctum where the communicated data is 'revealed to an *indeterminable* but *limited number of persons*'[1435] in which minimal expectations of secrecy and thresholds for the conduct of an OCI are required. This is a sanctum where the host or already existing participants have the power to limit or restrict the number of participants in the communication.

[1430] Hubbard, Brauti and Fenton *Wiretapping* 3-74 to 3-75.
[1431] Hubbard, Brauti and Fenton *Wiretapping* 3-74.
[1432] Para 3.4.3.3 of this chapter; Thompson *GPS monitoring* 256 -257.
[1433] See paras 2.2.2.1 and 2.6.2.2 of Chapter 2 and para 3.4.3.3 of the chapter of this study on o-toll system.
[1434] Para 3.4.3.3 of this chapter.
[1435] Italics mine, Roos 2012 129 *SALJ* 397; Gratton *Intesecrecy and wireless privacy* 6; Ellison et al *Privacy and SNS* 22.

This sanctum is in contrast with the public domain which has both *indeterminable* and an *unlimited* number of participants in the communication.[1436] It is relatively easy to justify the breach of secrecy at the outer edge of the continuum. The communications or activities at this level may arguably include availability of traffic data to other parties relating to the tracking of the location of a user on Facebook; [1437] use of cookies,[1438] chatting and adding contacts on SNSs such as Twitter or Facebook where parties use the public chat room or the general column.

Non-content, meta or traffic data will arguably be in the outer sanctum which entails data which though may be close to being grouped in the public domain —for one reason or the other, but still has some expectation of secrecy in the communication of the data. This may include non-content profiling of the sites visited by an individual (which inconclusively indicates some personal issues such as state of health, sex life, amongst others)[1439]on a device which was earlier used for o-mail communications by the same user. It may also include where the data is available for other positive and statutory, compelling, routine or processing reasons other than the conduct of an OCI. For example, the SANRAL may share the data collected from the o-toll system with other government departments for planning purposes only.

3.8.6 Public domain online communication interests

Where an online communication does not occur in all the four circumstances above,[1440] there is no legitimate expectation of secrecy of communication in the public domain since there is no determination or restriction of access to information whatsoever in the network[1441] except restriction in terms of registration and subscription or access fees to make use of the device.

[1436] Section 43 of the CCB B6-2017.
[1437] Roos 2012 129 *SALJ* 390-391.
[1438] Snail and Papadoulos *Privacy and data protection* 292.
[1439] See para 2.3.3.1 – 2.3.3.6 of Chapter 2 of this study.
[1440] Paras 3.8.2 -3.8.5 of this chapter.
[1441] Section 43 of the CCB B6-2017.

3.9 ROLE OF STAKEHOLDERS IN THE TECHNO-LEGAL INTEGRITY AND SECURITY OF THE SECRECY OF ONLINE COMMUNICATION IN MAJOR STATUTES RELATING TO THE PROTECTION OF ONLINE COMMUNICATION

3.9.1 Introduction

This study concurs that there are some dynamic, delicate and complex challenges in the security of the SOC,[1442] including the statutorily required installation of an inbuilt interception device in every online communication network, infrastructure or platform installed by a service provider.[1443] Nevertheless, this study disagrees that LEAs —as one of the groups of stakeholders in online communication— do not contribute to the problems encountered in cybersecurity[1444] in the protection of the SOC.

This is because in the 2016 JSCI of Parliament report submitted to Parliament by retired Constitutional Court Justice Yvonne Mokgoro, it was revealed that the SSA lacked the required 'intellectual and professional capacity in ICT security to enforce the law'[1445] which compromises the protection of the SOC. Similar *status quo* of lack of capacity in ICT[1446] exists in the FBI system of wiretapping in the U.S., which is impeachable.[1447]

Sequel to the abovementioned facts, it is submitted that information security is the gravamen in online privacy protection,[1448] or better still, the SOC. However, the numerous independent and interdependent government and non-government stakeholders in online communication security are rarely held civilly or criminally accountable for failing or refusing to maintain the

[1442] See the principle of online conscription in para 2.3.3 of Chapter 2, particularly paras 2.3.3.6 (b) and 2.3.3.7; Paras 3.5.7.2 – 3.5.7.14 and 3.8 of this chapter. In the U.S., information security is a concern, Landau *Lawful electronic surveillance in the face of new technologies* 221 and 227. The right to the SOC is the emerging and independent right that this study advocates for in this chapter; Landau *Lawful electronic surveillance in the face of new technologies* 229.

[1443] Failure to install an interception device is an offence, see s 30(1)(a) &(b) of RICA. In the U.S., due to the inability of the FBI not having the 'necessary technical capability to' conduct an OCI, the prosecutor had a weaker case and only secured a lesser sentence in the conviction of the target because other investigative procedures were used, despite having sufficient evidence to apply for an OCI direction, see Caproni *Lawful electronic surveillance* 206.

[1444] Landau *Lawful electronic surveillance in the face of new technologies* 229.

[1445] Parliament of the Republic of South Africa 'Announcement, Tablings and Committee Reports' No. 164 -2016 at 21.

[1446] Parliament of the Republic of South Africa 'Announcement, Tablings and Committee Reports' No 164 -2016 at 21.

[1447] Landau *Lawful electronic surveillance in the face of new technologies* 220.

[1448] Heink http://www.derebus.org.za/guide-protection-personal-information-act/ (Date of use:12 January 2019).

integrity and security of the SOC despite the extant law. The non-accountability or enforcement renders the purpose for which online communication takes place ineffective, unreliable and short-lived.

The emphasis of the role and responsibility of the stakeholders in the security of the SOC is a reality and central to the further conceptualisation, recognition and protection of the nature, components and scope of the right to the SOC in contemporary society.[1449] This emphasis requires that the pre and post processes involved in an online communication should 'remain complete and unaltered' in serving 'the purpose for which the information was generated' as well as other incidental relevant purposes.[1450]

The stakeholders —who range from 'trusted insiders',[1451] 'skilled outsiders' to 'non-skilled outsiders'— are charged with the responsibility of ensuring the integrity and security of the SOC.[1452]

The 'trusted insiders' are those who invent, create, and lay or maintain the technical foundation for the existence and operation of online communication. They include the following: manufacturers of online communication and interception devices; online communication service agents or providers[1453] comprising, amongst others, telecommunication service providers, online communications service providers and decryption key holders; and Interception Centre.

The 'skilled outsiders' are the next set of skilful entities or people in an online communication stakeholdership who —by law or opportunity— are in charge of the regulation, administration, management and operation of the devices, technologies, networks, applications and services invented, created, provided, and maintained by 'trusted insiders'.

The skilled stakeholders include, amongst others: the administrative and regulatory authorities such as the relevant ministers and ICASA, amongst others; executing and operational authorities such as domestic, foreign and international LEAs and institutions; professional and

[1449] Paras 2.2, 2.3, 2.5, 2.6, 2.7 and 2.8 of Chapter 2 and para 3.5 of Chapter 3 of this study.
[1450] Sections 14(2) (a) -(c), 15, 17(2) of the ECTA.
[1451] *State v Agliotti* supra 135, 138, 139 and 14.6.5.
[1452] Kosseff *Cybersecurity law* xxi - xxvii.
[1453] Landau *Lawful electronic surveillance in the face of new technologies* 219 and 229.

non-professional entities. The opportune stakeholders include business competitors, economic espionage perpetrators, domestic and cyber-terrorist groups, hackers,[1454] amongst others.

The 'non-skilled outsiders', which include customers or users of online communication, are those who are ordinary or mere consumers and are presumed to be with or without some skill to operate online communication devices, technologies, networks, applications and services. This rubric expresses one of the multi-dimensional or holistic approaches to this study,[1455] which considers the provision, enforcement of and compliance with the regulations in some Acts relating to the techno-legal integrity and security of the SOC. This is done by describing —or examining where necessary— the proportionate and direct, and indirect independent, interdependent, and collective pre-and post-performance[1456] strategic, administrative and non-administrative, operational and non-operational and supervisory and non-supervisory duties, functions or responsibilities of stakeholders in the techno-legal complex and risky protection of the integrity and security of the SOC.

3.9.2 Role of regulatory authorities -as one of the clusters of stakeholders- in protecting the secrecy of online communication

3.9.2.1 Introduction

Drawing on the obligation of experts in online communication security in the RSA[1457]and government of the U.S., such as ensuring the security of some specific online communications;[1458] ICASA —a representative of the government of the RSA— is one of the

[1454] Landau *Lawful electronic surveillance in the face of new technologies* 219 and 229.
[1455] Para 3.1 of this chapter.
[1456] The assessment of pre and post-performance duties, functions and responsibility of stakeholders relate to and include: the separation of powers; checks and balances or monitoring and evaluation in terms of consultation with National Assembly or other independent authorities before and after making a regulation or policy under an Act; progress report by relevant stakeholders (including non-statutory stakeholders such as the conventional and social media practitioners and users respectively) of the success or failure of the Act, regulation or policy; general and specific standardised reporting systems; assessment of performance of a public and private office holder, functionary or executor in relation to the protection of the SOC, etc. For example, if all stakeholders were proportionately or relatively held responsible as a user of an online communication device is held liable for its misuse, then the integrity and security of the SOC will be guaranteed in the RSA. In this regard, a user of an online communication device (a mobile cellular telephone, for example) has a duty to register a SIM card with an Online Communication Service Provider (pre-performance duty) and report the loss or theft of a SIM card to the police (post-performance duty), failing which an offence is committed by a user, see sections 39, 40, 41, 52, 53 and 54 of RICA.
[1457] *State v Agliotti* supra 135, 138, 139 and 14.6.5.
[1458] Such as the integrity and security of locational privacy, Blumberg and Eckersley *Locational privacy* 322.

main statutory authorities amongst other authorities that regulate various technical and non-technical online communication integrity, security, activities, functions, and interests.

Other regulatory authorities include advisory councils,[1459] the OIC, ACA, presidential commissions, committees etc. that assist in diverse ways in the regulation of online communication including the integrity and security of online communication.[1460]

ICASA is more particularly in charge of the fundamental technical and operational regulation of policy direction that guarantees the integrity and security of online communication devices in the public interests in the rapidly converging technological milieu in the RSA.[1461] ICASA is a significant public telecommunication utility regulator that generally provides for the facilitation of universal telecommunication access and management of scarce national spectrum resources.[1462]

However, there is no constitutional principle or provision that recognises ICASA[1463] amongst other institutions either in Chapter Nine or under any other chapter of the constitution[1464] that regulate online communication, more particularly, the integrity and security of online communication.

[1459] Thorton *Telecommunication law* 22.

[1460] Others that assist ICASA include Universal Service Agency ('USA') which is a specialized regulatory authority that focuses universal communication, see Chapter VII of Telecommunications Act.; Competition Commission; South African Council for Space Affairs; Ministry of Trade and Industry; Ministry of Justice and Constitutional Development, Thornton *Telecommunication law* 21-22 and 33. Others are the Computer Security Incident Response Team ('CSIRT') and the ECS-CSIRT serves as the South African Government Computer Security Incident Response Team, see State Security Agency 'Computer Security Incident Response Team' (CSIRT) http://www.ssa.gov.za/csirt.aspx (Date of use:18 February 2018).

[1461] See the Preamble and section 2 of ICASA No. 13 of 2000.

[1462] Thorton *Telecommunication law* 18, 19 and 24.

[1463] Section 3(3) of ICASA provides that ICASA is an independent authority; Thorton *Telecommunication law* 18, 20 and 23.

[1464] However, the South African Human Rights Commission is one the Chapter Nine Institutions that has general jurisdiction to pronounce on the right to privacy, which does not extend to the specialised powers granted to ICASA relating to online communication. Moreover, the three categories of LEAs established by the constitution —which are the SAPS, SANDF and SSA— are not empowered to have regulatory functions, let alone regulate the integrity and security of online communications and interception. There is an express constitutional provision of some principles in some important areas of governance stipulated in the Constitution such as the principles of cooperative governance (including Alternative Dispute Resolution ('ADR') mechanism), procurement, public administration, etc., see Chapter 3 (particularly section 41(1)(h)(vi), (2)(b), (3) and (4)) and sections 195 and 217 of the Constitution. ADR principle is also provided in section 57(7) of the CCB B6–2017, published in Gazette No 40487 of 9 December 2016. Section 69(1) of the ECTA provides for ADR in disputes relating to domain name dispute.

In protecting the integrity and ensuring the security of online communication, the regulatory duty of ICASA is to assist the various authorities to achieve their objects provided in the following statutes.[1465] These statutes are the ECA, ECTA, RICA, POPIA and the yet to be enacted the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017.

According to *State v Agliotti*,[1466] which highlights the significance of the specialised duty of experts or stakeholders in the protection of online communication, this rubric describes or — in some cases where necessary— examines the diverse and general responsibility and role of the regulatory authorities in upholding the multi-dimensional aspects of the techno-legal integrity and security of the right to the SOC.[1467]

3.9.2.2 Role of regulatory authorities in protecting the concept of the secrecy of online communication in the Electronic Communications Act

The ECA recognises the Minister of Communications as the main regulatory authorities in the use of online communication,[1468] more particularly in the area of ensuring direct and indirect protection of the integrity, security and reliability of online network communication.[1469]

On the one hand, the role of the Minister of Communication in regulating the integrity and security of online communication is as follows:

Firstly, the Minister of Communication may make a policy on the development of new technologies relating to online communication services, particularly in ensuring 'information security and network reliability' of online communication.[1470] However, this provision is flawed. In the first place, there is no requirement that the Minister must have adequate knowledge of the acceptable standard of technologies by stakeholders before being appointed to this technical position, though it is always argued that a Minister is always advised by technical experts in the field whose advice may not be heeded to by the Minister.

[1465] Section 2(c) of ICASAA.
[1466] *State v Agliotti* supra 135, 138, 139 and 14.6.5.
[1467] See also para 3.9.1 of this chapter.
[1468] See section 1 of the ECA.
[1469] Section 2(q) of the ECA.
[1470] Sections 2 (q) and 3 (1)(d) of the ECA.

Moreover, the use of the word 'may' is inadequate because there is no proper mandate in this regard. Invariably, these two defects adversely result in no or improper direction or some uncertainty in policy direction on how to secure online communication. Where any of these circumstances occurs, it arguably impacts on the competence of LEAs in understanding and applying the new or current technologies in the security of online communication.[1471]

Secondly, the Minister of Communication may, in pursuance of the object of the ECA – including section 2(q), issue directives to ICASA on how to determine the priorities for the development of online communication networks and other services.[1472] However, aside from the general criticisms that trail political appointment and leadership in a professional setting,[1473] the use of the word 'may' to describe the function of the Minister is inadequate. This is because the use of the word 'may' means that the issuance of a directive is not mandatory in this regard, which adversely and directly or indirectly impacts on the development, integrity and security of licensing framework for online communication.[1474]

On the other hand, ICASA regulates the security of online communication in the following persuasive ways. Firstly, ICASA may make regulation on technical matters, which are necessary for licensing framework of online communication.[1475] Such matters, it is suggested, should include the security of online communication. Secondly, ICASA may prescribe the type of equipment that is used by Online Communication Service Provider, which has been approved by the ETSA or other competent authorities.[1476] Thirdly, ICASA may prescribe technical standards for online communication equipment and facilities on the protection of and prevention of harmful interference with an online communication network.[1477] Fourthly, ICASA may prescribe measures in the online communication licence conditions such as the protection of privacy and personal data, 'prevention of fraud' and provision of assistance to LEAs.[1478] In all this, it does seem that these provisions are relatively adequate to secure online

[1471] Parliament of the Republic of South Africa 'Announcement, Tablings and Committee Reports' No 164 -2016 at 21.
[1472] Section 3(2)(b) of the ECA.
[1473] The Minister of Communication, a politician, who is most unlikely to be an expert in online communication technology let alone an expert in its integrity and security.
[1474] Section 3(2)b) of the ECA.
[1475] Section 4(1)(a) of the ECA.
[1476] Section 35(2)(a) & (b) of the ECA.
[1477] Section 36(2)(a) & (d) of the ECA.
[1478] Section 75 (a), (b), (d) & (f) of the ECA.

communication. Lastly, ICASA may recommend to the Minister on policy matters in pursuance of the objects of the ECA.[1479]

However, the use of the word 'may' in the various provisions described above does not give the much-required force to the obligation of ICASA to maintain the integrity and security of online communication. This is exacerbated by the fact that the penalties for non-compliance with these provisions are too lenient, do not have real deterring provisions or non-existent that such provisions will guarantee the integrity of online communication. For example, despite that, the scope of this study refrains from examining the adequacy of punishment for the unlawful invasion of online communication,[1480] for emphasis, the highlight of the penalty provisions for non-compliance with the provisions of the ECA is as follows.

Firstly, it is provided that no person may conduct a transmission and or own a radio signal and equipment save where permissible by law for use, for example by LEAs,[1481] because an unauthorised radio signal may be used to gather information from innocent online communication users. However, the penalty for the contravention of this provision is that ICASA may seal or alter such device, prevent the use of the equipment, grant a permit for a definite period, seize such equipment,[1482] until such a time that the provision of section 31 of ECA or court of the law authorises otherwise.[1483] The use of the word 'may' also takes away the certainty of the enforcement of the penalty where liability is obvious, unlike the wording of the penalty in RICA, which though is more authoritative[1484] but is not effective in curbing online communication breaches.

Secondly, save where it is approved by ICASA, it is prohibited for anyone who uses, supplies sells, offers for sale or lease or hire any online communication equipment or facility, which includes radio apparatus.[1485] However, there is no criminal remedy that is attached to this provision because the object of ECA seems more contractual or civil than regulatory in nature. In fact, there is no provision for general criminal remedy in the ECA, thus this inadequacy makes this provision redundant, which affects the security of online communication in this

[1479] Section 3(9) of the ECA.
[1480] Para 3.10 of this chapter.
[1481] Sections 31(1) and (5)(b) and 32 (1)(a) & (b) of the ECA.
[1482] Section 32(3)(a)(i)-(ii) & (b) of the ECA.
[1483] Section 32(4) of the ECA.
[1484] Sections 51 of RICA.
[1485] Section 35(1) of the ECA.

regard. This is unlike the repealed Telecommunication Act, some of which provisions prescribe 2 years or 500,000 as punishment for contravening the Act.[1486]

Lastly, the authority of ICASA in regulating the integrity and security of online communication is non-mandatory in some regard as described above. This is because, with the use of the word 'may', it would be surprising to have penalties for non-compliance of the provisions of the ECA. After all, no provision that is couched with the use of the word 'may' can effectively impose a duty on ICASA. The only way that there can be an effective imposition of a duty on ICASA is where the word 'shall' is used or where 'may' is interpreted to mean 'shall'.

Notwithstanding the foregoing inadequacies, the mandatory role of ICASA in the regulation of the integrity and security of online communication is as follows:

Firstly, ICASA must prescribe standard terms and conditions to be applied to individual and class licences of online communication equipment. In doing so, ICASA must take into account: the interest of the public in a bid to secure the efficient and effective functioning of online communication networks. The security includes the prevention and restriction of harmful interference in online radio communication frequency spectrum.[1487] In these terms, ICASA must also consider any universal access, universal service or international obligations,[1488] which include compliance with relevant international standards subscribed to by the RSA.[1489]

Secondly, in the performance of its function, ICASA must ensure that there is elimination or reasonable reduction of the harmful effect of the use of online communication frequency spectrum, while it must investigate and resolve all reported instances of harmful interference to licensed online services.[1490]

Third, ICASA must make regulations on the framework on how customers can connect to other networks.[1491]

[1486] Section 55 (1) & (2)(a)-(c) of the Telecommunications Act.
[1487] Section 8(2)(f) of the ECA.
[1488] Section 8(2)(g) of the ECA.
[1489] Section 8(2)(j) of the ECA.
[1490] Section 30(3) and (4) of the ECA.
[1491] Section 42(1)(b)(i) & (ii) of the ECA.

Fourthly, ICASA must also prescribe regulation on the accessing and securing of online communication facility leasing.[1492]

Fifthly, ICASA must prescribe regulation relating to the minimum standards for the protection of 'private end-user and subscriber information'.[1493]

In finalising the discourse on the role of ICASA in securing online communication, it does seem that the mandatory provisions for the protection of the integrity and security of online communication by ICASA are relatively adequate in the ECA, outweighing the earlier examined discretionary powers of ICASA, which are inadequate.

In summary, the powers of the Minister of Communication are limited and discretionary. However, because of the exercise of political fiat, the Minister, in practice, is dominantly involved in the general regulation and management of the use of online communication, which takes away the professional technical independence of ICASA[1494] and ultimately compromises the protection of the integrity and security of online communication. The wielding of this power by the Minister in the ECA is opposed to the repealed Telecommunication Act, which partially allowed the independence of ICASA to prevail by enabling it to make its regulations, though subject to the approval of the Minister.[1495] Furthermore, where the mandate of ICASA is discretionary, it whittles down the effect of making provision for the security of online communication.

Besides, there is no statutory provision that requires accountability or sanction for civil malfeasance or wrongdoing in the mandatory and discretionary functions performed by the

[1492] Section 44(3)(i) of the ECA.
[1493] Section 69(3) of the ECA.
[1494] This is because, for example, there are recorded cases of wrongful decisions taken by an erstwhile Minister of Communication on the migration of public communication broadcast from analogue to digital migration, which should have commenced in 2015. However, a new commencement date of 2020 has been set, Gedye L 'Faith Muthambi likely to bear brunt of the backlash over digital fail' https://mg.co.za/article/2016-06-02-backlash-likely-over-digital-fail (Date of use: 22 April 2019) (Gedye https://mg.co.za/article/2016-06-02-backlash-likely-over-digital-fail (Date of use: 22 April 2019); Lately, a minister of Communications and Telecommunication withheld funding for the annual performance plan for ICASA, Maqhina M 'Minister meddling in Icasa affairs' https://www.iol.co.za/news/politics/minister-meddling-in-icasa-affairs-22163646 (Date of use: 1 May 2019) (Maqhina https://www.iol.co.za/news/politics/minister-meddling-in-icasa-affairs-22163646 (Date of use: 1 May 2019).
[1495] Section 3(9) of ECA; Section 95(3) and 96(6) of Telecommunications Act; Thorton *Telecommunication law* 21 and 33. See also Chapter 4 of the book by Thorton L et al (eds) *Telecommunication law in South Africa* (2006).

regulators in ECA —such as negligence, dereliction of duty, incompetence, incapacitation etc. —[1496] which directly or indirectly affect the security of online communication. The ECA creates an administrative system where only the executing authorities or corporate or private entities are civilly and criminally held accountable or liable for malfeasance or wrongdoing, which in practical terms, is only remedial in nature.[1497]

In the overall analysis, the ECA recognises and protects the concept of the SOC, however, the provisions are inadequate to protect the integrity of and secure the right to the SOC in the contemporary society as examined above.

3.9.2.3 Role of regulatory authorities in protecting the concept of the secrecy of online communication in the Electronic Communications and Transactions Act

Although the Electronic Communications and Transactions Bill 2012 was published in the Gazette for comment by the public[1498] in which ICASA was proposed to be included as one of the authorities regulating some aspects of the provisions of the ECTA; however, no Act has been published in this regard as at the time of completion of this study.

Therefore, ICASA is not recognised as a regulatory authority in the ECTA. The regulatory authorities in the ECTA relating to the integrity and security of online communication are the Minister of Communication, ACA and .Za Domain Name Authority which are considered below.

i) Minister of Communication

The Minister of Communication is the political and regulatory head who —is not required by law to be a professional in the fundamental issues raised in the ECTA but— oversees the activities in the provisions of the ECTA[1499] as follows:

[1496] Maqhina M 'Minister meddling in Icasa affairs' https://www.iol.co.za/news/politics/minister-meddling-in-icasa-affairs-22163646 (Date of use: 1 May 2019).
[1497] Amongst others, s 74 of ECA provides for offences and penalties against executing authorities or entities, which do not include custodial or monetary sanction as provided in other forms of penology.
[1498] This bill has not been enacted, see section 1(y) of the Electronic Communications and Transactions Bill 2012 published in Notice No. 888 of 2012 in Gazette No. 35821 of 2012.
[1499] See commentary on the ministerial appointment in para 2.8.2.1 of this study.

a) In consultation with the ministers of Labour and Education, the Minister of Communication develops a training and human resource development programme in the information technology sector,[1500] which is suggested should include the integrity and security of online communication towards ensuring the protection of the right to the SOC.[1501]

b) The Minister of Communication may recognise accredited foreign products or services already accredited abroad for online communication in the RSA.[1502] However, although the accreditation is subject to the condition, there is no express condition provided in this regard, thus compromises the integrity and security of the foreign products and services that are being deployed in the RSA despite the accreditation of these foreign products and services.

c) The Minister of Communication may make regulations in respect of requirements or guidelines for information security.[1503] However, this provision is inadequate. One of the inadequacies in the provision is that, because the Minister makes regulations without any consultation with Parliament, there is no compliance with the principles of separation of powers and checks and balances. The non-compliance makes the provisions inadequate to regulate the integrity and security of online communication;

d**)** The Minister of Communication may declare certain classes of information as critical databases which are important to the national security and economic well-being of the citizens of the RSA.[1504] The declaration is a demonstration of the recognition and protection of the integrity and security of online communication, which includes online communication of users kept by the government;

e) The Minister of Communication may regulate the procedure for the declaration of a critical database, which includes registration of a database and may prescribe the minimum standards to manage the operation of the databases.[1505] However, the use of the word 'may' is discretionary, which is one of the inadequacies in guaranteeing the integrity and security of online communication;[1506]

[1500] Section 8(2) of the ECTA.
[1501] Section 8(3)(j) of the ECTA.
[1502] Section 40 of the ECTA.
[1503] Section 41(e) of the ECTA.
[1504] Section 53(a) of the ECTA.
[1505] Sections 52-55 of the ECTA.
[1506] Sections 52-55 of the ECTA.

f) The Minister of Communication must issue policy directive on electronic transaction policy;[1507]

g) The Minister of Communication may make regulations on any matter provided in ECTA,[1508] which should include the integrity and security of online communication.

In all this, firstly, the statutory provisions for the security of online communication by the Minister of Communication in ECTA are relatively adequate to the extent of the object of the ECTA. Secondly, save in one instance where the Minister of Communication is compelled to perform his or her function, the performance of the function of the Minister of Communication is not mandatory based on the use of the word 'may' in the aforementioned provisions.

The word 'may' does not compel the Minister to act swiftly or timeously in cases where it is foreseen that the integrity and security of online communication and interception might be compromised. However, it is noted that in some circumstances, the word 'may' connotes a mandatory function, thus the context in which the word is used is important to determine the effectiveness of the provision.

ii) Accreditation Authority

The Director-General of the Department of Communication is the ACA who regulates the provision for products and services accreditation and the affairs of the Authentication Service Providers.[1509] Therefore, the role of the ACA in protecting the integrity of and securing online communication is highlighted below:[1510]

a) The ACA has the power to register and regulate cryptography providers,[1511] which is a reasonable provision, given the presumption that the ACA is expected to comply with the civil service operational rules as opposed to the ministerial operations which are guided by political dynamism, rules and rulers;

[1507] Section 10 of the ECTA.
[1508] Section 94 of the ECTA.
[1509] See 'Authority' under the definition section and Chapter VI of the ECTA.
[1510] See 'Authority' under the definition section and Chapter VI of the ECTA.
[1511] Chapter V of the ECTA.

b) Although the Director-General of the Department of Communication is the ACA for the recognition of Authentication Service Provider of authentication product or service[1512] such as advance electronic signature;[1513] the accreditation of a service or product provider is voluntary.[1514] The option of making the accreditation of a service or product provider a voluntary requirement is inadequate because it becomes difficult for such service providers to be regulated in many ways including the regulation of the integrity and security of the SOC;

c) It is discretionary for the ACA to monitor the operations, systems and conduct of an authentication service provider. The former also has the discretion to temporarily revoke or suspend the accreditation of an authentic service provider if there is non-compliance with section 38, thus resulting in the appointment of an independent auditing firm to conduct periodic audits of the Authentication Service Provider in pursuance of section 38. Again, although these provisions relatively ensure the integrity and security of the SOC, however, the discretionary power to perform the abovementioned functions is inadequate;[1515]

d) It is discretionary for the ACA to stipulate the technical and other requirements expected of a certification service provider in their certificate.[1516] It is also the discretion of the ACA to stipulate the type of records to be kept, how the records are kept and the period for which they are kept[1517] and the consequential responsibilities and liabilities of the certification service provider that follow.[1518] However, the use of the word 'may' in the performance of the above functions whittles down the effect of the function in ensuring the integrity and security of the SOC;

e) Giving a wide discretion to the ACA to impose any conditions or restrictions where necessary in the accreditation of an authentication product or service is inadequate.[1519]

[1512] Chapter VI of the ECTA.
[1513] Section 37(1) of the ECTA.
[1514] Section 35 of the ECTA.
[1515] Section 36(1)(a)-(c) of the ECTA.
[1516] Section 38(4)(a) of the ECTA.
[1517] Section 38(4)(f) of the ECTA.
[1518] Section 38(4)(d) & (e) of the ECTA.
[1519] Section 38(5) of the ECTA.

This is because accreditation may be done at the whims and caprices of the Authority in terms of both the conditions for accreditation and discretion to accredit. The inadequacy lowers the standard for operation, including the integrity and security of the SOC;

f) On the satisfaction of the ACA that the Authentication Service Provider fails, refuses or ceases to meet any of the requirements for the accreditation in sections 38 or 40 of ECTA, the former may suspend or revoke the accreditation.[1520] The discretion herein is justifiable because the principle of fair hearing is required to be complied with before the ACA takes further steps against the Authentication Service Provider.[1521] However, this provision should be applied in accordance with a report from the relevant statutory and non-statutory standard organisations in the RSA relating to the integrity and security of the SOC to make the provision adequate;

g) The ACA has the discretion to request Cyber Inspectors or independent auditors to, from time to time, carry out an audit on the critical database administrator to evaluate the level of compliance with the provisions of Chapter IX of the ECTA[1522] However, a specific period for audit should be stipulated in addition to the periodic auditing, to make this provision adequate.

Finally, the same or similar conclusions and recommendations made regarding the role of the Minister of Communication in the ECTA especially the discretionary role[1523] are relatively adopted herein for the role of ACA in ensuring the integrity and security of the SOC.

iii) Domain Name Authority

Established under the Companies Act[1524] as a regulatory, professional or quasi-professional body; legal recognition is given to the .Za Domain Name Authority which generally regulates domain name issues or disputes,[1525] arguably, including intentional misrepresentation of domain contents and names.

[1520] Section 39(1) of the ECTA.
[1521] Section 39(1) of the ECTA.
[1522] Section 57(1) & (2) of the ECTA
[1523] Para 3.9.2.3 (i) of this chapter.
[1524] Sections 59-62 of the ECTA.
[1525] Section 43 of the ECTA.

For example, where online communication users are technically misled or manipulated in the domain name appearance or recognition, the integrity and security of the SOC is directly or indirectly compromised because information is sent or received by an unintended person as one of the effects of the misdirection or manipulation, thus impacts on the integrity and security of the SOC.

Misrepresentation arises from the various instances of: cloning of domain names; passing off of domain names; engaging in predictive registration of domain names of non-operational businesses which are later sold to another business owner with same business name who has no choice but to buy out the initial domain name owner and other related forms of online communication vices.

In addition to the abovementioned points, the role of Domain Name Authority in protecting the integrity of and securing the SOC is as follows:

a) The Domain Name Authority has the power to administer and manage the domain name space subject to the policy directive that the Minister of Communication may or must issue.[1526] It is however submitted that where the powers of a specialised authority —such as the Domain Name Authority— are subject to the regulation made by the Minister of Communication without a wider consultation with the National Assembly[1527] may compromise the integrity and security of the SOC in this regard.

   Moreover, the expertise of the Minister of Communication to make an independent and well-informed decision may be in doubt. This is because there is no statutory requirement for academic or professional qualification to secure the services of the Minister of Communication for these tasks, given that ministerial appointment is generally a political one, which is not the standard that is required in a technical, complex and delicate field such as online communication integrity and security.[1528]

[1526] Sections 65(1) and (4) of the ECTA.
[1527] Section 94 of the ECTA.
[1528] Paras 2.2.2.2, 2.3.1, 2.3.2, 2.3.3, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 3.4.5, 3.5.7.2 - 3.5.7.14 and 6.11 of this study.

b) In the performance of their role, the board of the Domain Name Authority submits a report to the Minister of Communication and in turn submits to Parliament.[1529] Although this provision seems adequate based on the application of the principle of checks and balances, however, the provision is inadequate. Submitting a report to the Minister of Communication takes away the independence of the Authority. This is because, in a way, the submission hands over the control of the Authority to the Minister of Communication, who is more likely to be influenced by political decisions as we have witnessed in recent time,[1530] which may not be in the overall interest of the society in terms of the integrity and security of the SOC.

c) Regulation may be made by Domain Name Authority with the approval of the Minister of Communications,[1531] which is inadequate. The submission made with regards to paragraph (a) above on section 65(1) and (4) of the ECTA is adopted herein.

In the final evaluation of the role of the three regulators in the ECTA, it is noted that there is no central, independent and professional point of coordination of the role and activities of the above three authorities in the ECTA that will adequately protect the integrity of and secure the SOC.[1532]

Furthermore, it is noted that although the ECTA makes diverse provisions for the maintenance of the integrity and security of the SOC, the discretionary nature of the power of the regulators is inadequate, which makes the enforcement of these provisions difficult to achieve, if not impossible in some instances. Although section 32(2) of the ECTA makes provision for criminal liability, it remains to be seen if the regulatory authorities can conventionally, generally and civilly or criminally be held accountable in the ECTA for incompetence, dereliction of duty, negligence or incapacitation in the mandatory performance of their functions.

For instance, the provision of section 29 of the ECTA which requires that the ACA must establish, maintain and regulate cryptography services and providers respectively, may

[1529] Section 67 of the ECTA.
[1530] Gedye L 'Faith Muthambi likely to bear brunt of the backlash over digital fail' https://mg.co.za/article/2016-06-02-backlash-likely-over-digital-fail (Date of use: 29 September 2017).
[1531] Section 68 of the ECTA.
[1532] See para 3.9.2.6 (d)(iv) of this chapter where the CCB provides a solution.

conventionally not be held liable in section 32(2) of the ECTA for non-compliance with Chapter V of the ECTA, more particularly section 29(1) and (2).[1533] To further demonstrate the conventional exemption of regulatory authorities —including executing authorities— from the offender list of non-complying entities in ECTA is section 32(1) of the ECTA, the law exonerates the National Intelligence Agency (now SSA)[1534] from liability for non-compliance with Chapter V of the ECTA.

In addition, since the enactment of the ECTA in 2002, the non-compliance with section 65(5) which requires that the ECTA should periodically be reviewed to determine the effectiveness of the Act[1535] has not resulted in the provision of civil or criminal sanction against the regulatory authorities for failure or refusal to review this Act. If there was a review, perhaps this aspect of this study would not have been necessary. This is because the inadequacies identified in this rubric would have been addressed in the reviewed Act. The review of the ECTA should include but not limited to the issues raised thus far under ECTA such that there is better integrity and security of the SOC.

In the overall analysis, although the ECTA recognises and protects the concept of the SOC, nonetheless, the provisions are inadequate to protect the integrity of and secure the SOC in contemporary society as examined above.

3.9.2.4 Role of regulatory authorities in protecting the concept of the secrecy of online communication in the Regulation of Interception of Communications and Provision of Communication-related Information Act

The regulatory authorities in RICA are the Minister of Justice, ICASA and OIC whose roles are as follows.

[1533] The ACA may also not be held liable for non-compliance with section 36(2) of ECTA despite the mandatory tone of the provision. In section 58 of the ECTA, an offence is created for the non-compliance by database administrator only but not for the Director-General of the Department of Communications whose duty of inspection of critical database is discretionary. Also, the criminal liability in Chapter XIII titled 'Cybercrime' does not touch on the liability of the regulatory authorities in ECTA.

[1534] See paras 4.3.5, 4.4.5 and 4.5.5 of Chapter 4 of this study.

[1535] Section 65(5) of the ECTA.

a. Role of the Minister of Justice

The role of the Minister of Justice in protecting the integrity and security of the SOC and conduct of an OCI is twofold.

Firstly, in consultation with the Minister of Communication, the Minister of Justice may determine the security standards for Online Communication Service Providers in securing and accessing the recordings in online communication.[1536] The provision for the consultative determination of security standards guarantees the protection of the right to the SOC.

However, given that there is no academic, professional or skill requirement for the occupation of the ministerial position in communication, it creates doubt in the quality of consultation on the determination of the standards by the Minister of Communication. Although it is expected that expert advice may be sought in the performance of this function by the Minister of Communication, however, not having adequate personal knowledge or skill in the field of information and communication technology to direct the affairs of the Department may compromise the advice given by or to the Minister of Communication to or consequently to the Minister of Justice.

In addition, the provision on standardisation is partially adequate in terms of the joint responsibility bestowed on the relevant ministers involved in the determination of standardisation, which satisfies the principle of checks and balances in ensuring the integrity and security of online communication. However, this provision is inadequate because the responsibility of the ministers is not mandatory in the performance of this function because of the use of the word 'may' in the provision.[1537]

Secondly, in consultation with other relevant ministers, the Minister of Justice shall declare listed equipment that will be primarily useful for the conduct of an OCI.[1538] This provision is partially adequate to the extent that the Minister of Justice involves other shareholder ministers in the declaration and all have a mandatory function because of the use of the word 'must' in

[1536] Section 40(4)(b) of RICA.
[1537] Section 40(4)(b) of RICA.
[1538] Section 44 of RICA, more particularly sub-section (2)(a)(i).

the provision. Besides, having a provision that regulates interception equipment is geared towards guaranteeing the security of the SOC.

However, save for the Minister of Justice who must be a lawyer —but not necessarily a cyber-lawyer— the other shareholder ministers are not required to have expert knowledge in this regard to make them take a rational and appropriate decision, which may adversely affect the decisions taken regarding the security of the conduct of an OCI.

b. Role of the Independent Communication Authority of South Africa

The role of ICASA in protecting the integrity and security of the SOC and the conduct of an OCI is that ICASA participates in the broad consultation by the Minister of Communication with other relevant ministers, who issue a directive on the 'security, technical and functional requirements' for the conduct of an OCI and storage devices.[1539]

The Minister of Communication in consultation with ICASA revokes licences of Online Communication Service Providers on third conviction for non-compliance with the requirements for the security of facilities for the conduct of an OCI and storage of online communication.[1540]

The involvement of ICASA in this regard guarantees broad consultation and fair hearing on the revocation process. However, the technical expertise of ICASA may be compromised by the political fiat of the Minister of Communication who may override the expert opinion of ICASA that should solely or ordinarily be responsible for the regulation of security issues in online communication save for the power of checks and balances that should vest in Parliament. This compromise is partially influenced by the non-requirement of special skill for the occupation of the office of the Minister of Communication.

[1539] Section 30(2) (a) (ii), (3)(b) and (7) of RICA.
[1540] Section 56 of RICA.

c. Role of the Office of Interception Centre

Firstly, although the OIC is a regulatory authority over Interception Centres, however, the OIC demonstrates that charity begins at home in terms of securing online communication under the provision that members or officers of the OIC are required to provide a security clearance before carrying out a task in the Office.[1541] Secondly, the OIC must prescribe the type of, the manner in, and period for which information is to be kept by the head of an Interception Centre,[1542] which ensures the protection of the integrity and guarantees the security of the SOC by an Interception Centre.

In the overall analysis, RICA recognises and largely protects the concept of the SOC by regulating the conduct of an OCI, however, the provisions are inadequate to protect the integrity of and secure the SOC in the contemporary society as examined above, hence the need for this study which covers issues beyond the aforementioned.

3.9.2.5 Role of regulatory authorities in protecting the concept of the secrecy of online communication in the Protection of Personal Information Act

Three main stakeholders are charged with the responsibility of protecting the right to the SOC in the POPIA, namely: the Information Regulator, Information Officer and a Responsible Party whose roles are described or examined below.

a. Information Regulator

The Information Regulator is an independent and impartial authority, which operates without fear, favour or prejudice[1543] and is subject to the law and Constitution.[1544] The Information Regulator is accountable to the National Assembly.[1545] Besides, the office is not listed in the Constitution, let alone under the Chapter 9 Independent Institutions that support the practice and enjoyment of democratic principles and values in the RSA.

[1541] Section 34(5)(c) of RICA.
[1542] Section 35(1)(f)(i)-(ii) and (g) of RICA.
[1543] Section 39(b) & (d) of the POPIA.
[1544] Section 39(b) of the POPIA.
[1545] Section 39 (d) of the POPIA.

One of the duties, functions and powers of the Information Regulator is to make public statements on what affects the protection of personal information or any class thereof and provide education on the promotion of an understanding and the basis for accepting the condition for engaging in lawful processing of personal information and object of the conditions stipulated.[1546] The other power of the Information Regulator is to monitor and enforce compliance with the law.[1547] In addition, the Information Regulator consults with interested parties and handles complaints submitted by an aggrieved party.[1548]

Furthermore, the Information Regulator conducts research and reports to the National Assembly on necessary legislative amendments and the cross-border relation and acceptance of international instrument on the protection of personal information.[1549] Added to the foregoing is that the Information Regulators issues, amends, and revokes codes of conduct on the processing of personal information and carries out incidental powers and functions.[1550] These provisions are relatively adequate to the extent of the purpose of the objects of the Act, which arguably do not adequately specify the protection of the right to the SOC in terms of the scope, context and approach of this study.

However, in all these provisions, it is clear that the duties, functions and powers of the Information Regulator are powers meant to regulate the general protection of personal information. These powers do not address the specific or direct issues concerning the role of the Information Regulator on the integrity and security of the right to the SOC, therefore, the provisions of the POPIA concerning the function of the Information Regulator are inadequate to protect the right to the SOC based on the scope, context and approach of this study.

It is important to note that some incidental issues which may impact on the integrity and security of online communication include the appointment requirement for members of the Board of the Information Regulator who 'must be appropriately qualified, fit and proper persons' while at least one member who must be an experienced advocate, attorney or a professor of law.[1551] This is a commendable requirement that raises the bar for the role,

[1546] Section 40(1)(a)-(h) of the POPIA.
[1547] Section 40(1)(a)-(h) of the POPIA.
[1548] Section 40(1)(a)-(h) of the POPIA.
[1549] Section 40(1)(a)-(h) of the POPIA.
[1550] Sections 40(1)(f) and 60-68 of the POPIA.
[1551] Section 40(1)(b)(i) and (ii) of the POPIA.

competence, performance and integrity of the regulator in protecting information, more particularly and arguably the information in online communication.

Anyone who acts on behalf of the Information Regulator is always required to keep as confidential any personal information that comes to his or her knowledge in the course of executing an official function in this regard.[1552] With this in place, it is likely that the need to specifically and arguably address the issues concerning the integrity and security of online communication will be paramount before the Board.

It is also important to note that the appointment of the Chair and members of the Board of the Information Regulator is performed by the President of the RSA on the recommendation of the National Assembly.[1553] The involvement of the two arms of government in the selection process largely guarantees transparency, the best choice from the broad pool of qualified applicants, checks and balances and accountability in the selection process of the Board. This arguably ensures the security of online communication if the POPIA was actually or specifically adequate or enacted to protect the right to the SOC, in which the POPIA is not.

b. Information Officer

The main duties and responsibilities of the Information Officer related to the encouragement of compliance of the conditions for the processing of personal information by responsible parties and working with the Information Regulator on the investigation of conduct relating to the extension of the use of personal information by responsible parties.[1554]

However, aside from the fact that the persuasive power of the Information Officer in enforcing compliance with the conditions for processing personal information is weak and a misnomer in law enforcement because the Information Officer does not have the power to bark let alone bite; it is equally, consequently and arguably noted that the risks involved in this regard in the protection of the integrity and security protection of the right to the SOC are not catered for in POPIA.

[1552] Section 54 of the POPIA.
[1553] Section 41(2) of the POPIA.
[1554] Section 55 of the POPIA.

c. Responsible Party

Although a responsible party is not a regulatory authority as titled in the major heading,[1555] it is however a party who processes or uses personal information and is professionally or according to industry rules, required to protect the integrity and security of information, which should include an online communication. A responsible party does this by identifying the internal and external reasonably foreseeable risks and takes appropriate technical and organisational measures to prevent unlawful access, damage and loss of personal information,[1556] which arguably should include an online communication.

A responsible party (i.e. an online service provider in this regard) who supplies or receives information in or from an online communication must ensure that the quality of personal information is accurate, complete, not misleading and updated, where necessary.[1557] A responsible party must comply with the processing scope and the eight requirements for the use of personal information and be held accountable for non-compliance,[1558] which arguably should include online communication. A responsible party must inform the regulator and data subject of any breach or compromise of the integrity and security of information,[1559] which should include online communication.

Section 69 of the POPIA prohibits direct marketing by means of unsolicited electronic communications provided a user of online communication who gives consent to the processing of personal information is a customer of the responsible party. Section 69 of the POPIA, which is the most direct expression of the protection of the right to the SOC according to the scope, context and approach in this study, recognises some of the features of the non-criminal online conscription examined in this study.[1560] However, Regulation 6 of the Regulations Relating to the Protection of Personal Information, 2017 weakens or neutralises the right of a user of online communication in section 69 by making the duty to request for consent from a user of online

[1555] See para 3.9.2 of this chapter.
[1556] Sections 19 and 21(1) of the POPIA; Moorcroft J 'POPI and the legal profession: What should you know? http://www.derebus.org.za/popi-legal-profession-know/ (Date of use: 18 January 2019).
[1557] Sections 16(1), 20 and 21 (1) of the POPIA.
[1558] Sections 4, 8-11, 13-15 and 21(2) of the POPIA.
[1559] Sections 5, 21(2) and 22(1), (2), (4)-(6) of the POPIA; Moorcroft http://www.derebus.org.za/popi-legal-profession-know/ (Date of use: 18 January 2019).
[1560] Para 2.3.3.6(a) of this study.

communication discretionary by virtue of the use of the word 'may'.[1561] Consequently, the weakness in Regulation 6 is demonstrated in the business models used by Online Communication Service Providers which enable direct, automated and default online marketing by means of unsolicited online communication without complying with section 69.

Another weakness in the implementation of section 69 of the POPIA is that the provision in Form 4 of Regulation 6 of the Regulations Relating to the Protection of Personal Information, 2017 that requires that the goods and services be marketed online shall be specified in the Form is difficult, perhaps impossible to implement in online communication. Save where there is an omnibus consent, the goods and services to be marketed in online communication are uncountable, therefore, it is difficult, if not impossible for a user of online communication to grant consent for direct marketing of all goods and services.

A responsible party is required to obtain prior authorisation from the Information Regulator to extend the use of personal information earlier obtained or link the personal information earlier obtained to other responsible domestic or foreign parties,[1562] which should include an online communication. Prior authorisation is also required for processing personal information for criminal behaviour, unlawful objectionable conduct and credit reporting purposes.[1563]

However, it is noted that these provisions, before authorisation by the Information regulator, seem not to be appropriate for the conduct of an OCI because the provisions herein do not require a proof of a relevant reasonable ground to investigate the commission of an offence.[1564] These provisions under the POPIA do not comply with the major provisions in RICA, one of which is that judicial direction must be obtained before an OCI is conducted.[1565] Therefore, most of these provisions under the POPIA herein are appropriate for civil proceedings or non-criminal investigative purposes *only*.

[1561] Protection of Personal Information Act, 2013 (Act 4 of 2013): Regulations Relating to the Protection of Personal Information, 2017.
[1562] Sections 57(1) (a) (i) -(ii) and (d), 58 and 59 of the POPIA.
[1563] Sections 57(1)(b) & (c), 58and 59 of the POPIA.
[1564] Paras 6.4.5 – 6.4.9 and 6.5 of Chapter 6 of this study.
[1565] Sections 2, 3, 15, 16, 17, 18, 19, 20, 21 and 23 RICA, amongst other provisions subject to non-direction interception in sections 4-11.

Moreover, prior authorisation is required to be requested for *only once* by a responsible party before information is processed for future purposes.[1566] This corroborates the earlier submission that POPIA is inadequate in regulating the conduct of an OCI. This is because the *once-off* authorisation creates a space for perpetual extension of processing of personal information and extending the use of such information for the conduct of an OCI without complying with the provisions of RICA, which require a judicial direction for every conduct of an OCI save in exceptional circumstances as required in RICA.[1567]

d. Conclusion

In the final analysis, the fact that the POPIA does not in its schedule amend or make reference to RICA[1568] —being an older law— in any way to demonstrate that the former Act addresses most of the issues that affect the protection of an online communication shows the large extent of the inadequacies in the provisions of the POPIA. In summary, aside from the words and phrases 'data message', 'signature' and 'writing', which are defined and referred to in the POPIA Regulation which refers to ECTA which is a legislation that regulates online communication; the POPIA only redefines the term 'personal information' which recognises online communication.

Essentially, the POPIA is a legislation that generally protects personal information but grossly fails to address the specific nature, components, scope and security of the right to the SOC and the conduct of an OCI in contemporary society.

3.9.2.6 Role of regulatory authorities in protecting the concept of the secrecy of online communication in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017

Though the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 has not been enacted as a law, this segment describes and examines the role of the stakeholders in protecting the

[1566] Section 57(4) of the POPIA.
[1567] Paras 2.8, 6.2-6.7 and 6.9-6.11 of this study.
[1568] In *Jwara v State* supra 14, the Supreme Court of Appeal held that any new law which seeks to cure the defect of an old law must expressly state so in the new law. In this case, a new law included a telephone as one of the devices through which an OCI can be conducted, which was not included in the old law. See also *S v Cwele & another* 2011 (1) SACR 409 (KZP).

integrity of and securing the SOC. These stakeholders comprise both regulators and executors of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 and other laws.

The stakeholders are the Online Communication Service Providers and financial institutions,[1569] Cyber Response Committee,[1570] government structures, which include Minister of Police and LEAs[1571] and Nodal Points and Private Sector Computer Security Incident Response Teams.[1572] However, only the Online Communication Service Providers and financial institutions are retained in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017. The other stakeholders are expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017. The expunged provisions are of no effect should the Bill be enacted as it is. However, this study examines the other aforementioned stakeholders to highlight the gap that is created by the exclusion of the other stakeholders aforementioned.

a) Online Communication Service Providers and financial institutions

Under the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, the Online Communication Service Providers or financial institutions must:

a) not later than 72 hours of knowing the involvement of their computer system in any category of compromise report to the SAPS of the commission of an offence.[1573] However, given the fact that this provision relates to cybercrime commission, it would be expected that an effective and efficient system is to make a simultaneous or immediate, automatic and direct online report to SAPS to ensure the security of the right to the SOC.

b) preserve any information that may be useful for the investigation of an offence by LEAs.[1574]

[1569] Chapter 9 of the CCB B6-2017, which is replaced by Chapter 9 of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1570] Section 53 of the CCB B6-2017 is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1571] Section 54 of the CCB B6-2017 is partially expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1572] Section 55 of the CCB B6-2017 is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1573] Section 52(1)(a) of the CCB B6-2017, which is replaced by section 54(1)(a) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017. See para 6.3.2 of Chapter 6 of this study on the issues raised relating to the type of offences that can be investigated through the conduct of OCI.
[1574] Section 52(1)(b) of the CCB B6-2017, which is replaced by section 54 (1)(b) of the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017.

In conclusion, the provisions in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 are relatively adequate if compared with the provisions in other Acts that provide for the techno-legal protection of online communication. However, it is obvious that the above roles are reactive in nature and not proactive in securing the right to the SOC in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, thus inadequate in this regard.

b) Minister of Police

In securing an online communication in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, the Minister of Police, who is included in the government structures supporting cybersecurity and whose functions are highlighted in this study,[1575] has the following direct and indirect powers to:

a) from the penological point of view, classify the types of offences that are reported to the SAPS by electronic communication service providers or financial institutions,[1576] which support the appropriate application of the relevant reasonable ground standard to conduct an OCI.[1577]

b) establish and maintain adequate human and operational capacity geared towards preventing, detecting and investigating cybercrimes.[1578] The capacity to detect and prevent cybercrime is a direct and proactive way of securing the right to the SOC.

c) direct members of the SAPS to undergo basic training in the areas of detection, prevention, and investigation of cybercrimes,[1579] which directly or indirectly encourage the protection of the right to the SOC.

d) develop and implement accredited training programmes for the members of SAPS — including the CI-SAPS and HAWKS— who are involved in the primary duty of detection,

[1575] See paras 4.4.2 and 4.4.3 of this study where the role of the Minister of Police in securing online communication and interception in the area of training members of CI-SAPS and HAWKS is examined under a more relevant rubric.

[1576] Section 52(2) (a) &(b) of the CCB B6–2017, which is replaced by section 54(2) (a) &(b) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

[1577] Paras 5.4.3, 6.3 6.4, 6.5 and 6.6 of this study.

[1578] Section 54(2)(a)(i) of the CCB B6–2017, which is replaced by section 55(1)(a) of the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017.

[1579] Section 54(2)(a)(ii) of the CCB B6 - 2017, which is replaced by section 55(1)(b) & (c) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

prevention and investigation of crime.[1580] Members of SAPS are at liberty to attend the programme at an institution of higher learning in the Republic or elsewhere.[1581] This provision also promotes the protection of the right to the SOC.

e) make regulation on the administration of any aspect referred to in paragraphs (ii)-(iv);[1582] the provision of which is defective due to the non-compliance with the principle of checks and balances that requires another independent authority to contribute to the regulation.

c) Cyber Response Committee

Prior to the introduction of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, which expunged the Cyber Response Committee, the Committee would have comprised the Director-General of the SSA (who is the chairperson), heads of representative departments and one of their nominees.[1583] If the provision relating to the Committee was not expunged, the Committee would have played an indirect role in securing online communication by implementing government policy on cybersecurity.[1584]

d) Other government departments and structures supporting cybersecurity

Prior to the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, the CCB established the expunged 'government departments and structures supporting cybersecurity' which included the following structures, with their mandatory functions highlighted:

i) The Minister of State Security shall perform the duties in securing online communication as follows, amongst others. Firstly, the Minister establishes, equips, operates and maintains a computer security incident response team in the State Security

[1580] Section 54(2)(a)(iii) of the CCB B6-2017, which is replaced by section 55(1)(c) &(3)(c) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1581] Section 54(2)(a)(iii) of the CCB B6-2017, which is replaced by section 55(1)(c) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1582] Section 54(2)(b) of the CCB B6-2017, which is replaced with section 55(2) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1583] Section 53(2) of the CCB B6-2017, which is expunged in the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017.
[1584] Section 53(4), (5) & (6) of the CCB B6-2017, which is expunged by the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

on behalf of the government.[1585] Secondly, the Minister establishes and maintains sufficient human and operational capacity in giving effect to the cybersecurity measures required of the SSA in its constitutional mandate.[1586] This capacity must be capable of dealing effectively with the protection of critical information infrastructure of government.[1587] Thirdly, the Minister declares any information infrastructure as critical information infrastructure, provided the infrastructure is of a strategic nature such that any interference with, loss of, damage, disruption or immobilisation to the infrastructure may substantially prejudice the physical, health or financial security of or essential services in the RSA.[1588] Fourthly, the Minister is required to submit a report of the protection and security of the critical information infrastructure of government to the JSCI of Parliament.[1589]

These provisions are substantially adequate to broadly or generally regulate the scope of protection of online communication which other Acts examined earlier do not cover nor protect or adequately protect. However, the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 is inadequate in areas relating to the expert knowledge that the Minister of SSA may not possess in carrying out these functions.

ii) The Minister of Defence shall, amongst others, establish and maintain a cybercrime and defensive capacity for SANDF,[1590] amongst the other functions of the Minister of Defence in securing an online communication.[1591]

iii) The Minister of Justice makes the regulation on the sharing of information regarding cybersecurity incidents and prevention, detection and investigation or mitigation of

[1585] Section 54(1)(a)(i) of the CCB B6-2017, which is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1586] Section 54(1) (a) (ii) (aa) of the CCB B6-2017, which is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1587] Section 54(1) (a) (ii) (bb) of the CCB B6-2017, which is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1588] Section 57 of the CCB B6 -2017, more particularly subsection (1) & (2) (a) -(f), which is expunged in the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017.
[1589] Section 54(1)(c) of the CCB B6-2017, which is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1590] Section 54(3)(a)(i) of the CCB B6-2017. See also section 54(3)(a)(ii) & (b) of CCB B6-2017. These provisions are expunged in the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017.
[1591] See para 4.4.6 of Chapter 4 of this study.

cybercrime.[1592] However, this provision is adequate to the extent that this provision exists, otherwise, it seems inadequate because other departments are consulted neither does the provision require the Minister to make the regulation in consultation with the National Assembly.

iv) The Minister of Communication and Telecommunication shall 'establish and maintain a Cybersecurity Hub'[1593] for the following purposes: firstly, to promote cybersecurity of online communication in a private sector,[1594] which provides online communication service and requires the establishment of a nodal point;[1595] secondly, to serve 'as a central point' of convergence for government and private sector on cybersecurity of online communication.[1596] In a way, this provision may cure the defects of coordination of the activities of regulatory authorities in the ECTA;[1597] thirdly, to be responsible for the encouragement and facilitation of the establishment of nodal points and online communication security incident response teams by the private sector;[1598] fourthly, to respond to cybersecurity incidents.[1599] These provisions are relatively adequate.

v) The Minister of Communication and Telecommunication shall equip, operate and maintain the Cybersecurity Hub.[1600] This is also an adequate provision, particularly in the area of politically mobilising resources by the Minister from the colleague in the Ministry of Finance. Where this responsibility is accomplished, it raises the hope that modern equipment will be available to secure online communication.

[1592] Section 56 of the CCB B6-2017, which is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1593] Section 54(4)(a)(i) of the CCB B6-2017, which is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1594] Section 54(4) (a) (i) (aa) of the CCB B6-2017, which is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1595] Section 55(1) (a) of the CCB B6-2017, which is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1596] Section 54(4) (a) (i) (bb) of the CCB B6-2017, which is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1597] See the conclusion of para 3.9.2.3 of this chapter.
[1598] Section 54 (4)(a)(i)(cc) of the CCB B6-2017. See also section 55 of the CCB B6-2017 for more information about the nodal points and private sector computer security incident response teams. These provisions are expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1599] Section 54(4) (a) (i) (dd) of CBB B6-2017, which is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1600] Section 54(4)(a)(ii) of CCB B6-2017, which is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

vi) The Minister of Communication and Telecommunication shall ensure that members of the Hub receive accredited training programmes through the cooperation of accredited higher training programmes to establish and maintain a Hub,[1601] which is an adequate provision like the immediate foregoing provision.

vii) Under the CCB, the Minister of Communication and Telecommunication declares different sectors that provide electronic communication services as Nodal Points and Private Sector Computer Security Incident Response Teams.[1602] Each Private Sector Computer Security Response Team performs the main functions of receiving and distributing information within the sector and the Nodal Point on issues relating to cyber incidents as well as respectively reporting and receiving cybersecurity incidents to and from the Cybersecurity Hub.[1603] This is an adequate provision that brings the public and private sectors together in the area of the security of the right to SOC which cures the defect in other Acts examined above.

In summary, some of the technical aspects of online communication security fall under the jurisdiction of the Minister of Communication and Telecommunication. However, donating almost all responsibilities of the administration and function of the Cybersecurity Hub in the cluster to the Minister of Communication and Telecommunication without assigning responsibility to the Director-General of SSA is partially inadequate. This is because there is no check and balance in the performance of these roles, given the precedent in leadership crises recorded in some ministries, including the Department of Communication.[1604]

However, there would have been a solace in the provision of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 in this regard, which requires that the Minister of

[1601] Section 54(4)(a)(iii) of the CCB B6-2017, which is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1602] See section 55 of CCB B6 - 2017, which is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1603] Section 55(2) (a)-(d) of the CCB B6-2017, which is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1604] Gedye https://mg.co.za/article/2016-06-02-backlash-likely-over-digital-fail (Date of use: 22 April 2019); Maqhina https://www.iol.co.za/news/politics/minister-meddling-in-icasa-affairs-22163646 (Date of use: 1 May 2019.

Communication and Telecommunication shall submit an annual report to Parliament on the objects and functions of the Cybersecurity Hub.[1605]

Finally, despite the pendency of the enactment of the provisions of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, it is reported that the provisions on the integrity and security of online communications have regrettably been expunged from the bill,[1606] otherwise, the provisions of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 as it is, would have relatively and adequately addressed the challenges identified in the four legislations examined earlier which are the ECA, ECTA, RICA and POPIA.

3.9.2.7 Conclusion

Firstly, none of the Acts examined above under this rubric expressly use the description 'SOC' or a similar name or title to describe the value, interest or right in the protection of online communication in the contemporary South Africa society. Nevertheless, in the five legislations examined above, it is concluded that save for the provisions of the POPIA which generally protect personal information without convincing reference to online communication in relation to this study; the provisions of the ECA, ECTA, RICA and Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 recognise and protect —though with relative gross inadequacies— the right to the SOC in different ways, manners and styles.

Secondly, in most of the provisions in the five legislations examined in this regard, the exercise of powers by the regulators and executing authorities are discretionary in nature. The discretion makes it difficult to hold the regulatory authorities accountable for their failure or refusal to comply with the various provisions in the legislations in ensuring the integrity and security of online communications.

Therefore, there is a need to make the performance of the functions or roles of the regulatory and executing authorities in the five legislations mandatory in ensuring the integrity and security of the right to the SOC. The imposition of mandatory provisions in these legislations

[1605] Section 54(4)(d) of CCB B6-2017 is expunged in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

[1606] Privacy International 'State of Privacy South Africa' https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa (Date of use: 25 April 2019).

lays the foundation for the logical application of criminal sanction in this regard because penological jurisprudence[1607] will not allow punishment without making the various roles of the regulators and executing authorities mandatory in this regard.

3.9.3 Role of manufacturers in securing online communication

After approval by the National Assembly, the Minister of Communication —upon considering an application in the public interest— issues a certificate to manufacture, assemble, sell, possess, purchase or advertise online communication and interception devices to authorised persons —such as Ericsson, Sony, Internet Service Providers, Telecommunication Service Providers or LEAS respectively— who must comply with the various technical and non-technical standards provided.[1608] This provision is administratively adequate because it complies with the various issues raised thus far, one of which is the principle of checks and balances.

However, the fast pace at which technology is developing without a commensurate development of law to protect the integrity and guarantee the security of an online communication results in a breach of the right to the SOC in this regard. This is because in some instances manufacturers design or build systems that are capable of collecting data without the modern cryptographic techniques[1609] and adequate law. It follows therefore that a manufacturer installs such interception software application, which does not only operate by default but by intentional step-by-step activation[1610] without cautionary clicks by the user in the process of conducting an OCI.

3.9.4 Role of Online Communication Service Providers in securing online communication

An Online Communication Service Provider includes Telecommunication Service Providers, Fixed Line Operators, Mobile Cellular Operators, Internet Service Providers, etc.

[1607] See para 3.10 of this chapter.
[1608] Sections 44, 45 and 46 of RICA.
[1609] Blumberg and Eckersley *Locational privacy* 316.
[1610] Section 30(1) (a), (b), (2)(a)(i) -(ii) (aa) &(bb) and (3) of RICA.

An online agent is a confidant while LEAs are skilled strangers or outsiders,[1611] thus, Online Communication Service Providers play a significant role in knowing a user and at the same time warding off third parties actual or potential threats in online communication, which include the authorised legal strangers, non-authorised legal strangers and illegal strangers.

In most online communication devices,[1612] a user is expected to provide personal information to an Online Communication Service Provider or its agent to activate an online communication service. This information is recorded and saved by the Online Communication Service Provider in its database.[1613] A person, Telecommunication Service Provider or employee of a Telecommunication Service Provider must ensure that the information stored or recorded is secure and accessible to only those designated to have access to online communication.[1614]

Although a Telecommunication Service Provider can be in possession of listed equipment to conduct an OCI, conditions are attached to the possession of the equipment[1615] used by Telecommunication Service Providers to transfer an intercepted data to LEAs. The attachment of condition is to ensure that online communication and interception are not compromised.

Finally, the RICA Directive prescribes relatively adequate techno-legal provisions for Online Communication Service Providers to protect the integrity and guarantee the security of online communication and the conduct of an OCI.[1616] However, the key challenge in implementing this Directive is the low compliance level with the Directive, which results in breaching the protection of the SOC and the conduct of an OCI.[1617]

[1611] Crump *Geolocational Privacy and Surveillance Act* 280. Para 3.9.1 of this chapter.
[1612] There is no legal requirement to activate an email account, for example.
[1613] Section 39(1) & (2) and 40(5) (a) &(b), (6) and (9) of RICA.
[1614] Sections 40(4) (a) (i) -(iii), 42 and 43 of RICA.
[1615] Sections 45 - 46 of RICA.
[1616] Para 7.3 of Chapter 7 of this study where the role of executing authorities in RICA Directive is examined.
[1617] eNCA 'Inspector-General considers Magashule phone-tapping claims' https://www.enca.com/news/inspector-general-considers-magashule-phone-tapping-claims (Date of use: 3 May, 2019; eNCA 'Ace Magashule says he has reported his phone being tapped to intelligence' http://www.702.co.za/articles/346668/ace-magashule-says-he-has-reported-his-phone-being-tapped-to-intelligence (Date of use: 3 May 2019).

3.9.5 Role of the Interception Centres in securing online communication

The Interception Centre is a centre that intercepts both online and offline communication.[1618] After an OCI has been conducted, the head of the Interception Centre keeps proper records of the information gathered.[1619] The head of the Interception Centre sends a report to the Director of the OIC on a quarterly basis or as often as a report may be requested by the Director of OIC on records kept by the Interception Centre regarding defects or abuses of the interception system.[1620] Thereafter, the report is submitted to the JSCI of Parliament,[1621] thus protects the integrity, and guarantees the security of online communication and interception in this regard.

Although the head of Interception Centre performs the above administrative functions and others,[1622] the greater part of these administrative functions are performed by other authorities including the Director of OIC and the relevant ministers.[1623]

The head of the Interception Centre does not have any technical responsibility in terms of the protection of the security of the SOC and the conduct of an OCI given that other authorities assume this responsibility including the ministers of SSA and Finance and other relevant ministers and Director of OIC respectively.[1624] As posited in other submissions relating to the absence of professional requirement by ministers in performing the technical function required in securing an online communication, same or similar position is held here where the function of the head of Interception Centre is usurped by the ministers.

In effect, there is the absence of professional requirement from the Director of OIC to occupy the office because there is no such provision required in RICA.[1625]

It is also submitted that where the head of the Interception Centre is not charged with technical responsibility of securing the Interception Centre, it opens the door for blame game or a shift

[1618] Section 1and 32(1)(a) of RICA.
[1619] Section 37(1) of RICA.
[1620] Section 37(2)(a)(ii) & (iii) of RICA.
[1621] Section 37(3) of RICA.
[1622] Section 36(6) of RICA.
[1623] Section 32 (1)(d) & (2), 35 (1) (b), (c) &(e) and 36 (2) & (4) of RICA, amongst others.
[1624] Sections 32(1) (b) &(c), 35(1) and 36(2) of RICA.
[1625] Section 34(1) & (3) of RICA.

in the responsibility between the head of Interception Centre and the aforementioned functionaries. This has an adverse impact on the integrity and the security of the SOC.

3.9.6 Role of data controller in securing online communication

A 'data controller' is someone 'who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject.'[1626]

In one breath, the ECTA stipulates that a data controller *voluntarily* subscribes to and enforces the principles of collecting and protecting online personal information, without a breach; which is adequate in this regard, while in another breadth, the same provision somehow contradicts itself by stipulating that such data controller must fully enforce the principles of collecting personal online information.[1627] Furthermore, the fact that a data controller *voluntarily* subscribes to the principles in an online agreement with a data subject,[1628] which, in most cases, is imposed on a data subject in online communication, is extremely incongruous.

The incongruity arises from the fact that an online offeror —data controller— expects an offeree —data subject— to easily understand or be versatile or conversant with all the clauses of an online agreement within a jiffy of accessing such online agreement, whereas online transaction is risky, delicate and spontaneous inaction or omission.

Therefore, it behoves the data controller to inform a data subject in an appropriate and clear manner of the intent to enter into such agreement and in such reasonable terms. Such notice must not be presented in small prints, to ensure the guarantee of the integrity of online communication. Where there is compliance with the foregoing recommendation, it prevents an online communication user from sending personal information through the network to the offeror if there is no *consensus-ad-idem* safety of the online communication between the offeror and offeree, thus protects the integrity and security of online communication in this regard.

[1626] See the definition section in section 1 of the ECTA.
[1627] Section 50(1)-(3) of the ECTA.
[1628] Section 50(2) of the ECTA.

3.9.7 Role of law enforcement agencies in securing online communication

The law enforcement agencies or officers ('LEAs' or 'LEOs') include applicants identified in RICA,[1629] Decryption Key Holders, Cyber Inspectors and other entities identified in this study as having similar roles in conducting or assisting LEAs or LEOs to conduct an OCI.[1630] The role of the LEAs or LEOs is as follows.

3.9.7.1 Law enforcement agencies or officers

Amongst the other roles of LEAs or LEOs in the protection of the right to the SOC and the conduct of an OCI which are examined in various chapters in this study,[1631] a LEO *may*, prior to the conduct of an OCI, confirm from a Telecommunication Service Provider whether a customer is or was registered with the network of a Telecommunication Service Provider.[1632] The confirmation is to ensure that an OCI is not conducted on a wrong person, thus, partially guarantees the integrity and security of online communication.

This is because although the use of the verb 'may' is reasonable to justify the fact that in some urgent or emergency cases such as the use of section 23 oral application procedure in RICA and the robotic online criminal investigation[1633] may not be feasible or reasonable for a LEO to make a confirmation from a Telecommunication Service Provider before embarking on an OCI. However, in general or other circumstances, the word 'may' weakens the effect of the requirement for the confirmation of the identity of the OCI target before an OCI is conducted on the OCI target. The confirmation prevents the erroneous occurrence that led to a Minister of Police being intercepted, which led to the conviction of the LEO.[1634]

[1629] See the definition of 'applicant' in section 1 of RICA and para 4.2 of Chapter 4 of this study.
[1630] Paras 2.5, 2.11, 4.2 of this study and sections 30(3), 31(4) and 32(1) and (2) of the CCB B6-2017, which are replaced by sections 32(3), 33(4) and 34(1) and (2) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1631] See more particularly chapters 4-7 of this study.
[1632] Section 40(7)(a) & (b) of RICA.
[1633] Para 2.11.4 of Chapter 2 of this study.
[1634] Right2Know 'Spooked- Surveillance of Journalists in SA' at 13-14 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018 (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

Although a LEA can be in possession of listed equipment to conduct an OCI, however, some conditions are attached to the possession of the equipment.[1635] The attachment of conditions is an adequate provision, which ensures that online communication and interception are not compromised as it has been happening for some time in the RSA.[1636]

In *Jwara v State*, although an innocent and insignificant technical error was made which did not affect the root of the OCI application, however, the Supreme Court of Appeal in its review application held that the SAPS in investigating its members did not compromise the integrity of the conduct of an OCI. This is because SAPS did not supply false information that would have had a material negative impact on the integrity of the conduct of an OCI and consequently, the display of good faith in the application secured the integrity of the right to the SOC in this regard[1637] as opposed to *State v Pillay & others* where material false information was furnished in the OCI application.[1638]

3.9.7.2. Cyber Inspectors

A Cyber Inspector —'Online Communication Special Police'— who is an online communication specialist is required to have an in-depth technical online communication knowledge to assist an ordinary LEO who conducts an OCI and who may not be generally trained in the cyber inspection. This is because a LEO is assisted by a Telecommunication Service Provider and an Interception Centre to conduct an OCI, therefore, a LEO may not be required to have the same specialised technical online communication knowledge required of a Cyber Inspector for purposes of conducting an OCI.

It is provided that a Cyber Inspector may monitor, inspect, search and seize any online communication or activity of cryptography and authentication service providers and thereafter, submit a report of any unlawful activity in online communication to the appropriate

[1635] Section 45-46 of RICA.

[1636] United Nations para 42 at 8 https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fZAF%2fCO%2f1&Lang=en (Date of use: 18 January 2019); Michalson https://www.michalsons.com/blog/un-human-rights-committee-concerned-about-privacy-and-interc (Date of use: 18 January 2019); Maphumulo 2016-08-30 *The Sunday Independent* 1; Maphumulo 2015-11-03 *The Star* 2.

[1637] *Jwara v State* supra 13 and 25 is one of the few cases where SAPS held their members accountable by conducting an OCI on them.

[1638] *State v Pillay* supra 410.

authority.[1639] These provisions serve as a check and balance and ensure compliance with the accountability principle in the protection of the integrity and security of online communication and the conduct of an OCI.

However, no Cyber Inspector has been appointed since the enactment of ECTA,[1640] which may perhaps be due to the fact that the power of the Director-General of the Department of Communication to appoint is discretionary.[1641] The donation of discretionary power to regulatory or executing authorities to perform a mandatory function defeats the purpose of a provision in an Act.

In essence, where no appointment is made in this regard, it frustrates the conduct of an effective OCI because, given the fact that cyber inspection is a specialised function, as opposed to the routine function of a LEO who conducts an OCI, a non-accredited or non-registered Cyber Inspector might be tempted to assume this duty erroneously or innocently, thus compromises the integrity and security of SOC. However, in adopting or relying on the conceptualisation in this study of the *Popoola QOCI* protocol which requires every LEO to go through an automated and interdependent application process to conduct an OCI,[1642] the techno-legal challenges in the conduct of an OCI are eliminated which protects the integrity and security of the right to the SOC.

3.9.7.3. Decryption key holder

A 'Decryption Keyholder" is someone who is in possession of a decryption key which is used in subsequent decryption of encrypted information in online communication.[1643]

The provision that a Decryption Keyholder is expected to perform his or her job according to his or her ability,[1644] is inadequate to guarantee the integrity and security of the SOC and the conduct of an OCI. Instead, standard performance ability and capacity established by the Act or regulation should be the norm in this regard.

[1639] Sections 80, 81(1)(a), 82 and 83 of the ECTA.
[1640] *State v Miller* supra 41 and 56.
[1641] Section 80(1) of the ECTA; *State v Miller* supra 41 and 56.
[1642] Para 6.11 of Chapter 6 of this study.
[1643] Section 1 of RICA.
[1644] Section 29(5) of RICA.

Generally, no person —including a Cyber Inspector,[1645] LEAs, a Decryption Keyholder or its employee— may disclose any information obtained concerning the performance of his or her duty under RICA save as required by RICA or other law, which must be disclosed to the extent that is required for the performance of the duty or for other official obligations.[1646] This provision protects the integrity and security of the SOC.

3.9.8 Role of users in securing online communication

The advice that your data is yours if and only if you control and manage it cannot be overemphasised in highlighting the role of users of online communication in securing the SOC.[1647]

It is posited by technologists, legislators and privacy advocates that the more users are protected the more users abandon their personal responsibility in online communication, thus users must be put on their toes in protecting the integrity and security of the SOC.[1648] Although users are not experts in the technical handling of online communication, however, users can personally be held liable for the integrity and security of online communication that users reasonably have administrative, operational and end-user capacity to control and manage.

For example, an owner or person in possession or control of a mobile cellular telephone that gets lost must report to a police official about the loss, failing which a penalty applies.[1649] Second, failing to give a satisfactory account of the possession of a SIM card is also an offence.[1650]

Furthermore, a user has a reasonable primary duty to ensure that his or her 'iPhone' is not activated to broadcast his or her exact location to friends where there is no intention to do so,[1651] thus must 'opt-out' of the service[1652] if not needed or required. A service that tells you where your friends are also requires the consent and activation of the user of the mobile cellular

[1645] Section 56(2)(c) of the ECTA. It is noted that this provision does not state that non-compliance is an offence.
[1646] Sections 42 and 43 of RICA.
[1647] Harper *It's modern trade: Web users get as much as they give* 371.
[1648] Harper *It's modern trade: Web users get as much as they give* 374.
[1649] Section 41(1) of RICA
[1650] Read together s 51(1)(b)(ii) with sections 52, 53(1) and 55(1) of RICA.
[1651] Wood *Prison without walls* 307.
[1652] Madrigal *I'm being followed: How Google-and 104 other companies- Are tracking me on the web* 346.

telephone, who cannot reasonably hold a Telecommunication Service Provider liable for such action or inaction.

In summary, although some of these provisions are relatively and reasonably adequate in these regards, however, a user does not have absolute control and management of an online communication device because of the role played by other stakeholders. All that a user could do is to use the end-to-end communication service.[1653]

3.9.9 Conclusion

In the examination of the various independent and interdependent responsibilities and roles of stakeholders in the integrity and security of online communication, this study reveals that:

Firstly, the five statutes examined above regulating the processing of personal information — which are the ECA, ECTA, RICA, POPIA and Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017— recognise the need to ensure the protection of the techno-legal integrity and security of the SOC in contemporary society, hence the promulgation of these extant statutes.

Nevertheless, the statutes do not expressly, effectively and practically make adequate provision for the protection of the integrity and security of the SOC as a specific right that should be outstandingly defined and protected in the statutes given the unique nature and features of the concept of the SOC, which is not just an ordinary right in the broad family of privacy concept. The worst amongst these statutes that do not provide adequate protection for the SOC is the POPIA, which regulates the broad concept of processing of personal information without convincingly making provision for the specific protection of the SOC —which is similar to section 14 of the Constitution.

The latter provision broadly protects the concept of privacy without identifying the concept of the SOC in contemporary society. Consequently, these inadequacies undermine the philosophy

[1653] Right2Know 'Spooked- Surveillance of journalists in SA' at 13-14 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018) (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

behind the need to accord a higher level of protection to the right to the SOC than the other channels or forms of privacy communication;[1654]

Secondly, the five statutes examined above do not consistently make adequate provision for the mandatory role of the regulatory and executing authorities in ensuring the integrity and security of the SOC in the same or similar way that non-regulatory stakeholders are mandatorily expected to perform their roles, failing which the latter is civilly, and criminally held liable. As a result, the former inadequacy compromises the integrity and security of the SOC;

Thirdly, most of the provisions of the five legislations examined in this segment do not comply with the principles of separation of powers, checks and balances and accountability of the functions or responsibility of the stakeholders in the protection of the integrity and security of the SOC.

Fourthly and finally, the law regulating the integrity and security of the SOC is scattered all over in the various Acts,[1655] thus, to some extent makes it difficult for proper coordination and coherence in many ways, given the complex and risky nature and features of online communication which require great expert knowledge, skill and attention in its objects, formulation, enforcement, monitoring and evaluation.[1656] Amongst others, the five pieces of legislation do not provide for a centralised, coordinated, independent and professional regulatory authority that has specialised sub-regulatory authorities to cater for the specialised areas —such as the right to the SOC and its security.

In pursuance of the calls made in 1978 that legislation be enacted to regulate the collection, storage, management and use of personal information by data banks, public and private entities, investigators[1657] and other stakeholders, including the regulatory and executing authorities, it is submitted that a stronger and immediate call is made to address the challenges in the contemporary society. This is aimed at regulating the different aspects of the protection of the integrity and security of the SOC, ranging from the licencing, manufacturing, importation,

[1654] See para 3.5.7 of this chapter.
[1655] Kosseff *Cybersecurity law* xxi.
[1656] See generally Chapter 2 of this study.
[1657] McQuoid-Mason *Privacy I* xl.

possession, advertising to the sale of online communication devices to interception or listed equipment.[1658]

3.10 SIGNIFICANCE OF IMPOSITION OF SANCTION AGAINST STAKEHOLDERS IN ENSURING THE TECHNO-LEGAL INTEGRITY AND SECURITY OF THE SECRECY OF ONLINE COMMUNICATION

Based on the level of breaches of online communication in the RSA, this column describes or highlights the significance of the impact of the imposition of criminal sanctions that should be meted out against specific and general stakeholders for non-compliance with the required integrity and security of online communication statutory provisions,[1659] to ultimately protect the right to the SOC.

This is opposed to the partial or absolute absence of provision of same or similar statutory criminal sanctions for non-compliance with the rules or non-existing rules of protection in non-online communication protection. This description explains one of the multi-dimensional or holistic approaches to this study.[1660] This approach serves as a foundation for the examination of issues in this study, including the need to recognise, protect, enforce and regulate both the right to the SOC and the practice and profession of an online criminal investigation by online criminal investigators respectively.[1661]

Nevertheless, the description herein excludes the examination of the adequacy or otherwise of the penalty prescribed below against stakeholders for non-compliance with the requirements in the conduct of an OCI. It is also noted that although the role of stakeholders —including that of LEAs— is considered in this and other segments of this study, however, the description of the penalty against other stakeholders herein is not an indication that a comprehensive

[1658] McQuoid-Mason *Privacy I* xl.
[1659] See para 3.9 of Chapter 3 of this study.
[1660] Para 3.1 of this chapter.
[1661] For instance, the sanctions imposed on LEAs herein and the performance of obligations by LEAs in the conduct of an OCI constitute one of the justifications for the recognition of the activities of LEAs in the conduct of OCI as an independent professional body. This body is distinct from the general investigative, security or intelligence services that LEAs have been erroneously fused into, see para 4.6 of this study titled 'Recognition and regulation of the profession of electronic criminal investigators'.

examination of the role of other stakeholders will be carried out in this study except where it is required.[1662]

3.10.1 There is an imposition of a penalty of a fine not exceeding R2, 000, 000 or 10 years against anyone who, without consent from the system controller, intercepts an online communication relating to a business[1663] or against any person who unlawfully intercepts, attempts to intercept or procures someone to intercept.[1664] It is arguably noted that this provision does not imply that LEAs require consent from the internal system controller to conduct an OCI, otherwise, the conduct of an OCI would be difficult, if not possible to embark upon.

3.10.2 There is an imposition of a penalty of a fine not exceeding R2,000,000 or 10 years imprisonment on a LEO. This penalty arises where, after a LEO intercepts, fails to furnish a written report to a designated judge of a request made to and recordings from the Telecommunication Service Provider to intercept an online communication to prevent serious bodily harm of a person or determine a location in case of rescuing a person in an emergency.[1665]

3.10.3 There is an imposition of penalty of a fine not exceeding R2, 000, 000 or 10 years imprisonment against an authorised person who receives or owns a decryption key and who fails or refuses to destroy the entire record of the decryption key disclosed to him or her where there are no prospects of the institution of civil or criminal proceedings arising from the gathered information.[1666]

3.10.4 There is an imposition of penalty of a fine not exceeding R2,000,000 or 10 years in imprisonment on a person who unlawfully discloses any information gathered in the exercise of his or her duty, save where required by law.[1667]

[1662] See para 7.3 titled 'Conducting online criminal investigation by executing authorities and entities' where the role of Cyber Inspectors, decryption key holder, Cryptographers, authentication service providers, TSPs, NCC and Interception Centres is examined in terms of the pre and post interception obligations.
[1663] Read together section 51(1)(a)(i) & (b)(i) with section 6(2) of RICA.
[1664] Read together section 51(1)(a)(i) &(b)(i) with section 49(1) of RICA.
[1665] Read together section 51(1)(a)(i) & (b)(i) with sections 7(4) and 8(4) of RICA.
[1666] Read together section 51(1)(a)(i) & (b)(i) with section 29(8) of RICA.
[1667] Read together section 51(1)(a)(i) &(b)(i) with section 42(1) of RICA.

3.10.5 There is an imposition of penalty of a fine not exceeding R2,000,000 or 10 years imprisonment on any person —other than an authorised person— who manufactures, assembles, possess, sells, purchases or advertises any listed equipment.[1668]

3.10.6 There is an imposition of penalty of a fine not exceeding 2 years imprisonment on any person who fails or refuses to report loss, theft or destruction of a mobile cellular phone or SIM card or fails or refuses to satisfactorily furnish information on the possession of a mobile cellular telephone or a SIM card, where such a person is unable to reasonably prove that the mobile cellular telephone or SIM was legally properly acquired.[1669]

3.10.7 There is an imposition of penalty of a fine not exceeding R2, 000, 000 or 10 years imprisonment on any person who is involved in the alteration, modification, reconfiguration interfering or tampering with online communication or device or on any person who performs a related activity in online communication or device.[1670]

3.10.8 There is an imposition of penalty of a fine not exceeding R5,000,000 on a Telecommunication Service Provider for failing to submit an affidavit to the designated judge explaining the steps taken by the Telecommunication Service Provider in routing the communication to prevent serious bodily harm to a person and the outcome of the steps taken.[1671]

3.10.9 There is an imposition of penalty of a fine not exceeding R5, 000, 000 on a Telecommunication Service Provider for failing to submit an affidavit to the designated judge explaining the steps taken by the Telecommunication Service Providers in intercepting or determining the location of a customer in case of emergency and outcome of steps taken for the recording, transcripts or notes therefrom.[1672]

[1668] Read together section 51(1)(a)(i) & (b)(i) with section 45(1) of RICA.
[1669] Read together section 51(1)(b)(ii) with sections 52, 53(1) and 55(1**)** of RICA.
[1670] Read together section 51(1) (a) &(b)(i) with section 54(1) & (2) of RICA. The foregoing provisions basically mean that having a 'new technology in online communication that 'legally thwart[s] legally authorizes wiretap' in the U.S. constitutes an offence in the RSA, Landau *Lawful electronic surveillance in the face of new technologies* 229.
[1671] Read together section 51(3)(a)(iii) with section 7(5) of RICA.
[1672] Read together section 51(3)(a)(iii) with section 8(5) (a) & (b) of RICA.

3.10.10 There is an imposition of penalty of a fine not exceeding R5,000,000 on a Telecommunication Service Provider for failing to obtain, retain and verify the identity or any other document of a customer —be it natural or juristic person— who enters into a contract of service for telecommunication services.[1673]

3.10.11 There is an imposition of penalty of a fine not exceeding R5, 000, 000 on a Telecommunication Service Provider or a decryption key holder for unlawfully disclosing information obtained in the exercise of his or her duty which is contrary to the provisions of RICA.[1674]

3.10.12 There is an imposition of penalty of a fine not exceeding R5, 000, 000 on a Telecommunication Service Provider for acting contrary to the letter of a direction; forging, altering or tampering with a direction and obstructing, hindering or interfering with the activity of an authorised direction.[1675]

3.10.13 There is an imposition of penalty of a fine not exceeding R5, 000, 000 on a Telecommunication Service Provider who provides telecommunication service to a person other than a customer to whom an online communication relates.[1676]

3.10.14 There is an imposition of penalty of a fine not exceeding R100, 000 for each day against an Online Communication Service Provider for the occurrence of the offence of failing to comply with the directive on the 'security, technical and functional requirements' for interception and storage devices.[1677] It is an offence to refuse to confirm or provide the details of a customer in a request by LEAs as well as failing to comply with the directive to obtain, keep and verify the details of a mobile cellular telephone customer and telephonic number, save where a customer roams into the RSA.[1678]

Further, there is a penalty imposition not exceeding R50, 000 on an Online Communication Service Provider or financial institution —excluding the Reserved Bank or a regulator— that

[1673] Read together section 51(3)(a)(iii) with section 39(1) or (2) of RICA.
[1674] Read together section 51(3)(a)(iii) with section 42 (2)(a) of RICA.
[1675] Read together section 51(3)(a)(iv) with section 51(1)(a)(iii), (v) and (vii) of RICA.
[1676] Read together section 51(3) (b) (i) (bb) with section 50(1) of RICA.
[1677] Read together section 51(3A) (a) with section 30(2)(a)(i)-(iii) of RICA.
[1678] Read together section 51(3A) (b) with sections 40(1)-(4), (6), (7), (9) or (10) of RICA.

fails to report to SAPS later than 72 hours of the involvement of their computer system in the commission of an offence.[1679]

3.10.15 There is an imposition of penalty of a fine not exceeding 12 months imprisonment on any person —other than a family member— who receives a SIM card without providing his or her details to an Online Communication Service Provider.[1680]

3.10.16 There is an imposition of penalty of a fine not exceeding 12 months imprisonment on an employee or agent of an Online Communication Service Provider who knows or suspects and refuses to report to the police of the submission of a suspected registration document by a customer.[1681]

3.10.17 There is an imposition of penalty of a fine not exceeding R2, 000,000 or 10 years imprisonment on any juristic person. This penalty is for the failure of the juristic person to record and verify the details of its employee to whom a SIM card has been provided by the company or on any person who rents out a SIM card without recording and verifying the details of the customer respectively.[1682]

3.10.18 There are impositions of penalties of a fine not exceeding R2, 000, 000 or 10 years imprisonment on a natural person who is a Decryption Keyholder or its employee or R5, 000,000 on a juristic person. These penalties are for failures to provide decryption assistance and not comply with the various disclosure provisions in sections 29 and 42(2) of RICA.[1683]

3.10.19 Despite the provision for indemnity from prosecution of a person involved in the contravention of RICA in good faith and based on reasonable ground belief,[1684] there is no exoneration or relief of obligation of stakeholders in the following instances to ensure that online communication and interception integrity and security are not compromised or sabotaged:

[1679] Section 52(3) of the CCB of B6-2017, which is replaced by section 54(3) of the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017.
[1680] Read together section 51(3B) with section 40(5) of RICA.
[1681] Read together section 51(3C) with section 40(8) of RICA.
[1682] Read together section 51(3D) (a)& (b) with section 62C (1) & (2) of RICA.
[1683] Read together section 51(4) (a) & (b) with sections 29(1), (2), (3) (b), (5) & (7), 42 (2) of RICA.
[1684] Section 51(7) of RICA; Paras 6.4.2 - 6.4.9 of Chapter 6 of this study.

a) where a LEO unlawfully conducts an OCI;[1685]

b) whereupon receiving a request from a LEA, a Telecommunication Service Provider fails to immediately route a communication to the IC;[1686]

c) where a Telecommunication Service Provider fails to determine the location of a customer[1687] —especially where there is a technique that can be used to prevent the collection of data in locational privacy—[1688] at own cost;

d) where a Telecommunication Service Provider fails to make necessary connection and interception assistance or provide communication to the LEAs for interception purposes;[1689]

e) where a Telecommunication Service Provider fails to install an online communication device that has an interception and storage capability;[1690]

f) where a Telecommunication Service Provider fails to comply with a directive from the ministers of Communication, Justice and other relevant departments in consultation with ICASA on the security, technical and functional requirements of interception and storage facility;[1691]

g) where an Online Communication Service Provider fails to comply with the directive on providing interception and storage devices,[1692] such as installing a software browser called TACO, which blocks online tracking;[1693]

[1685] Defenceweb 'Former police crime intelligence officer guilty of phone spying https://www.defenceweb.co.za/security/national-security/former-police-crime-intelligence-officer-guilty-of-phone-spying/ (Date of use: 27 September, 2018).

[1686] Read together sections 51(3) & (5) with sections 7(2), 8(3)(a) and 28(1)(b)(i) & (ii), (2) (a) & (b) of RICA.

[1687] Read together section 51(3) & (5) with sections 8(3) (a) &(b) of RICA.

[1688] It is contended that it is possible to develop a cryptographic technique that can does not collect data for locational privacy, see Blumberg and Eckersley *Locational privacy* 316.

[1689] Read together sections 51(3) & (5)(b) with sections 7(2), 8(3), 28(1)(b) or (2), 30(1) & (4) or 39(4) of RICA. There is an imposition of penalty of a fine not exceeding R2, 000, 000 or10 years imprisonment on a natural person or an employee of a TSP or R5, 000, 000 on a juristic person.

[1690] Read together section 51(5) (b) with ss 30(1)(a) & (b) of RICA.

[1691] Read together section 51(5)(b) with sections 30(2) (a) (i) -(iii) and (4) of RICA.

[1692] Read together section 51(5) (bA)(i) with sections 30(2)(a) of RICA.

[1693] Angwin *Loss of online privacy* 333.

h) where an Online Communication Service Provider fails or refuses to make provision relating to obtaining, verifying and storing of details of a customer and assigning of a number to the SIM card of a customer;[1694]

i) where a Decryption Keyholder or its employee fails to comply with the disclosure of information provision.[1695]

In conclusion, firstly, the various Acts protect online communication to the extent that criminal sanctions are imposed on non-regulatory[1696] stakeholders for non-compliance with the various provisions that put online communication in greater risks than the already existing inherent risks in protecting the integrity and security of online communication.

The highlight of these criminal sanctions is in pursuance of the conclusion made earlier in this study that there are severe sanctions against LEOs for infringing on online communication than offline privacy.[1697] In other words, it is clear that none of these penalties hold the regulatory authorities accountable for non-compliance with strategic, administrative, policy and supervisory provisions in the various Acts that seek to protect the unique and complex right to the SOC.[1698]

Secondly, given that there are criminal sanctions against non-regulatory authorities for non-compliance with the provisions of RICA and other laws, what remains to be seen is the adequate enforcement of the right to the SOC by implementing the penalties for non-compliance provided in the various Acts described above because few cases of prosecution have been reported in this regard.[1699] This results in weak compliance with the various provisions of the law in the protection of the integrity and security of the SOC.

[1694] Read together section 51(5) (bA)(ii) with sections 40(1)-(7), (9) or (10), and 62 (6)(a)-(d) of RICA.
[1695] Read together section 51(5) (bA)(c) with sections 29(1) of RICA.
[1696] Para 3.9.3-3.9.8 of this chapter.
[1697] Para 3.5.7.11 of this chapter. See also Chapter 11 of POPIA.
[1698] See para 3.9.2.1- 3.9.2.7 of this chapter.
[1699] Para 3.5.7.11 of this chapter. Section 51(7) of RICA. Defenceweb 'Former police crime intelligence officer guilty of phone spying https://www.defenceweb.co.za/security/national-security/former-police-crime-intelligence-officer-guilty-of-phone-spying/ ((Date of use: 27 September 2018). See also Phillip B http://www.sabcnews.com/sabcnews/interception-of-communication-applications-decrease/ (Date of use: 12 January 2019) and Swart H https://www.dailymaverick.co.za/article/2018-05-20-your-cellphone-records-and-the-law-the-legal-loophole-that-lets-state-spying-run-rampant/ (Date of use: 12 January 2019).

Furthermore, should there be any enforcement of these laws, the lower echelon of human resource persons in an organisation is generally held criminally accountable than the top management echelon in the administration or implementation of these statutory provisions.

A junior official —who was a captain in the CI-SAPS— was held liable for the unlawful intercept of the mobile cellular telephone of the former Commissioner of Police and sitting Minister of Police.[1700] The captain was convicted by Pretoria Commercial Crimes Court in 2017 for an unlawful interception with three-year suspended sentence.[1701]

3.11 SIGNIFICANCE OF THE PROTECTION OF THE TECHNO-LEGAL RIGHT TO THE SECRECY OF ONLINE COMMUNICATION IN THE BILL OF RIGHT

3.11.1 Introduction

Despite that section 14 of the Constitution does not expressly recognise or that it inadequately recognises the right to the SOC, this rubric serves as one of the conclusions for the argument in this chapter that the right to the SOC —and its sub-rights—[1702] be recognised, protected and enforced as an independent right in section 14 of the Bill of Right of the Constitution of the RSA. This inadequacy is contrary to the recognition and protection of the right to the secrecy of online communication in Europe and the U.S. as a fundamental individual right, which can only be entrenched in the Constitution.[1703]

It is further submitted that the advocacy for the justification of the protection of the SOC in the RSA is premised, amongst others, on the significance of the basic and special nature and features of the fiduciary relationship in, non-compartmentalised, non-passworded compartmentalised, interoperable, conscriptive and inherent risk-based online

[1700] Right2Know 'Spooked- Surveillance of Journalists in SA' at 13-14 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November, 2018 (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[1701] Right2Know 'Spooked- Surveillance of Journalists in SA' at 13-14 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018 (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[1702] See para 8.8 of Chapter 8 of this study where the list of sub-rights is highlighted.

[1703] Ruiz *Privacy in telecommunications* 21-22; *Katz v U.S.* 389 U.S. 347 (1967).

communication.[1704] The special nature and features favourably place the right to the SOC on a scale higher than the general or broad right to privacy, which is the minimal level of protection of the various rights of the personality of an individual or juristic person.[1705]

3.11.2 Constitutionalism of the concept of the secrecy of online communication

Before one considers the constitutionalism of a legal value, interest or right, posing a constitutional hypothesis is a necessity that is required to ensure an entrenchment of a neutral principle in the examination of a constitutional right in the RSA, which can be modelled after foreign jurisprudence. This position is echoed as follows:

> '…An important way of testing one's *hypotheses*, of preventing the unwarranted intrusion of one's personal preferences, of dangerous intuitions, is *the constant search for 'neutral principles of constitutional law*'. This concept cannot be explicated here, but is one coined and fully developed by some of *the finest United States legal scholars*. It is in the search for such neutral principles that *comparative law* comes into its own, as *a critical testing tool* and *a source of new solutions to old questions*.'[1706]

Having posed the constitutional hypothesis earlier,[1707] this study proposes that a neutral constitutional principle of the SOC be entrenched in the Constitution of the RSA. Modelled after the European and U.S jurisprudence on the secrecy of telecommunication,[1708] the entrenchment of this right in the Constitution of the RSA is the litmus test consideration for and a source of panacea to the inadequate provision of privacy concept in section 14(d) of the Constitution. The consideration and panacea arise from the enormous risks encountered in online communication in contemporary society.

[1704] See paras 2.2.2 and 2.3.1-2.3.3 of Chapter Two and para 3.5.7.1 – 3.5.7.14 of this chapter. On special regulation of online communication, see also Thorton *Telecommunication law* 18-20 and Gereda *Electronic Communications and Transactions Act* 279-280.

[1705] Neethling J, Potgieter J M and Visser P J *Neethling's law of personality* (1996) 3 (Neethling, Potgieter and Visser *Neethling's law of personality*); Para 3.3 of this chapter.

[1706] Ackermann 2006 Vol 123 Issue 3 *SALJ* 514-515. Italics mine.

[1707] Para 1.2 of Chapter 1 of this study.

[1708] Ruiz *Privacy in telecommunications* 56.

One of the hypotheses to be considered in the constitutionalism of the concept of the secrecy of online communication, is, whether the concept of dignity, which is a broad one, will always evolve into new rights as expressed below?:

> '*Foundational constitutional concepts* such as *dignity*, equality and freedom *are not self-defining*. Even after all relevant historical materials and other legitimate aids to interpretation have been properly consulted and exhausted, *there are innumerable questions which can still arise in the interpretation and application of these concepts, which cannot be solved (or fully or satisfactorily solved) by looking backwards*.'[1709]

Given that the concept of dignity is not self-defining, it includes privacy concept, from which the concept of the SOC is derived in contemporary society, influenced by the great risks in online communication. The identification of the risks in online communication is one of the innumerable issues that can satisfactorily be interpreted and solved by the right to the SOC, looking into the future of the concepts of dignity and privacy in contemporary society.

Since the constitution always considers new hypotheses such as the consideration of the need for dignity in online communication, the constitution '…is a continually evolving dynamic' substance[1710] which is objectively motivated by someone, who may be a scholar —as it is being canvassed in this thesis— and not necessarily motivated by a court. A Constitution drafted by a collective front is a living substance that is subject to amendment, driven by a non-consenting mind —such as the author of this study— who reasonably identifies a dispute in the Constitution in the following observation:[1711]

> 'The determination of *a single collective original intention* on the part of persons enacting a constitution is, in my view, *a legal fiction and a dangerous one at that*…It is simply *impossible* that *all consenting minds* would have a *coherently similar understanding*, particularly of those provisions that give rise to subsequent dispute.'[1712]

[1709] Ackermann 2006 Vol 123 Issue 3 *SALJ* 504. Italics mine.
[1710] Ackermann 2006 Vol 123 Issue 3 *SALJ* 504. Italics mine.
[1711] Ackermann 2006 Vol 123 Issue 3 *SALJ* 503. Italics mine.
[1712] Ackermann 2006 Vol 123 Issue 3 *SALJ* 503. Italics mine. Similarly:

> 'Linked to the above is my belief in *the Constitution as a living reality, an objective normative corpus. The answers to problems should, ideally, be found within this system; a dialogue with it should, eventually, produce the right constitutional answer; and the judge should intrude his own personality and predilections as little as possible*. An important way of testing one's hypotheses, of preventing the

Simply put, it is a legal fallacy and catastrophe where everyone in a society coherently consents and confines itself to the original intention of a collective front in section 14(d) of the Constitution of the RSA despite the current and subsequent undeniable disputes on the risks in online communication. Given that the Constitution of the RSA has been amended sixteen times since 1996, it confirms that the Constitution of the RSA is a living substance that bows to the principle that law is made for man, and that man is not made for the law, thus, the Constitution of the RSA is elastic to accommodate the concept of the SOC. The existence and inclusion in the Constitution of the RSA of the concept of the SOC is obvious to the contrarian view of the author of this thesis who does not consent to the existing coherent general view that the concept of the SOC be confined to the broad privacy concept.

Put differently, given the broad scope of the concept of dignity, which, in contemporary society, includes the concept of the SOC,[1713] great philosophers believe that law is not static but flexible with principle, which can be included in the constitution, in which Tony Honoré generally postulates that:

> 'Ulpian's search for a philosophy underpinning the law is not surprising. Around AD 200 *intellectuals were becoming dissatisfied with the view that whatever is traditional or customary in a society is automatically right. They were looking in both politics and religion for something more universal, rational, and philosophical . . . [but] . . . [p]hilosophically minded lawyers are not members of this or that school of philosophy*. It is *a mistake to attribute to a lawyer a system of philosophy rather than a set of values*.'[1714]

In applying this postulation, philosophically minded lawyers are not expected to be intellectually stagnant with what has always been regarded as an axiom in law, if and only if those lawyers are able to stir the ship with a different set of universal, rational and philosophical sets of values, which in the exhaustive writing of this thesis are summed up in the right to the SOC. As highlighted in the scope and limitation of this study, no political,[1715] worse still,

---

unwarranted intrusion of one's personal preferences, of dangerous intuitions, is *the constant search for 'neutral principles of constitutional law*', see Ackermann 2006 Vol 123 Issue 3 *SALJ* 514 -515. Italics mine.

[1713] Paras 3.2 and 3.4.4.2 of this study.

[1714] Ackermann 2006 Vol 123 Issue 3 *SALJ* 497. Italics mine.

[1715] Para 1.7 of this thesis.

religious dimensions of online communication were considered in this study in arriving at the concept of the SOC in the Constitution.[1716]

In further advancing the need for the constitutionality of the right to the SOC in the RSA, the observation of Ackermann is instructive to unequivocally recommend the constitutionality of the right to the SOC which is modelled after foreign jurisprudence, the general basis of which is noted as follows:

> '*Without the correct formulation of a constitutional problem, it is hardly possible to come up with the right constitutional answer. Of course the right problem must, in the end, be discovered in one's own constitution and jurisprudence, but to see how other jurisdictions have identified and formulated similar problems can be of great use. I say this both from personal experience and as a matter of epistemology*.'[1717]

In other words, one of the problem statements in this study compels the formulation of the correct constitutional enquiry, which is, whether section 14(d) of the Constitution of the RSA is adequate to protect the values and interests in online communication in contemporary society in light of the heightened risks in online communication? Having painstakingly, with different approaches in this thesis, examined the rights in online communication; the problem, without doubt, can, *as most western constitutions surprisingly regard it as a fundamental right*,[1718] be located in the inadequacy of the constitutional jurisprudence and epistemology of the right to privacy in online communication in the RSA. Simply put, does privacy jurisprudence in the RSA protect or adequately protect the right to the SOC? In response to this enquiry, the right to privacy is a broad one which does not adequately protect the values and interests in online communication in contemporary society.

3.11.3 Constitutional comparativism with foreign jurisprudence on the concept of the secrecy of online communication

For over a century, the tasks of a judge have always been to, with a minimum of fuss and without any specific consciousness of doing so, *find*, *develop*, and *make* the common law in a

[1716] Para 1.7 of this thesis.
[1717] Ackermann 2006 Vol 123 Issue 3 *SALJ* 508.
[1718] Ruiz B R *Privacy in telecommunications–A European and American approach* (1997) 56 (Ruiz *Privacy in telecommunications*).

mixed system of necessity.[1719] This necessity requires and adopts a comparative or relative legal approach from judgements and scholars from other jurisdictions such as the United Kingdom, other commonwealth countries, United States of America, Netherlands and Germany, not ignoring old authorities in Holland and Western Europe.[1720] Incorporating foreign law into the domestic law of the RSA on cyber law jurisprudence is not a danger to the sovereign national legal system of the RSA; rather it is a critical development of the law in the RSA which is corroborated by this pronouncement:

> '*There seems to be the fear that in referring to foreign law one is bowing to foreign authority and thereby endangering the national sovereignty of one's own legal system*. This is manifestly not so. One may be *seeking information, guidance, stimulation, clarification or even enlightenment, but never authority binding on one's own decision*. *One is doing no more than keeping the judicial mind open to new ideas, problems, arguments, and solutions*[1721]…In my own experience I have been struck by how often, when difficulties were experienced in finding the right answer in a case, this was caused by an *incorrect* or *inadequate identification of the problem* presented by the case. *Recourse to foreign law often helped me (at least) to identify the correct problem, or to identify it properly, and I am at a loss to see what danger can lurk herein. There are, after all, few human and societal problems that are not, in their essence, universal. It is also useful to see how foreign courts have solved the problem, what methodology has been used to this end, what the competing considerations have been, and whether any potential dangers were identified in the process*.' [1722]

To model the right to the SOC in the Constitution of the RSA after the secrecy of telecommunications in foreign jurisprudence[1723] is not an actual or potential fear of submission to the jurisprudence of other countries. Rather, the relativism is the necessity that the right to the SOC be protected in the Constitution of the RSA due to the global, undeniable and enormous risks in the values and interests involved in online communication in contemporary society.

In fact, comparativism of legal issues is not limited to the right to the SOC, it generally extends to other areas in this study. For example, to find a solution to some of the legal problems in

[1719] Ackermann 2006 Vol 123 Issue 3 *SALJ* 500. Italics mine.
[1720] Ackermann 2006 Vol 123 Issue 3 *SALJ* 500 and 507. Italics mine.
[1721] Ackermann 2006 Vol 123 Issue 3 *SALJ* 507-508. Italics mine.
[1722] Ackermann 2006 Vol 123 Issue 3 *SALJ* 508. Italics mine.
[1723] Ruiz *Privacy in telecommunications* 56.

conducting an OCI in the RSA, this thesis comparatively and vehemently opposed the self-imposed U.S principle of '*no server, no law*' and adopts the principle of '*no server, but law*'.[1724] The former principle controversially requires other countries —including the RSA— to seek for and obtain consent from the U.S. authorities before conducting an OCI in an Internet-based system despite committing a serious offence in the RSA.[1725] Without doubt, this principle hinders the effective conduct of an OCI in the RSA.[1726]

However, the principle of '*no server, but law*' supports the parallel creation and adoption that states that the U.S. authorities shall not have an exclusive right over the Internet particularly in conducting an OCI[1727] of serious offences committed within the territory of the RSA or elsewhere under an international public law obligation other than in the U.S.

Therefore, if the author of this study did not engage in adequate excavation of resources in line with the principles of comparativism or summarised reference,[1728] this thesis would have been an inchoate piece of work, worthless of being considered for the award of an LL.D degree. This is because the loop-hole of submitting to the jurisdiction of the U.S. principle of '*no server, no law*' in conducting an OCI without a comparative approach would have been negligently or carelessly created and left unattended to in a scholarly form such as an LL.D degree.

Thus, in the absence of a comparative study or summarised reference in this thesis, there might not be an adequate information with which the courts in South Africa may comparatively consider the various issues which are generally raised in this thesis. For example, aside from the right to the SOC, there might not be a meaningful contribution in this study if a comparative study on the following was not conducted: formulation of mathematical formulae to solve a

[1724] Para 2.8 of this study.
[1725] For the examination of this controversial issue, see para 2.8 of this chapter.
[1726] This is one of the most used abbreviations in this study which is listed under the 'key words' at the abstract page, therefore, it may not be written in full in subsequent appearances.
[1727] *Yahoo! Inc* [2015] supra and *Yahoo! Inc* [2013] supra; *eBay Canada* supra 3, 17, 48 and 51; *UEJF et Licra* c. *Yahoo! Inc. et Yahoo France* supra; *Microsoft II*; *Microsoft I*; Osula *Remote search and seizure of extraterritorial data* 25 and 31; *Michaels R* 'Some Fundamental Jurisdictional Conceptions as applied in Judgment Conventions' 9-10 https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2281&context=faculty_scholarship (Date of use: 21 March 2016; Blackman and Srivastava (eds) *Telecommunication regulation handbook* 146 -147. 2016 (Michaels 9-10 https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2281&context=faculty_scholarship (Date of use: 21 March 2016).
[1728] Paras 1.6 and 1.7 of this study.

legal problem of conducting an OCI;[1729] application of an OCI through an audio-visual means and not the current physical application process; [1730] judicial authorisation of an OCI as opposed to the general administrative authorisation of an OCI in the U.S and UK,[1731] amongst others.

The architecture of constitutional law is not limited to domestic law and historical perspective of South Africa but attributed to some global minimum core standards where judicial notice can be relied upon[1732] as follows:

> 'In what follows, my argument assumes that *constitutional law* in the twentieth century —quite apart from the influence of binding international law— *is not a wholly nationalistic and exclusively historical enterprise*, but *embodies a certain universally normative minimum core, or at least aspires thereto*. There are, of course, limits to the impact of rationality and ethical persuasion that make further discourse impossible…'[1733]

Applying the above statement to this study, it is argued that, due to the global, undeniable and enormous risks involved in the use of online communication, there are some global normative minimum core standards and values required for the protection of online communication in the Constitution in contemporary society, the substance of which is examined in this thesis.

Despite some differences in jurisprudence, the South African courts expressly acknowledge and incorporate the role that the U.S constitutional jurisprudence plays on the development of the constitutional jurisprudence of the former in the following statement:

> 'In any event foreign law may *stimulate*, in Einstein's words, '*creative imagination' by 'rais[ing] new questions, new possibilities, . . .* regard[ing] old problems from a new angle.' In this context I should like to acknowledge my own great indebtedness to the American example and to *American constitutional* and *human rights scholarship*.'[1734]

[1729] Para 6.11 of this study.
[1730] Para 6.11 of this study.
[1731] Para 4.2 of this study.
[1732] Ackermann 2006 Vol. 123 Issue 3 *SALJ* 507.
[1733] Ackermann 2006 Vol. 123 Issue 3 *SALJ* 506. Italics mine.
[1734] Ackermann 2006 Vol. 123 Issue 3 *SALJ* 501, 505 and 509. Italics mine.

Although this study was conducted in relation to the laws of the RSA and with different and independent approaches, however, the concept of the SOC is modelled after the European and U.S jurisprudence on the secrecy of telecommunication, which is protected as a *fundamental right* by *most western constitutions*.[1735] The concept of the SOC in the RSA is stimulated by the global uniformity of the undeniable existence of the nature and features of the values, interests and rights in online communication in contemporary society.

Relying on the following quote, the refusal or failure to draw on a legal precedent from other jurisprudence where there is no clarity in the domestic legal system of the RSA is tantamount to being consumed in a legal labyrinth:

> '*I have, personally, found the comparative legal approach not only rewarding, but salutary —even admonishing— in the South African context, quite apart from all the benefits I have alluded to previously*[1736]…my experience — both of myself and other lawyers — has been that in judicial problem-solving *one can easily become trapped into a sort of tunnel vision, from which it is difficult to escape, or to see other or lateral answers*. *One's thinking becomes unimaginative*. One often ends up by rehearsing the same line of reasoning or —in a type of inductive process— by trying to find additional authority for the provisional conclusions one has already reached. *It is in this context that foreign law can play a particularly valuable role*'[1737]

The failure or refusal to consider the incorporation of the invaluable role of the concept of the SOC in Europe and U.S. into the jurisprudence of privacy as a concept giving birth to the SOC in the RSA in contemporary society where the nature and features of online communication are universally and undeniably risky is a trap in a legal tunnel in the RSA. This trap opens doors for the unimaginative actual and potential losses that will occur to a user of online communication in the RSA, if there is no adequate protection of online communication by recognising and protecting the right to the SOC.

Similar view of driving our legal system to the labyrinth if no comparative study is done in the RSA is strongly expressed by O'Regan J in *K v Minister of Safety and Security* who observes that:

[1735] Ruiz *Privacy in telecommunications* 56.
[1736] Ackermann 2006 Vol. 123 Issue 3 *SALJ* 514.
[1737] Ackermann 2006 Vol. 123 Issue 3 *SALJ* 509.

> 'Counsel is correct in drawing our attention to the different conceptual bases of our law and other legal systems. As in all exercises in legal comparativism, it is important to be astute not to equate legal institutions which are not, in truth, comparable. Yet in my view, the approach of other legal systems remains of relevance to us. *It would seem unduly parochial to consider that no guidance, whether positive or negative, could be drawn from other legal systems' grappling with issues similar to those with which we are confronted*. *Consideration of the responses of other legal systems may enlighten us in analysing our own law, and assist us in developing it further*. *It is for this very reason that our Constitution contains an express provision authorising courts to consider the law of other countries when interpreting the Bill of Rights*. *It is clear that in looking to the jurisprudence of other countries, all the dangers of shallow comparativism must be avoided*. *To forbid any comparative review because of those risks, however, would be to deprive our legal system of the benefits of the learning and wisdom to be found in other jurisdictions. Our courts will look at other jurisdictions for enlightenment and assistance in developing our own law. The question of whether we will find assistance will depend on whether the jurisprudence considered is of itself valuable and persuasive. If it is, the courts and our law will benefit. If it is not, the courts will say so, and no harm will be done.*'[1738]

To ignore the role played by foreign jurisprudence on the need to protect the right to the SOC in the Constitution of the RSA is to figuratively submit to legal suicide or succumb to abortion or still birth on the jurisprudence of cyber law in the RSA without examining the merit of the cyber constitutional relativism with other jurisdiction.

In *Bernstein v Bester No*, the court reiterated the usefulness of embarking on a comparative study where it grappled with resolving a constitutional issue as expressed below:

> '*Comparative study is always useful, particularly where courts in exemplary jurisdictions have grappled with universal issues confronting us. Likewise, where a provision in our Constitution is manifestly modelled on a particular provision in another country's constitution, it would be folly not to ascertain how the jurists of that country have interpreted their precedential provision*.'[1739]

[1738] *K v Minister of Safety and Security* 2005 (9) BCLR (CC) paras 34-35; Ackermann 2006 Vol. 123 Issue 3 *SALJ* 509.

[1739] *Bernstein v Bester No* 1996 (2) SA 751 (CC) or 1996(4) BCLR 449 (CC) paras 132-133; Ackermann 2006 Vol. 123 Issue 3 *SALJ* 510.

Since the globe —including the RSA— is grappling with the protection of the invaluability of the interests in online communication, it is folly or foolhardy of this study not to consider protecting the values and interests in online communication in the Constitution of the RSA as an independent or dependent right to the SOC, which is modelled after the secrecy of telecommunication jurisprudence of Europe and U.S.[1740]

Remedying the wrongs in terms of relativising a fundamental right in the Constitution of the RSA with the global perspective is worthwhile:

> '*Any attempt to present fundamental human rights in terms that may lead to greater global understanding and acceptance of these core concepts and values, and that may contribute to the elimination of 'barbarous acts which . . . outrag[e] the conscience of mankind' is worthwhile*. *One should try, as far as is possible, to avoid these rights being rejected on the basis of cultural relativism, one of its arguments being that these rights are not universal, and the entitlement of all humankind, but relative to the cultures and political philosophies of only certain communities*. I would suggest that by *adopting a comparative legal approach*, one would at least *start a process of greater understanding of the fundamental values of other legal systems* and, in the resulting dialogue, *work towards a greater universalizing of these values as enforceable rights*. This may, in the long term, help *diminish the continuing* and *widespread assault* on *human dignity*, which appears no longer to outrage the conscience of humankind to the same extent as previously.'[1741]

The protection and enforcement of the independent right to the SOC should not be rejected in the Constitution of the RSA on the basis that it is protected under the broad privacy concept in section 14(4) of the Constitution, which, in any case, is inadequate to protect the values and interests in online communication in contemporary society. The undeniable and enormous risks in online communication, which are universal, are eliminated by the protection of the fundamental right to the SOC, which is comparatively enforceable in the Constitution of the RSA, to better comprehend and acknowledge the international perspective to the core values and interests in online communication.

[1740] Ruiz *Privacy in telecommunications* 56.
[1741] Ackermann 2006 Vol. 123 Issue 3 *SALJ* 515. Italics mine.

3.11.4 Conclusion

Considering the overall analysis in this chapter, it is believed that although it may be argued in some quarters that the current legal *status quo* in section 14(4) of the Constitution protects the right to the SOC in the right to privacy, however, there is arguably no express protection of the right to the SOC in section 14(4). It therefore follows that, given the findings in this study,[1742] the arguments canvassed in this chapter favourably place the right to the SOC on the same or similar pedestal with other rights that are expressly or specifically provided in the Constitution, including the right to privacy, from which the right to the SOC is derived and should be incorporated in the Constitution. The argument for the protection of the latter right is in response to the exponential and unpredictable nature and features of the fiduciary relationship in, non-compartmentalised, non-passworded compartmentalised, interoperable, conscriptive and inherent risk-based online communication, which has become anatomic to almost every human being in contemporary society.[1743]

3.12 CONCLUSION

The concept of State secrets states that no matter how 'trivial or momentous' government information is, it is still protected by the law.[1744] Drawing on this concept, although there is no absolute secrecy,[1745] however, it is submitted that no matter how trivial a data is in online communication, its communication relatively remains a secret once an individual uses an online channel of communication, subject to the principle of professional communication privilege.[1746]

Diverse arguments have been canvassed by the courts —including the Constitutional Court— and scholars on the understanding of the 'amorphous and elusive' concept of privacy[1747] in

[1742] Reliance can be placed on para 2.12 of Chapter 2 of this study titled 'Conclusion' aside from other findings in this study.
[1743] See paras 2.2.2 and 2.3.1-2.3.3 of Chapter Two and para 3.5.7.1 – 3.5.7.14 of this chapter. On special regulation of online communication, see also Thorton *Telecommunication law* 18-20 and Gereda *Electronic Communications and Transactions Act* 279-280.
[1744] Mathews *State secrecy* 39.
[1745] Mathews *State secrecy* 36.
[1746] See para 6.15 of Chapter 6 of this study.
[1747] *Bernstein v Bester No* supra 65; Rautenbach 2001 Vol. *TSAR* 115; Neethling 2005 122 *SALJ* 18-19; Solove 2002 Vol. 90 *California Law Review* 1088; Rautenbach 2009 3 *TSAR* 550 and 554; Currie 2008 3 *TSAR* 550-551.

different ways in both offline and online communication regimes. There is no doubt that an individual relies on the principles of the legitimate expectation of privacy and the reasonable continuum of privacy interests in enforcing his or her rights in personality right.

The privacy right includes amongst others, the right to personhood, human dignity and autonomy; right to intimacy; right to be left alone; right to limit access to the self; right to control information and communication, all of which is applicable in this study and the contemporary society in the right to the SOC.[1748]

Although the Constitutional Court and other courts certainly have the mandate to effectively embark on the development of post-apartheid judicial constitutionalism,[1749] however, the protection of online privacy is, in a way, at its infancy or underdeveloped in South African law.[1750] One of the reasons for its infancy is that the Constitution of the RSA has not recognised the indispensable contemporary societal right to the SOC —modelled by Europe and the U.S.— despite the non-compartmentalised, non-passworded compartmentalised, interoperable, conscriptive, 'no server, no law', inherently risky and fiduciary relationship based online communication.[1751]

In Europe and U.S., the authorities and scholars posit that the right to the SOC should not be dependent on the right to privacy because the former is a distinct right, therefore, the right to the SOC should be independent of the right to privacy.[1752] This study canvasses for the right to the SOC comprising, amongst others,[1753] four sub-rights to the indispensable access to online communication; control intangible, intellectual and invaluable property; controlled online conscription and the integrity and security of online communication.[1754]

Drawing on the statement by Hill that 'one cannot say that the concept of privacy does not exist…only that it is different from the Western world',[1755] similarly, one cannot conclude that the concept of the right to the SOC does not exist in the contemporary society such as the RSA.

[1748] Paras 3.4.4.1 – 3.4.4.6, 3.4.5.1- 3.4.5.5 and 3.5 of this chapter.
[1749] *Bernstein v Bester NO* supra 2; *Mistry v Medical and Dental Council* supra 3.
[1750] SALRC 2.4.3. http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016
[1751] See paras 2.2, 2.3, 2.8 and 3.5.7.2 – 3.5.7.14 of this study for the examination of the features of online communication.
[1752] Ruiz *Privacy in telecommunications* at 9 and 16.
[1753] See para 8.8 of Chapter 8 of this study where other sub-rights of the right to the SOC are highlighted.
[1754] Para 3.4.5 of this chapter.
[1755] McQuoid-Mason *Privacy I* 2.

It is only that the courts —including the Constitutional Court— do not unequivocally recognise the right to the SOC but unconsciously or unwittingly recognise the activity, event or transaction of secrecy involved in online communication.

There is no doubt that 'Freedom is not something which can be given, it is only taken'.[1756] In a similar vein, if the right to the SOC —which is a form of online freedom— is not recognised, claimed or taken now especially in the pending litmus test case of *AmaBhugane*[1757] at the Constitutional Court, then, an opportunity is for some time lost to restore the dignity of users in online communication, which is long overdue.

From the survey of literature and statutory provisions on the jurisprudence of the concept of the SOC in the RSA,[1758] the following main cumulative or alternative findings conclude that the right to the SOC is a reality in the contemporary society.

Firstly, using the substantive approach in examining the existence of the jurisprudence of the right to the techno-legal right to the SOC,[1759] a higher level of protection for the SOC above other channels of privacy communications is established and supported in this study. This study does not canvass for the position that the right to 'secrecy is for the sake of secrecy'[1760] in online communication.

Rather, there is overwhelming evidence to prove that the right to the SOC is a well-deserved right in contemporary society such as the RSA due to the seriousness of risks involved in the protection of the content and activity of online communication, the right of which should be incorporated in the Constitution of the RSA. Some descriptions of the concept of SOC in this chapter are either same or similar to the descriptions in the established concept of the 'right to secrecy of telecommunication' in the US, German and European privacy jurisprudence.[1761]

[1756] De Villeirs F 'Confidentiality and journalism' in Oosthuizen G C et al (eds.) *Professional secrecy in South Africa* (1983) 66 (De Villeirs *Confidentiality and journalism*).

[1757] *AmaBhungane v Minister of Justice* supra.

[1758] See para 3.5.7 of this study generally.

[1759] See paras Chapter 2 and paras 3.2-3.8 and 3.11 in pursuance of the first objective in this chapter described in para 3.1 of this study.

[1760] Pakendorf H 'The Journalist and his sources' in G C Oosthuizen et al (eds.) *Professional secrecy in South Africa* (1983) 69.

[1761] See *Riley v California* and *US v Wurie* supra 1-4 of the Syllabus and 4, 8-12, 17-21, 24 and 25 of the Opinion and 4 and 5 of the minority judgment of Alito J and Ruiz *Privacy in telecommunications* 1-5, 15, 20-23, 45-46, 59-67, 70, 81-83, 86-87, 143, 151-159, 171-172, 175-177, 179- 257, 313-318 and 322-323.

Secondly, although the right in online communication is generally recognised and protected in the RSA because stakeholders are apportioned responsibility in ensuring the integrity and protection of online communication, nevertheless, there are relative inadequacies in the provisions of the statutes which do not address the role of stakeholders in the recognition, protection and enforcement of the right to the SOC in contemporary society. The inadequate provisions in the protection of the right to the SOC are opposed to the non-existing or non-coordinated responsibility of stakeholders in the non-online communication privacy protection.

Thirdly and finally, the criminalisation for non-compliance with the provisions of some statutes regulating an online communication also translates into the recognition, protection and enforcement of the right to the SOC in the RSA.

I am a Haast's eagle with a seemingly dysfunctional brain, ears, eyes, legs, nose, tongue and wings, yet saddled with overwhelming operational expectations of being a panopticon of criminal activity in the aves kingdom; otherwise, I drown in the labyrinth of the sea, condemned by the supreme oversight of the superjacent beings. Who am I? I am a poor, dying, staggering, wobbling and shadowed eagle, with fainting breathe, without any hope of survival in the stormy eagling but if you rescue me as flotsam, I would survive the jetsam in the kingdom.

CHAPTER 4: MANAGEMENT OF THE AFFAIRS AND ACTIVITIES OF LAW ENFORCEMENT AGENCIES IN THE CONDUCT OF ONLINE CRIMINAL INVESTIGATION

4.1 INTRODUCTION

Given the central and indispensable role that LEAs or LEOs play in the conduct of an OCI, which is the other side of the coin in this study, this chapter investigates the legal framework on the institutional[1762] and structural[1763] independence,[1764] impartiality[1765] and transparency[1766]

[1762] Pieters C 'Institutional independence: Why is it important and what are we doing?' http://www.ngopulse.org/article/2016/02/10/institutional-independence-why-it-important-and-what-we-are-doing (Date of use: 16 February 2019).

[1763] Moodley D *The Perceptions of Crime Intelligence manager's on the organizational structure of the Crime Intelligence Division of the South African Police Service* (2006) at v; Right2Know at 7 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November, 2018).

[1764] De Vos P 'The South African Police Service Amendment Bill: Compliance with *Glenister v President of the Republic of South Africa*' at 3 http://constitutionallyspeaking.co.za/pierre-de-vos-memo-on-sa-police-service-amendment-bill/ (Date of use: 1 October 2013) (De Vos http://constitutionallyspeaking.co.za/pierre-de-vos-memo-on-sa-police-service-amendment-bill/ (Date of use: 1 October 2013); Reeves C 'After Glenister-The case for a new dedicated agency' 2012 39 *SACQ* 23 at 24-29 (Reeves 2012 39 *SACQ* 23); Lewis M and Stenning P 'Considering the Glenister judgment –Independence requirements for anti-corruptions institutions' 2012 39 *SACQ* 11 at 12-15 (Lewis and Stenning 2012 39 *SACQ*).

[1765] *State v Jackie Sello Selebi* Case No. 25/09 paras 5 and 6 and *Jackie Sello Selebi v State* Case No. 240/2011. Sections 1 of GILAA *II*. Ministry for Intelligent Services 'Regulation 4 -Profile of an intelligence officer' Notice No 1505 Regulation No. 7797 Gazette No. 25592 of 2003.

[1766] South African History Archives 'General Intelligence Laws Amendment Bill' at 4 http://db3sqepoi5n3s.cloudfront.net/files/docs/120322saha_1.pdf (Date of use: 17 July 2013 (South African History Archives http://db3sqepoi5n3s.cloudfront.net/files/docs/120322saha_1.pdf (Date of use: 17 July, 2013); Sections 32 (1), 101(3) and 36 of the Constitution and section 41 of Promotion of Access to Information

of the management of the affairs and activities of LEAs or LEOs in the RSA.[1767] In particular, this study examines the different[1768] thresholds for the appointment and skills required of LEOs, the operations and funding and the accountability and oversight[1769] of the six categories of LEAs recognised by RICA in conducting an OCI[1770] in the RSA,[1771] keeping in mind the basic principles of separation of powers and checks and balances, amongst other principles.

4.2 OBLIGATION TO CONDUCT ONLINE CRIMINAL INVESTIGATION BY SELECTED LAW ENFORCEMENT AGENCIES

The obligation to conduct an OCI in the RSA lies in six categories of LEAs only[1772] who are assigned some specialised functions in RICA.[1773] However, RICA does not include the other

Act No. 2 of 2000 (PAIA No. 2 0f 2000); Applicants' affidavit in *AmaBhungane v Minister of Justice* supra194.

[1767] OECD "Effective means of investigation and prosecution of corruption" at 10 http://www.oecd.org/corruption/acn/47588859.pdf (Date of use: 21 March, 2014; De Vos at 3 http://constitutionallyspeaking.co.za/pierre-de-vos-memo-on-sa-police-service-amendment-bill/ (Date of use: 1 October 2013); *Pharmaceutical Manufacturers Association of SA: In Re Ex parte President of the Republic of South Africa* 2000 (2) SA 674 (CC) para 90; Kapoor H L *Police Investigation and Procedure* (1989) at xv; See the definition of intelligence, OIGI 'White Paper on Intelligence' at 2 http://www.oigi.gov.za/Legislation/white_paper_on_intelligence.htm (Date of use: 20 January 2014 (OIGI at 2 http://www.oigi.gov.za/Legislation/white_paper_on_intelligence.htm (Date of use: 20 January 2014); NIA 'Investigations on Mr. Macozoma' 6; Jurgens and Savides 2015- 07-12 *Sunday Times* 1-2; Maphumulo 2016-08-30 *The Sunday Independent* at 1; Shaikh 2015-08-30 *The Sunday Independent* 3; Puren 2015-10- 29 *You* 136 -137; Maphumulo 2015-11-03 *The Star* 2; Right2Know 'Spooked- Surveillance of Journalists in SA' https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018 (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[1768] Although section 195(5) of the Constitution stipulates that different or special legislation may be enacted to address the needs of 'different sectors, administration or institutions' in the RSA, however, this study posits otherwise in the areas of specialized staff and training, operation and funding and accountability and oversight of LEAs in the specialized field of conducting of an OCI.

[1769] Calland R and Masuku T 'Tough on crime and strong on human rights: The challenge for us all' (2009) *Sabinet Law, Democracy and Development* 2009 131; Fazel I 'Who shall guard the Guards? Civilian Operational Oversight and the Inspector-General of Intelligence' in Hutton L (ed.) To Spy or Not to Spy? (2009) 157 *Monograph* 32 (Fazel 2009 157 *Monograph*); Hartley W 'Single intelligence body wields great power' http://www.bdlive.co.za/national/2013/08/08/single-intelligence-body-wields-great-power (Date of use: 28 February 2014) (Hartley http://www.bdlive.co.za/national/2013/08/08/single-intelligence-body-wields-great-power(Date of use: 28 February 2014); OIGI at 2 http://www.oigi.gov.za/Legislation/white_paper_on_intelligence.htm (Date of use: 20 January 2014; Kohn L 'The Burgeoning Constitutional Requirement Rationality and Separation of Powers: Has Rationality Review gone Too Far' 2013 130 *SALJ* at 813 (Kohn 2013 130 *SALJ*).

[1770] Section 1 of RICA.

[1771] AmaBhugane 'Advocacy: amaB challenges Snooping Law' https://AmaBhungane v Minister of Justice.org/advocacy/advocacy-amab-challenges-snooping-law/ (Date of use: 20 April 2017 (AmaBhugane https://AmaBhungane v Minister of Justice.org/advocacy/advocacy-amab-challenges-snooping-law/ accessed 20 April 2017); Right2Know at 2 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[1772] See section 1 of RICA.

[1773] Section 16(3)(a)-(d), (5)(a)(i)-(v) of RICA.

independent and specialised public institutions and private entities which are in the same or similar position with the six LEAS in the enforcement of the law in the RSA.[1774] The roles of the six categories of LEAs are described below.

Firstly, the CI-SAPS, which is a unit like any other unit under the management and control of SAPS,[1775] does not have its functions coded in law[1776] but it is at the centre of discharging the functions of an OCI as required by RICA. CI-SAPS generally deals with the investigation of the offences occurring domestically.[1777]

Secondly, the DPCI or Hawks oversees the investigation of priority crimes which the CI-SAPS may not be able to deal with or that may be conducted in conjunction with CI-SAPS, where cooperation is required.[1778]

Thirdly, the IPID polices the SAPS for wrongful police action, inaction, misconduct or wrongdoing.[1779]

[1774] Section 16(3)(a)-(d), (5)(a)(i)-(v) of RICA.

[1775] Section 209(1) of the Constitution. Sections 11(2)(d) and 15 of the SAPSA; SAPS Civilian Secretariat for Police 'Green Paper on Policing' at 30 http://www.policesecretariat.gov.za/downloads/green_paper_policing.pdf (18 September 2013 (SAPS Civilian Secretariat for Police at 30 http://www.policesecretariat.gov.za/downloads/green_paper_policing.pdf (Date of use: 18 September 2013); SAPA 'Phiyega does "Structural Change" on Crime Intelligence' http://www.enca.com/south-africa/phiyega-does-structural-change-crime-intelligence (Date of use: 21 February 2014) (SAPA http://www.enca.com/south-africa/phiyega-does-structural-change-crime-intelligence (Date of use: 21 February 2014); CI gathers, collates, analyses and manages crime intelligence with a view to provide technical support for investigations and crime prevention. Joint Standing Committee on Intelligence 'Annual Report of the Joint Standing Committee on Intelligence for Financial Year Ending 31 March 2010' at para 4.9 http://www.pmg.org.za/docs/2011/comreports/110921jcintelligencereport.htm (Date of use: 13 October 2013 (Joint Standing Committee on Intelligence at para 4.9 http://www.pmg.org.za/docs/2011/comreports/110921jcintelligencereport.htm (Date of use: 13 October 2013)**;** Sections 1(f) and (g) and 5 of the GILAA *II*.

[1776] Privacy International 'State of Privacy South Africa' https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa (Date of use: 25 April 2019 (Privacy International https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa (Date of use: 25 April 2019).

[1777] Sections 199(1) and 205(3) of the 1996 Constitution; Zinn R 'Inside information- Sourcing Crime Intelligence from Incarcerated Armed Robbers' (2010) 32 *SACQ* 27 at 27-29b (Zinn 2010 32 *SACQ*)**.**

[1778] Berning J and Montesh M 'Countering Corruption in South Africa-The Rise and Fall of the Scorpions and Hawks' 2012 39 *SACQ* 3 at 5-8; Kinnes I and Newham G 'Freeing the Hawks-Why an Anti-Corruption agency should not be in SAPS' 2012 39 *SACQ* 33 at 33-39 (Kinnes and Newham 2012 39 *SACQ*); Mashele P 'Will the Scorpion Still Sting?-The future of the Directorate of Special Operations' 2006 17 *SACQ* 24 at 24-29; Wannenburg G 'Putting Paid to the Untouchables?- The Effects of Dissolving the Directorate of Special Operations and Specialized Commercial Crime Units' 2008 24 *SACQ* 17 at 17-20; Section 199(1) of the 1996 Constitution and *Glenister v President of the Republic of South Africa and others* 2011 (7) BCLR 651 (CC) (*Glenister*). DPCI succeeds the former Directorate of Special Operations ('DSO' - 'Scorpion') which was under the control of the NPA.

[1779] See the preamble of the IPIDA; Section 50 of SAPSA establishes the IPID which replaces the Independent Complaints Directorate (ICD); Faull A 'On the record- Interview with Francois Beukman, Executive Director Independent Complaint Directorate' 2011 36 *SACQ* 37 at 38-40.

Fourthly, the ID-NPA, which is a directorate under the NPA, conducts prosecution led-investigation into some high priority crimes.[1780]

In 2011, the Constitutional Court disbanded the ID-NPA under the name 'Scorpions'.[1781] However, the proclamation in 2019 by the President of the RSA on the powers, functions and jurisdiction of the special investigating unit is, arguably, in furtherance of the already existing ID-NPA because, after the provision in the NPAA was enacted, at no time did the provision establishing the ID-NPA was repealed by NPAA.[1782] Therefore, the 2019 proclamation only reactivates the suspended functions or operations of the erstwhile Scorpion, which was abolished before the 2019 proclamation.

It is important to note that the re-introduction of the re-branded 'Scorpion' contravenes the principles of separation of powers and checks and balances as stated in the case involving the

[1780] The decisions in *Glenister* supra 163, *National Director of Public Prosecutions v Zuma* 2009 2 SA 277 (SCA) and *Democratic Alliance v President of the Republic of South Africa and others* Case CCT 122/11 -[2012] ZACC 24 http://www.saflii.org/za/cases/ZACC/2012/24.html (Date of use: 8 March 2013) (*DA v President*) are in support of the principle of separation of powers and the disbandment of the Directorate of Special Operations ('DSO' popularly known as the Scorpions) as an independent special investigating directorate created under National Prosecuting Authority Act ('NPAA') 32 of 1998, see Wolf L 'The Prosecuting Discretion: A Power under Administrative Law or Criminal Law?' 2011 4 *TSAR* at 704. The second leg of s 179(2) of the 1996 Constitution read in conjunction with section 7 of NPAA may empower NPA to maintain an Investigating Directorate (ID-NPA). The Directorate is necessary or incidental to instituting criminal proceedings in pursuance of a request under section 17D (3) of SAPSA. Sections 199(1) and 205 (3) of the Constitution and sections 26 and 28(1)(d) of NPAA (as amended) reiterate the supreme and primary function of SAPS in terms of investigation. Provision is made for checks and balances in the creation of the office of the ID-NPA; Sections 1,1A, 5(2)(c) and 7(1), (2) and (3) of NPAA.

[1781] *Glenister* supra 6; Section 179(2), (3)(b) & (7) of the Constitution, Sections 13(1)(c) and 24 (3) & (7) of the National Prosecuting Authority Act ('NPAA') No.32 of 1998. *SAPS v Zim & Dugard* supra 51, 56 and 60 echoes the judgement in *Glenister* supra 6. NPA *Lawyers for the People- South African Prosecuting Service* (2011) at 25-27 and 38-43 https://oldsite.issafrica.org/uploads/Mono53.pdf (Date of use: 15 June, 2016 (NPA '*Prosecuting Service'*). Gevers C '*Southern Africa Litigation Centre &another v National Director of Public Prosecutions & others*' (2013) 130 *SALJ* at 293-309 (Gevers 2013 130 *SALJ*); NPA 'Prosecution Policy' (2013) at 12-13 https://www.npa.gov.za/sites/default/files/Library/Prosecution%20Policy%20%28Final%20as%20Revised%20in%20June%202013.%2027%20Nov%202014%29.pdf (Date of use: 15 June 2016 (NPA https://www.npa.gov.za/sites/default/files/Library/Prosecution%20Policy%20%28Final%20as%20Revised%20in%20June%202013.%2027%20Nov%202014%29.pdf (Date of use: 15 June 2016).

[1782] Sections 13(1)(c) and 24 (3) & (7) of the NPAA**.** At the February 2019 State of the Nation Address (SONA) in the National Assembly, the President of the Republic of South Africa announced the need to reintroduce special powers to investigate priority crimes, which analysts say is a re-birth of the erstwhile 'Scorpion', Mailovich C 'Cyril Ramaphosa set to sign proclamation to establish NPA directorate' https://www.businesslive.co.za/bd/national/2019-03-19-breaking-news-cyril-ramaphosa-set-to-sign-proclamation-on-npa-directorate/ (Date of use: 31 March 2019; Proclamation No. 20 of 2019–Government Gazette No. 42383 of 4 April 2019. Nonetheless, this study holds that the primary, broad and unfettered investigative powers of the ID-NPA was re-introduced as mentioned in the main text before the announcement by the President.

disbanded and erstwhile investigating authority, the 'Scorpion'.[1783] Nevertheless, the following is further ventilated.

In reality, should the ID-NPA be allowed to continue to maintain its legal status, such powers to conduct an OCI must be qualified,[1784] specific, secondary[1785] and limited to the investigation of some more or most serious offences only.[1786] Such offences must be offences that affect the sovereign integrity of the RSA and other related offences only to prevent abuse, clash or duplication of power or function with other LEAs or discourage the complacency of LEAs whose daily, routine or primary duty may be compromised or undermined by the functions of ID-NPA.

Mandating the ID-NPA to investigate offences that fall under the primary obligation of DPCI or HAWKS[1787] and SSA —for example— directly and indirectly makes the HAWKS and SSA rest on their oars because of the belief that ID-NPA will, after all, perform the duty of HAWKS and SSA, thus, may encourage or promote complacency in the HAWKS and SSA, for example.

Furthermore, it is submitted that instead of making the conduct of an OCI the primary duty of ID-NPA, rather make ID-NPA work in cooperation —under the security cluster arrangement or other arrangements— with the LEAs whose primary duty is to conduct an OCI of such offences.[1788]

However, one of the benefits of having ID-NPA as one of the LEAs that conduct an OCI is that ID-NPA may intervene in law enforcement proceedings by conducting an OCI where the primary LEAs fail or refuse to conduct an OCI —for whatever reason, including favouritism, nepotism, political influence or victimisation.

Fifthly, the controversially consolidated SSA —which before its consolidation had in its

[1783] Section 179(2), (3)(b) & (7) of the Constitution, Sections 13(1)(c) and 24 (3) & (7) of the NPA Act; *Glenister* supra 6; Gevers 2013 130 *SALJ* at 293-309; NPA at 12-13 https://www.npa.gov.za/sites/default/files/Library/Prosecution%20Policy%20%28Final%20as%20Revised%20in%20June%202013.%2027%20Nov%202014%29.pdf (Date of use: 15 June 2016); NPA '*Prosecuting Service'* 38-43.
[1784] NPA '*Prosecuting service'* 26.
[1785] Section 179(2) of the Constitution; *SAPS v Zim & Dugard* supra 56 and 60.
[1786] Para 6.3 of Chapter 6 of this study.
[1787] Section 17D (3) of SAPSA.
[1788] Section 199(1) of the 1996 Constitution.

structures other intelligence agencies under different authorities— deals with intelligence matters.[1789]

Lastly, the DI-SANDF —which though is under the management and control of SANDF 'has a limited public profile'—[1790] deals with military intelligence matters.

The provision that restricts the obligation of the conduct of an OCI to six categories of LEAs without including some independent public institutions,[1791] public and private entities[1792] and 'objects'[1793] is unreasonable, irrational, unjustifiable, and inadequate in the conduct of an OCI. The restriction hinders the object of collective crime control responsibility, hampers the independent investigative operations of some public institutions and entities and obstructs the sacrosanct practices of checks and balances principle amongst the LEAs, public institutions and entities in the conduct of an OCI.

However, mixed solace is found in section 15 of RICA and section 205 of the CPA,[1794] which on the one hand, allow the excluded authorities and entities to conduct an OCI and on the other hand, present their shortcomings in the conduct of an OCI. Firstly, the conduct of an OCI under sections 15 and 205 respectively is a short-cut to conduct an OCI because these two provisions

[1789] Sections 199(1) and 209 of the Constitution; The SSA is at the centre of intelligence gathering for other structures under the auspices of the National Intelligence Structure (NIS) in accordance with GILAA *II* and by virtue of sections 2(1)(a)(ii) and 6(4) of NSIA 39 of 1994. Sections 1(b) -(h) and (k), 2,(a),(b), (c) and (e), 5, 15, 17 and 52 of GILAA *II*; Section 3 of the Intelligence Services Act (ISA No. 65 of 2002); Section 4 of the NSIA 39 of 1994 and section 5 of GILAA *II* establish the National Intelligence Co-ordinating Committee (NICOC). See section 4(2), 5(1) and (2) and 6(1),(2) and (4) of the NSIA 39 of 1994; Section 6(4) of the NSIA 39 of 1994 has been condemned by some scholars and security practitioners, Hartley http://www.bdlive.co.za/national/2013/08/08/single-intelligence-body-wields-great-power (Date of use: 28 February 2014).

[1790] Privacy International https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa (Date of use: 25 April 2019).

[1791] These include Chapter Nine Institutions, Information Regulator, South African Revenue Services ('SARS') and Special Investigating Unit ('SIU'), amongst others, see Parliament of the Republic of South Africa 'Announcement, Tablings and Committee Reports' No 164 -2016 para 4.7.4 at 22 and para 10 at 47 and 50; Sections 81-88 of the POPIA; Swart H Communication 'Surveillance by the South African Intelligence Services' 2016 at 2 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf. (Date of use: 13 August 2016); Section 3(1) & (2)(b) of ITU 'Interception Policy & Legislative Text' (2012) recognises Financial Intelligence Centre ('FIC') as one of the agencies to conduct OCI, see s 1(b) and 2(b) of Financial Intelligence Amendment (FICA) Act No 10 of 2017.

[1792] See generally para 2.11 of this study titled 'Types of online criminal investigators'.

[1793] 'Objects' include robotic online criminal investigator, see para 2.11.4 of this study titled 'Robotic online criminal investigator'.

[1794] See para 6.12 of Chapter 6 of this study.

do not comply with the broad, strict and relatively reasonable provisions of RICA,[1795] resulting in the infringement of the right to the SOC.

Secondly, although sections 15 and 205 respectively and controversially make omnibus provisions that empower public institutions and entities to conduct an OCI, nevertheless, it is submitted that these provisions provide an unintended consequence of including —through NPA— all public institutions and entities on the list of LEAs qualified to conduct an OCI including all government departments. Thus, this process unnecessarily opens the floodgate for every public and private entities to conduct an unreasonable and unjustifiable OCI, which may not be the object of sections 15 and 205.

In Canada,[1796] U.K.[1797] and U.S.,[1798] numerous independent LEAs and public institutions are included as applicants that are qualified to conduct an OCI, though some of these jurisdictions allow the conduct of an OCI without obtaining or securing court direction, in which this study does not subscribe to, save where the exclusion of the direction of the court is concerning the conduct of an OCI in RICA,[1799] by robotic investigators[1800] and other circumstances.[1801]

Drawing on the experience of these three countries, it is submitted that the public institutions, entities and 'objects' that should be included as OCI applicants in the RSA under stringent and relevant requirements include the Chapter Nine Institutions in the Constitution,[1802] other

[1795] See generally chapters 6 and 7 of this study. 'The one difference is that section 205 warrants are used much more often than RICA warrants: in 2017 R2K got statistics from MTN, Vodacom, Cell C and Telkom which suggest that law enforcement agencies send them 25,000-50,000 'section 205' warrants every year, as opposed to 500 or 600 'RICA' warrants', see Right2Know at 4 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[1796] Though some of the authorities are not absolutely independent, they are permitted to conduct OCI which include public officers, peace officers, Attorney-General of a province, Deputy –Attorney General of a province, Minister of Public Safety and Emergency, Hubbard, Brauti and Fenton *Wiretapping* at 3-20.13 and 3-22.1.

[1797] Section 6 of Regulation of Investigatory Powers Act (RIPA) 2000 RIPA has ten categories of 'persons' ('interceptors ') who may apply for interception direction.

[1798] Numerous LEAs exist at both federal and state levels, Jimenez A (ed.) *Wiretapping* 17, 18, 41, 49-51, 57, 63 and 67.

[1799] Chapter 2 Part 1 of RICA.

[1800] See para 2.11.4 of Chapter 2 of this study for the role and regulation of the operation of a robotic online criminal investigator.

[1801] Paras 3.5.7.2 and 3.5.7.14 of Chapter 3 of this study.

[1802] Chapter 9 of the Constitution of the Republic of South Africa.

similar institutions[1803] such as the South African Revenue Service,[1804] private investigators[1805] and robotic and special LEOs.[1806]

For instance, the requirements for permitting a private investigator to conduct an OCI should *mutatis mutandi* be the same or similar to the invocation of the conditions for private prosecution,[1807] while special LEOs must have undergone some professional training with some level of responsibility in the field of OCI to be qualified to conduct an OCI in the RSA.[1808]

4.3 APPOINTMENT AND SPECIALISED SKILL FOR LAW ENFORCEMENT AGENCIES IN THE CONDUCT OF ONLINE CRIMINAL INVESTIGATION

4.3.1 Introduction

The integration of technologies and human resource in the conduct of an OCI is an important part of an investigation in contemporary society which requires that every LEO employed in the unit charged with the responsibility of conducting an OCI —including responding officers and laboratory technicians— must be capable of and be efficient in employing technology to conduct an investigation not only from the technical aspect[1809] but also from the legal perspective.

Such LEOs must also be able to interpret and use such data or statistics that are available for

---

[1803] These include the Special Investigating Unit ('SIU') and National Assembly ('NA'), amongst others. It is submitted that the origin of the powers of the NA to conduct an OCI is derived from its broad power to summon anyone to its sittings for question, such as the summons that was issued in Steinhoff fraud saga, see section 56 (a) of the Constitution.

[1804] 'Commission of inquiry into tax administration and governance by SARS–Final Report' file:///C:/Users/Microlab/Downloads/SARS%20Commission%20Final%20Report.pdf (Date of use: 18 December 2018). It was recommended that SARS should have a covert investigative unit and be extensively independent with appropriate checks and balances in place, Nugent R *Commission of inquiry into tax administration and governance by SARS report* (2018) at 70-71, 158 and 160 (Nugent *Commission of inquiry into tax administration and governance by SARS report*); Parliament of the Republic of South Africa 'Announcement, Tablings and Committee Reports' No 164 -2016 at 22; Right2Know 'Spooked- Surveillance of Journalists in SA' at 9 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November, 2018 (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[1805] McQuoid-Mason D J *The law of privacy in South Africa* (1978) 148-149 (McQuoid-Mason D J *Privacy I*').

[1806] See para 2.11.3 and 2.11.4 of this study.

[1807] Sections 7 -16 of CPA.

[1808] Para 4.6 of this chapter.

[1809] Police Executive Research Forum 'Cameras' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 114 -115 (Police Executive Research Forum *Cameras*).

the conduct of an OCI to enable the effective conduct of an OCI in contemporary society.[1810] However, what is generally available for use by LEOs are old and inadequate devices for an investigation that cannot match the occurrence of the reality of an incident and the required sophistication of some crime commission in contemporary society. [1811]

Consequently, in the RSA, there is a dearth of, non-compliance with and inadequate regulation on the appointment of LEOs and the requirements for special knowledge, experience, training and skill in the employment, retention, deployment and execution[1812] of the functions of LEOs as a specialised group or unit[1813] in the techno-legal conduct of an OCI,[1814] which requires some relevant level of technocracy and professionalism.[1815]

4.3.2 Appointment and specialised skill for the Crime Intelligence of South African Police Service in the conduct of online criminal investigation

Given the almost unending instabilities, controversies and political interferences that have plagued the CI-SAPS for some time,[1816] the provision that the National Commissioner of SAPS

[1810] Police Executive Research Forum *Cameras* 114-115.
[1811] Police Executive Research Forum *Cameras* 117-118.
[1812] Reference can be made to the call for mediators to be trained theoretically and practically and swear to domestic and international ethical codes as professionals in the RSA as other professions do, Marnewick C *Mediation practice in the Magistrates' Courts* (2015) 139-149 (Marnewick *Mediation in the Magistrates' Courts*).
[1813] Section 195(5) of the Constitution stipulates that different or special legislation may be enacted to address the needs of 'different sectors, administration or institutions.
[1814] Applicants Affidavit in *AmaBhungane v Minister of Justice* supra 175.3. In preparation for the implementation of cyber capacity to ensure the protection of critical information infrastructure for government in CCB B6-2017, judicial officers and prosecutors only are expressly mentioned to participate in the training in this regard. In other words, LEOs and other organs of state and entities involved in the conduct of OCI are excluded from the training in this regard which would have generally added to the knowledge of LEOs and other relevant stakeholders in generally understanding the online investigation, see para 86 of the Memorandum on the Objects of the CCB B6-2017. In the U.S., specialised training is required of every investigator according to the field of specialisation, see CIA 'Training in investigative techniques' https://www.cia.gov/library/readingroom/docs/CIA-RDP57-00012A000200090081-3.pdf (Date of use: 11 September 2016).
[1815] South African Police Service *Annual report* 2017/2018 at 184; Para 5.3.3.1 of Chapter 5 of this study.
[1816] See Privacy International https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa (Date of use: 25 April 2019); Letsoalo M 'Spooks' cash 'used to spy on Cyril Ramaphosa'' https://mg.co.za/article/2017-09-08-00-secret-funds-used-to-spy-on-cyril (Date of use: 8 September 2017 (Letsoalo https://mg.co.za/article/2017-09-08-00-secret-funds-used-to-spy-on-cyril (Date of use: 8 September 2017); Mashego A and Masondo S 'Secret plot to oust Mbaks' https://www.news24.com/SouthAfrica/News/secret-plot-to-oust-mbaks-20170827-2 (Date of use: 30 August 2017) (Mashego and Masondo https://www.news24.com/SouthAfrica/News/secret-plot-to-oust-mbaks-20170827-2 (Date of use: 30 August 2017); Serrao A 'Senior crime intelligence officials without top secret clearance' https://www.news24.com/SouthAfrica/News/senior-crime-intelligence-officials-without-top-secret-clearance-20171130 (Date of use: 1 December 2017 (Serrao https://www.news24.com/SouthAfrica/News/senior-crime-intelligence-officials-without-top-secret-

appoints the head of CI-SAPS without any National Assembly approval[1817] is inadequate.[1818] The inadequacy is traceable to the lack of provision for the application of the principles of separation of powers and checks and balances, which should have been included in the provision to ensure the sanctity of the appointment of an independent, competent and impartial head to oversee the conduct of an OCI.

Between 2011-2018,[1819] the leadership of CI-SAPS was in disarray because of the rancour, instability, favouritism, nepotism and victimisation that bedevilled the organisation, resulting in it being steered by 12 acting heads within five years of the seven years under review.[1820]

The appointment in 2018 of the first permanent national head of CI-SAPS within five years in 2018 has not been made without some controversies arising from the inadequacy in appointing the CI-SAPS. It was alleged that the National Commissioner of Police —being the sole appointing authority— requested that the four pending internal petitions against the candidate

---

clearance-20171130 (Date of use: 1 December 2017). In the U.S., some service providers never comply with court orders while some delay in complying with court orders, with considerable effort and expense, Caproni *Lawful electronic surveillance* 205 and 213. In the U.S., it has been opined that 'The problem with online law enforcement is not the need for new law or for government to ''do more'' Government should get better at carrying out its existing responsibilities', see The Economist *Online privacy* 362; In Italy, monetary motivation –such as bribes and blackmail influenced the massive collection of the online dossiers of politicians, financiers, business people, bankers, journalists and judges, see Landau *Lawful electronic surveillance in the face of new technologies* 220.

[1817] Sections 6, 7, 11(2)(d), 27 and 28 of SAPSA; Goko C 'Crime intelligence boss Ngcobo on special leave, credentials probed' http://www.bdlive.co.za/national/2013/10/22/crime-intelligence-boss-ngcobo-on-special-leave-credentials-probed (Date of use: 18 January 2014) (Goko http://www.bdlive.co.za/national/2013/10/22/crime-intelligence-boss-ngcobo-on-special-leave-credentials-probed (Date of use: 18 January 2014). Section 207(1) of the 1996 Constitution; *National Directorate of Public Prosecution and others* v *Freedom under Law* Case No. 67/2014 http://www.saflii.org/cgi-bin/disp.pl?file=za/cases/ZASCA/2014/58.html&query=supremecourtdecisiononrichardmdluli (Date of use: 20 April 2014). Section 7(1) and (2) of SAPSA; Gould C 'On the record-Sindiswa Chikunga, Chairperson of the Parliamentary Portfolio Committee on Police' 2012 40 *SACQ* 39 at 41 (Gould 2012 40 *SACQ*). Arguably, the phrase 'fit and proper person' is a broad, vague and fluid phrase that covers everything in the legal profession.

[1818] The former CI-SAPS head was accused of employing family members at the CI-SAPS as paid police officers and also mismanaging the slush fund, see Mitchley A 'Crime Intelligence boss position up for grabs https://www.news24.com/SouthAfrica/News/crime-intelligence-boss-position-up-for-grabs-20180117 16 November 2018 (Mitchley https://www.news24.com/SouthAfrica/News/crime-intelligence-boss-position-up-for-grabs-20180117 (Date of use: 16 November 2018).

[1819] Naidoo S 'SAPS should boost its crime intelligence division: ISS' http://www.sabcnews.com/sabcnews/saps-boost-crime-intelligence-division-iss/ (Date of use: 18 March 2018 (Naidoo http://www.sabcnews.com/sabcnews/saps-boost-crime-intelligence-division-iss/ (Date of use: 18 March 2018); South African Police Service *Annual Report* 2017/2018 at 207.

[1820] Shange N 'New crime intelligence boss is squeaky clean…his bosses say' https://www.timeslive.co.za/news/south-africa/2018-03-29-new-crime-intelligence-boss-is-squeaky-clean-his-bosses-say/(Date of use: 12 June 2018) (Shange https://www.timeslive.co.za/news/south-africa/2018-03-29-new-crime-intelligence-boss-is-squeaky-clean-his-bosses-say/(Date of use: 12 June 2018))

appointed as the head of CI-SAPS be withdrawn to pave way for a clean slate in the appointment of the head of CI-SAPS in 2018.[1821]

Drawing on a recent giant, transparent and unprecedented step taken in the appointment of the National Director of Public Prosecution in 2018 by the President of the RSA,[1822] the appointment process of the CI-SAPs is inadequate. In the appointment of the National Director of Public Prosecution, the President constituted a Selection Committee headed by a minister in the Presidency with representatives from the public and bar as members to recommend to him the most suitable candidate for the position of National Director of Public Prosecution.[1823] The President took the giant stride although no law or policy was compelling for the President to establish a selection panel in government or National Assembly for this purpose.

However, despite the discretionary appointment of a panel by the President of the RSA, Right2Know Campaign ('R2K') —a non-governmental organisation— was dissatisfied with the independence of the head of the panel and non-public broadcast of the proceedings, given the public interest in and sensitive nature of the function of the office.[1824] As a result, R2K only secured a court order to compel the selection panel to allow live broadcast of the interviews.[1825]

It is important to note that the step taken by R2K was meant to demonstrate absolute transparency in the appointment process of the National Director of Public Prosecution since there was no absolute separation of powers and checks and balances between the President and the minister in the Presidency who presided over the Selection Committee of the National Director of Public Prosecution.

[1821] Shange https://www.timeslive.co.za/news/south-africa/2018-03-29-new-crime-intelligence-boss-is-squeaky-clean-his-bosses-say/(Date of use: 12 June 2018); Mailovich C and Shange N 'Anthony Jacobs first new permanent head of crime intelligence in seven years' https://www.businesslive.co.za/bd/national/2018-03-29-anthony-jacobs-first-new-permanent-head-of-crime-intelligence-in-seven-years/ (Date of use: 7 November 2018). As at the submission of this thesis, no legal action in any form in court or any commission of inquiry has been reported in this regard.

[1822] It is also known as the National Prosecuting Authority ('NPA').

[1823] Ngqakamba S 'New NPA boss: Advisory panel veers away from the usual appointment process' https://www.news24.com/SouthAfrica/News/new-npa-boss-selection-panel-met-for-first-time-set-time-frame-20181022 (Date of use: 16 November 2018).

[1824] Merten M 'Glynnis Breytenbach: Decision to withdraw from 'dream job' made easier due to other competent candidates' https://www.dailymaverick.co.za/article/2018-11-14-glynnis-breytenbach- decision-to-withdraw-from-dream-job-made-easier-due-to-other-competent-candidates/ (Date of use: 16 November 2018 (Merten https://www.dailymaverick.co.za/article/2018-11-14-glynnis-breytenbach- decision-to-withdraw-from-dream-job-made-easier-due-to-other-competent-candidates/ (Date of use:16 November 2018).

[1825] Merten https://www.dailymaverick.co.za/article/2018-11-14-glynnis-breytenbach- decision-to-withdraw-from-dream-job-made-easier-due-to-other-competent-candidates/ (Date of use: 16 November 2018).

The absence of the application of the principles of separation of powers and checks and balances adversely impacts on the vetting and appointment processes and practices of the CI-SAPS.[1826] Despite the requirement that the head of CI-SAPS[1827] must be a 'fit and proper person',[1828] this study reveals that a former acting head of CI-SAPS did not only fail to possess the required top-secret security clearance for some time while he was in office, but it was also alleged that he had a criminal record, which was questioned by the National Assembly Standing Committee on Police.[1829]

Generally, it was also reported that in some cases, senior officials of CI-SAPS falsify security clearance certificates.[1830] Thus, it is submitted that it is unlikely that the labour turn-over of the head of CI-SAPS would have been so high if the appointment provision had, in the first place, incorporated the principles of separation of powers and checks and balances in the employment process of the head of CI-SAPS.

Unlike one of the requirements for members of the SSA[1831] who are expected to secure a security clearance at pre and post-employment stages because of the sensitive nature of the conduct of intelligence, more particularly in the conduct of an OCI,[1832] the general members of CI-SAPS[1833] are not statutorily required to undergo or pass a general 'fit and proper person' test in the SAPSA save as required by the Children's Act.[1834]

[1826] Cowan K and Wa Afrika M 'Head of SAPS crime intelligence still has no security clearance' https://www.timeslive.co.za/politics/2017-07-23-head-of-saps-crime-intelligence-still-has-no-security-clearance/_21 August 2017(Cowan and Wa Afrika https://www.timeslive.co.za/politics/2017-07-23-head-of-saps-crime-intelligence-still-has-no-security-clearance/ (Date of use: 21 August 2017).

[1827] See the Glossary of Terminology.

[1828] SAPS Civilian Secretariat for Police at 30 http://www.policesecretariat.gov.za/downloads/green_paper_policing.pdf accessed (Date of use:18 September 2013; Faull A 'Oversight Agencies in South Africa and the Challenge of Police Corruption' *ISS* Paper 227 Nov. 2011 at 10 http://www.issafrica.org/uploads/Paper227.pdf (Date of use: 17 July 2013) (Faull *ISS* Paper 227); Section 34 of SAPSA.

[1829] Cowan and Wa Afrika https://www.timeslive.co.za/politics/2017-07-23-head-of-saps-crime-intelligence-still-has-no-security-clearance/ (Date of use: 21 August 2017).

[1830] ANA Reporter 'Peter Jacobs appointed new SAPS crime intelligence boss' https://www.iol.co.za/news/south-africa/western-cape/peter-jacobs-appointed-new-saps-crime-intelligence-boss-14152684 (Date of use:12 June 2018).

[1831] This is one of the LEAs recognised to conduct OCI in the RSA.

[1832] Sections 39, 40 and 43 of GILAA *II* and ss 27, 28(1) and 31 of ISA No. 65 of 2002; Paras 2.2, 2.3 and 2.5 - 2.11 of Chapter 2 of this study.

[1833] See the power of the head of CI-SAPS in the definition of 'applicant' in section 1 of RICA.

[1834] See Chapter 7, Part 2of Children's Act 38 of 2005. Other statutes include National Sex Offenders Register [section 42 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (Act 32 of 2007)].

In addition, the appointment process of the members of the CI-SAPS does not require the authorities to undergo a procedure that considers the application of the principles of separation of powers and checks and balances. Given the various sagas that occurred at CI-SAPS between 2011-2018,[1835] the statutory provisions for the appointment of CI-SAPS staff members are inadequate to ensure the effective and efficient conduct of an OCI and protect the right to the SOC because the independence of the appointing authority may not be guaranteed where all powers in this regard lie in one authority, which is the executive. Therefore, there is a need to sanitise CI-SAPS due to the bad state of affairs in the last seven years.[1836]

Moving to the requirement for the academic qualification, the head of CI-SAPS, who oversees the CI-SAPS, is not statutorily or strictly required to be an expert in the conduct or administration of OCI,[1837] given that there are other effective methods of covert investigation and electronic surveillance, which are also unique and important such that the head may be an expert in. It could be argued that statutorily requiring the head to have expert skill in the conduct of an OCI may as well be required in other methods of investigation for the head, which would be difficult to achieve for an officeholder to be a jack of all trades.

However, considering the techno-legal complex and delicate nature and overall effectiveness of the conduct of an OCI,[1838] the law, policy, tradition or norm should stipulate, amongst other requirements, that the head of CI-SAPS be relatively and formally competent[1839] in overseeing

---

[1835] Naidoo S 'SAPS should boost its crime intelligence division: ISS' http://www.sabcnews.com/sabcnews/saps-boost-crime-intelligence-division-iss/ (Date of use: 18 March 2018) (Naidoo http://www.sabcnews.com/sabcnews/saps-boost-crime-intelligence-division-iss/ (Date of use:18 March, 2018); South African Police Service *Annual Report* 2017/2018 at 207.

[1836] Naidoo http://www.sabcnews.com/sabcnews/saps-boost-crime-intelligence-division-iss/ (Date of use: 18 March 2018); South African Police Service *Annual report* 2017/2018 at 207.

[1837] For example, relying on the advert placement for the position of 'Crime Intelligence (Pretoria) REFERENCES: Post No 18/01/3027(1 post), no stipulation of academic or skill acquisition requirement, see file:///I:/LI-SA-%20CI-SAPS%20-%20ADVERT%20FOR%20CRIME%20INTELLIGENCE%20-%20CI%203027.pdf. This is opposed to the requirement of specific academic or skill competence of the knowledge of Serious Organised Crime Investigation at the Directorate of Priority Crime Investigation available at file:///I:/LI-SA-%20SAPS-%20ADVERT%20PLACEMENT%20FOR%20SECTION%20HEAD%20OF%20SERIOUS%20ORGANISED%20CRIME%20INVESTIGATION%20NORTH%20WEST%20-2018%20DPSI%20SMS%2011%202018.pdf (Date of use:16 November 2018).

[1838] Paras 2.2, 2.3 and 2.5 - 2.11 of Chapter 2 of this study.

[1839] Mbhele Z 'Professionalise the police and start with its leaders' https://www.news24.com/Columnists/GuestColumn/professionalise-the-police-and-start-with-its-leaders-20190328 (Date of use: 31 March 2019) (Mbhele https://www.news24.com/Columnists/GuestColumn/professionalise-the-police-and-start-with-its-leaders-20190328 (Date of use: 31 March 2019).

the affairs of the conduct of an OCI, requiring the possession of an NQF certification in this regard.[1840]

In the 2018 appointment of the permanent national head of CI-SAPS, it does seem that the successful candidate met the academic qualifications, going by the commendation by the Minister of Police,[1841] though the qualifications were not specified nor published for public scrutiny. The competency requirement for the head of CI-SAPS should be implemented in a progressive manner such that in the very nearest future, a certified qualification -above a matric certificate- in the conduct of an OCI, amongst others, for the position of the head of CI-SAPS should be a condition *sine qua non* for the position.

Also, in a 2018 advert for two Crime Intelligence posts, an NQF Level 6 —which is an equivalent of a degree— was required,[1842] which is relatively adequate because the requirement does not specify the possession of any special skill in the administration or conduct of an OCI.

However, in one of the previous appointments of the provincial head of CI-SAPS made, it was faulty and outrageous. In the advert placement for the position, the police union and public raised some questions on the justification for lowering the requirements for the position from a degree according to the National Instruction 4\2010 to a matric qualification.[1843]

Although condonation may be considered in the intervening period with regards to the failure of possessing a certified qualification in the conduct of an OCI by the head of CI-SAPS at the provincial level, however, lowering the educational qualification to a matric qualification, without any other higher qualification, is grossly inadequate. This inadequacy tends to lower the ethical and professional competence required for the conduct of an OCI, thus compromises the effective and efficient conduct of an OCI and the right to the SOC.

[1840] Para 4.6 of this chapter.

[1841] PMG 'Minister of Police on SAPS and IPID policy; SAPS & IPID 2018/19 Annual Performance, with Minister and Deputy' https://pmg.org.za/committee-meeting/26410/ (Date of use: 12 July 2018).

[1842] South African Qualification Authority Act 58 of 1995('SAQA'); SAPS 'Location: Crime Intelligence (Pretoria): References: CI 07/07/2018' file:///C:/Users/Microlab/Downloads/CI%203027.pdf (Date of use: 17 September 2018).

[1843] Solidarity 'Matric only requirement for position as provincial head of crime intelligence' https://solidariteit.co.za/en/matric-only-requirement-for-position-as-provincial-head-of-crime-intelligence/ (Date of use: 19 June 2016); Shange https://www.timeslive.co.za/news/south-africa/2018-03-29-new-crime-intelligence-boss-is-squeaky-clean-his-bosses-say/(Date of use: 12 June 2018); Mailovich and Shange https://www.businesslive.co.za/bd/national/2018-03-29-anthony-jacobs-first-new-permanent-head-of-crime-intelligence-in-seven-years/ (Date of use: 7 November 2018).

In the training of the members of CI-SAPS, the National Commissioner —who is a political appointee and who may not be a career police officer because the law does not provide that the position be occupied by a career police officer— establishes and maintains training institutions for members of SAPS, which arguably include members of CI-SAPS.[1844]

Although the National Commissioner determines the training programmes,[1845] it is submitted that this provision is inadequate because the National Commissioner may not be in the best position to determine the adequacy of the training programme, especially where the commissioner is not a career police officer. However, the programme is regulated by the SAQA[1846] which provides a check and balance mechanism in this regard.

The training programme for members of SAPS comprises one-year basic training and tactical policing and compulsory one-year post-basic practical training in uniform as a constable at a police station[1847] under the supervision of the FTO.[1848] Any member who fails to complete the basic compulsory training within two years of appointment is discharged from the service,[1849] however, a second chance is given to deserving candidates who do not pass in the first instance.[1850] These provisions promote competent general policing competence in the performance of domestic and international law duty,[1851] which duty arguably should include the conduct of an OCI at both domestic and international levels.

Additionally, it is worrisome to note that the 24-month training period was reduced to 8 months

[1844] Sections 11(2)(e) and 32 of SAPSA. Section 180 (a) and (c) of the Constitution makes provision for training programmes for judicial officers and the participation of non-judicial officers in the administration of justice.
[1845] Sections 11(2)(e) and 32 of SAPSA. Section 180 (a) and (c) of the Constitution makes provision for training programmes for judicial officers and the participation of non-judicial officers in the administration of justice.
[1846] SAQA; Montesh M *A Critical analysis of crime investigative system within the South African criminal justice system: A comparative study* (PhD thesis Unisa 2007) 14 (Montesh *Crime investigative system*); SAPS 'New class of police officers' https://www.saps.gov.za/careers/downloads/new_class_police_officer.pdf (Date of use: 16 November 2018).
[1847] SAPS 'Careers in SAPS' https://www.saps.gov.za/careers/downloads/saps_career_booklet_part1.pdf at 5 (Date of use: 16 November 2018) (SAPS https://www.saps.gov.za/careers/downloads/saps_career_booklet_part1.pdf at 5 (Date of use: 16 November 2018).
[1848] Montesh *Crime investigative system* 14; In the U.S., all police officers are expected to undergo some training in the First and Fourth Amendment training before embarking on the use of the electronic systems, Police Executive Research Forum *Cameras* 110.
[1849] Section 37 of SAPSA; Relying on art 15(4) of UN Office on Drugs & Crime *Model Legislative Provision Against Organised Crime* 2012 which requires that infiltrators should be specially trained and designated, similar principle is necessary for all categories of LEAs conducting OCI.
[1850] SAPS https://www.saps.gov.za/careers/downloads/saps_career_booklet_part1.pdf at 5 (Date of use: 16 November 2018).
[1851] *Kaunda v President* supra 273 (*Kaunda*); Section 199(5) of the Constitution.

in Durban for operational expediency.[1852] It is submitted that where the adequate basic training programme is not conducted to lay the foundation for policing and investigation, it ultimately creates a vacuum in conducting a specialised and advance training such as OCI training.

The duration of the post-basic training for members of SAPS in the specialised area of Communication Interception Official is uncertain.[1853] In one of the reports by the National Assembly, queries were raised on the shortage, length and standard of training required for cybercrime investigation,[1854] which is a concern in this regard. However, in the Memorandum of the proposed Cybercrime and Cybersecurity Bill ('CCB') which is replaced by the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, provision is made for the implementation of training programmes for SAPS officials only on the detection, prevention and investigation of offences which have some cybercrime elements.[1855] Again, the duration of the training in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 is not stipulated.

However, it is expected that this project will be extended to members of the CI-SAPS who will be exposed to an aspect of the curriculum on OCI since the conduct of an OCI is not limited to the investigation of offences committed online. This expectation is in pursuance of the advice of the Minister of Police who said that training of CI-SAPS members should be conducted continuously.[1856] Towards this end, the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 provides that the Minister of Police must, on an annual basis, report to the National Assembly on the number of SAPS members who have undergone training on the investigation of cybercrimes.[1857]

[1852] Maphumulo S 'Police training reduced to 8 months' https://www.iol.co.za/news/police-training-reduced-to-8-months-2012636 (Date of use: 16 November 2018).

[1853] SAPS https://www.saps.gov.za/careers/downloads/saps_career_booklet_part1.pdf at 5 (Date of use: 16 November 2018).

[1854] Parliamentary Monitoring Group 'SAPS Crime Intelligence; SAPS Specialised Training' https://pmg.org.za/committee-meeting/14743/ (Date of use: 12 June 2016). It does seem that there is general apathy to training in SAPS.

[1855] Section 54(2)(a)(ii) & (iii) & (c)(iii) of the CCB B6-2017, which is replaced with sections 55(1)(b) &(c) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017; Para 87 of the Memorandum on the Objects of the CCB B6-2017, which is not provided in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

[1856] Harper P 'Cele takes aim at crime intelligence' https://mg.co.za/article/2018-03-02-00-cele-takes-aim-at-crime-intelligence (Date of use: 19 June 2018) (Harper https://mg.co.za/article/2018-03-02-00-cele-takes-aim-at-crime-intelligence (Date of use: 19 June 2018).

[1857] Section 54(2)(c)(iii) of the CCB B6-2017, which is replaced by section 55(3)(c) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

Despite its drive for mass recruitment of crime intelligence officials, the SAPS —including CI-SAPS— encounter the challenge of attracting adequate human resources within SAPS since the available applicants lack necessary detective skills,[1858] including skills in the conduct of an OCI.[1859]

However, should the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 be enacted as law in the current text that it is, it will mandate the Minister of Police to compel members of the SAPS to undergo basic training in 'detection, prevention, and investigation' of cybercrimes[1860] through the cooperation of accredited higher learning institutions.[1861]

Finally, despite the high-level significant complexity involved in the techno-legal aspects of conducting an OCI in online communication in contemporary society and the provisions of RICA, there is no specific, published, and complementary legal framework —including advert placement, decision or policy— that requires the head[1862] and members of CI-SAPS[1863] in charge of the conduct of OCI to be specialists or have some level of competence in the field of OCI as part of the requirements for the relevant positions.[1864]

Hence, the pending the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 makes provision for the recruitment of external experts to assist the CI-SAPS in conducting an

---

[1858] Bruce D 'New blood - Implications of e*n-masse* recruitment for the South African Police Service' 2013 43 *SACQ* 17 at 18-25; Joint Standing Committee on Intelligence at para 4.9 http://www.pmg.org.za/docs/2011/comreports/110921jcintelligencereport.htm (Date of use: 13 October 2013). It was reported in June, 2013 that the SAPS had twenty one thousand, five hundred and thirteen (21, 513) fully trained detectives in SAPS, see Parliamentary Monitoring Group 'Question 855 of 2013/17B Parliamentary Monitoring Group question posed to the Minister of Police' http://www.pmg.org.za/node/36638 (Date of use: 12 December 2013) (Parliamentary Monitoring Group http://www.pmg.org.za/node/36638 (Date of use: 12 December 2013). However, the CI-SAPS unit of SAPS remains understaffed, see SAPS Civilian Secretariat for Police at 32 http://www.policesecretariat.gov.za/downloads/green_paper_policing.pdf (Date of use: 18 September 2013); South African Police Service 'Strategic plan 2010-2014' at 9 and 16 http://www.saps.gov.za/about/stratframework/strategic_plan/2010_2014/strategic_plan_2010_2014.pdf (Date of use: 6 June 2013), South African Police Service '*Annual Report 2012/13'* at 142 at http://www.saps.gov.za/about/stratframework/annualreports.php (Date of use: 6 June 2013).

[1859] Sutherland E 'Governance of cybersecurity - The case of South Africa' *AJIC* Issue 20 (2017) 85.

[1860] Section 54(2)(a)(ii) of the CCB B6-2017, which is replaced with section 55(1)(b) of the Cybercrime Bill 2018 –Amendments Proposed to Bill B6-2017**.**

[1861] Section 54(2)(a)(iii) of the CCB B6-2017, which is replaced with section 55(1)(c) of the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017.

[1862] Mbhele https://www.news24.com/Columnists/GuestColumn/professionalise-the-police-and-start-with-its-leaders-20190328 (Date of use: 31 March 2019).

[1863] Crime Intelligence of the South African Police Service.

[1864] SAPS 'Location: Crime Intelligence (Pretoria): References: CI 07/07/2018' file:///C:/Users/Microlab/Downloads/CI%203027.pdf (Date of use: 17 September 2018).

investigation,[1865] which should include an OCI,[1866] though the chapter on investigation generally deals with both OCI and non-OCI forms of investigation.[1867]

4.3.3 Appointment and specialised skill for the Directorate of Priority Crime Investigation in the conduct of online criminal investigation

The head of the DPCI or HAWKS is appointed by the Minister of Police in agreement with the national cabinet for a non-renewable fixed term of between seven to ten years which must be determined at the time of appointment.[1868] Although the involvement of cabinet in this process, to a narrow extent, shows some level of consultation, however, there would have been adequate consultation if National Assembly was consulted before the appointment, instead of the post-appointment report submitted by the Minister of Police to the National Assembly.[1869]

The fact that the Minister of Police reports to the National Assembly only after the appointment of the head of HAWKS[1870] is substantively and procedurally defective and peremptory of the outcome of the National Assembly proceeding whose role in the process becomes insignificant because it becomes an act of *fait accompli*. This is because the National Assembly would have been denied the opportunity of contributing to the debate in the appointment process.[1871] The reporting process by the Minister of Police is only informative.

This procedure creates doubt in the institutional, structural and operational independence, credibility and accountability in the recruitment mechanism of the head of HAWKS[1872]

[1865] See ss 27(3), 31(4), 32, 33(1), 34) (1), 35(1)-(4) and 37(1) & (3) of the CCB B6-2017 where these provisions impliedly allow non-permanent employees officers of the various LEAs to be hired and accompany LEOs to conduct an investigation. These provisions are replaced by sections 29(3), 33(4), 34, 35(1), 36(1) (a) &(b), 37(1)-(4) and 39(1) & (3) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

[1866] Section 38(1) of the CCB B6-2017, which is replaced by section 40(1) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

[1867] See Chapter 5 of CCB B6-2017, which is replaced by Chapter 5 of the Cybercrime Bill 2018 - Amendments Proposed to Bill B6-2017.

[1868] Section 17CA (1) (b) and (2) of SAPSA.

[1869] Sections 17CA (3) and 17K (9) of SAPSA.

[1870] Sections 17CA (1), (2) and (3) and 17K (9) of SAPSA.

[1871] Previous confirmation of appointments in some cases by Parliament has shown the abuse of dominance by the ruling party (African National Congress 'ANC') to veto some candidates for public offices with unquestionable character. The opposition contends the unjustifiable endorsement of candidates whose integrity is in question; *DA v President* supra 24.

[1872] Politics Webs 'W Cape High Court rules Hawks Act Unconstitutional- HSF Helen Suzman Foundation' http://www.politicsweb.co.za/politicsweb/view/politicsweb/en/page71654?oid=480785&sn=Detail&pid=71616 (Date of use: 20 February 2014); Hoffman P 'Hawks in SAPS are neither Effective nor Sufficiently Independent' http://www.ifaisa.org/Hawks_neither_effective_nor_sufficiently_independent.html (Date of

including the management of the affairs of the LEOs in conducting an OCI since the administration of an OCI under the HAWKS is like the general administration of any other unit in HAWKS.

In the management of the affairs of the HAWKS, the power of the head of HAWKS may be weakened by the fact that the Minister of Police has the power to provisionally suspend the incumbent, though a dismissal must be approved by a two-third vote of the National Assembly.[1873] However, in *Suzman Foundation v Min of Police*,[1874] the court declared that the Minister of Police did not have the power to suspend the head of HAWKS, neither did he have the power to appoint an acting head of HAWKS.

In the appointment of the head[1875] and members of HAWKS, there is no statutory, regulatory, professional or advert recruitment or retention requirement of knowledge and skill to conduct an OCI, neither is there any provision for focused training for the head and members of the HAWKS in the complex and delicate conduct of an OCI.[1876] The Constitutional Court in

use: 20 January 2014 (Hoffman http://www.ifaisa.org/Hawks_neither_effective_nor_sufficiently_independent.html (Date of use: 20 January 2014).

[1873] Sections 16(2), 16(2A) and 17D of SAPSA; *SAPS v Zim & Dugard* para 60. Section 17DA of SAPSA. In *The Helen Suzman Foundation v The Minister of Police and Others* HC Case No: 1054/2015 para 66 (*Suzman Foundation v Min of Police*) the court declared the Minister of Police did not have the power to suspend the head of HAWKS, neither did he have power to appoint an acting head of HAWKS; Politics Webs 'W Cape High Court rules Hawks Act Unconstitutional- HSF Helen Suzman Foundation' http://www.politicsweb.co.za/politicsweb/view/politicsweb/en/page71654?oid=480785&sn=Detail&pid=71616 (Date of use: 20 February 2014); Hoffman http://www.ifaisa.org/Hawks_neither_effective_nor_sufficiently_independent.html (Date of use: 20 January 2014)

[1874] *Suzman Foundation v Min of Police* paras 90 and 110(e).

[1875] Sections 17CA (1), (2) and (3) and 17K (9) of SAPSA. *DA v President* supra 24. The Times http://news.howzit.msn.com/da-has-police-chief-mcbride-in-its-sights (Date of use: 5 March 2014); In the last advert placement for the position of the head of HAWKS in January 2018, there was no requirement for the knowledge, skill or competence in the conduct of an OCI or information and communication technology, amongst other requirements, see HAWKS 'Vacancy in the Directorate for Priority Crime Investigation (DPCI)' http://www.policesecretariat.gov.za/downloads/posts/VACANCY_THE_DIRECTORATE_FOR%20PRIORITY_CRIME_INVESTIGATION_(DPCI).pdf (Date of use: 3 May 2018).

[1876] Section 16(2)(g) of SAPSA; Politics Webs 'W Cape High Court rules Hawks Act Unconstitutional-HSF Helen Suzman Foundation' http://www.politicsweb.co.za/politicsweb/view/politicsweb/en/page71654?oid=480785&sn=Detail&pid=71616 (Date of use: 20 February 2014); Hoffman http://www.ifaisa.org/Hawks_neither_effective_nor_sufficiently_independent.html (Date of use: 20 January 2014. Shortage of skilled cybercrime investigators exit in Hawks, therefore required training on OCI must be conducted, Pieterse N B 'Electronic Crime Unit: Directorate for Priority Crime Investigation' Workshop for Policy Design towards Digital Security, Cybercrime and Cybercrime Prevention (2015) 65 and 73 (Pieterse 'Electronic Crime Unit: Directorate for Priority Crime Investigation'.

Suzman Foundation v Min of Police logically confirms this.[1877] The court unwittingly exacerbates matters in the requirement of legal qualification or knowledge in the conduct of an OCI by holding that LEOs or special investigators are not required to possess legal qualification or knowledge as investigators.[1878]

This, according to the Court, is because a LEO or special investigator is in the investigative unit which does not deal with legal issues but prosecutors who take decisions that necessarily require some qualifications of law.[1879] Since the apex court held that LEOs and special investigators do not require legal qualifications or knowledge to conduct an offline investigation, it is argued that it is ironically and irrefutably conclusive that the court is positing that requiring LEOs who conduct an OCI to possesses legal qualification or knowledge, as proposed in this chapter,[1880] is unreasonable, irrational, fallacious and unjustifiable. However, this study vehemently contests the position of the Constitutional Court.

The judgment of the apex court convincingly and regrettably explains one of the reasons for the gross incompetence and incapacitation in the general investigation which spills over to the conduct of an OCI which is more complex and delicate to lawfully conduct as displayed in herein. In the High Court case of *State v Naidoo*, despite the possession of two diplomas in Police Management and Business Management by a captain with a ten-year experience with the SAPS and without a legal qualification, the captain gathered information from MTN —one of the telecommunication service providers in the RSA— without obtaining a section 205 of the CPA summons by assuring the MTN employee that they were in the process of obtaining the summons.[1881]

It is obvious that qualifications or skills in other areas other than in the area of the conduct of an OCI cannot be a substitute for a certified training or skill in the conduct of an OCI, thus, it is argued that the illegality of the conduct of an OCI in *State v Naidoo* could have arisen from or contributed to the failure or refusal of the captain to appreciate or comprehend the consequence of his action or omission as a LEO in the conduct of an OCI.

[1877] *Suzman Foundation v Min of Police* para 66.
[1878] *Suzman Foundation v Min of Police* para 66.
[1879] *Suzman Foundation v Min of Police* para 66.
[1880] Para 4.6 of this chapter.
[1881] *State v Naidoo* supra 521 B-E.

However, if the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 was enacted as a law in the current text concerning the provision for training, it would in a way ameliorate the challenges raised immediately above. The Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 stipulates that the Minister of Police must, on an annual basis, report to the National Assembly on the numbers of SAPS members who have undergone training on the investigation of cybercrimes[1882] and non-cybercrimes,[1883] in which an OCI can be conducted. Besides, the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 should be reviewed to recommend that the head of HAWKS should be included in the team of HAWKS employees[1884] that will undergo a training programme in the conduct of an OCI[1885] if same qualification, knowledge or skill has not been acquired by the head.

Since the HAWKS is under the control and management of SAPS, the provision of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 addresses the gap concerning the absence of training provision in the SAPSA, which should be extended to the administration of an OCI, including the annual reporting system on the training of members of HAWKS who are in charge of the conduct of an OCI.

In summary, despite the high level of significant complexity involved in the techno-legal aspects of conducting an OCI[1886] and the provisions of RICA, there is no specific, published, and complementary legal framework —including advert placement, decision or policy— that requires the head and members of HAWKS in charge of the conduct of an OCI to be specialists or have some level of competence in the field of OCI as part of the requirements for the relevant positions.

[1882] Section 54(3)(c)(iii) of the CCB B6-2017, which is replaced by section 55(3)(c) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1883] Section 55 (3)(b)(iii) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[1884] *Helen Suzman Foundation v President of the Republic of South Africa and Others* in: *Glenister v President of the Republic of South Africa and Others* [2014] ZACC 32 para 43 (*Suzman Foundation v President of the RSA* in: *Glenister v President of the RSA*).
[1885] See para 4.3.8 of this Chapter.
[1886] Sections 27(3), 31(4), 32, 33(1), 34) (1), 35(1)-(4) and 37(1) & (3) of the CCB B6-2017, which are replaced by sections 29(3), 33(4), 34, 35(1), 36(1), 37(1)-(4) and 39 (1) & (3) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

4.3.4 Appointment and specialised skill for the Independent Police Investigative Directorate in the conduct of online criminal investigation

The IPIDA requires that the Minister of Police must nominate a candidate for the position of Executive Director of IPID for appointment by the National Assembly Committee on Police which may confirm or reject the nomination.[1887] However, where there is a usurpation by the Minister of Police of the National Assembly powers to appoint the Executive Director of IPID, it constitutes a gross breach of the law.[1888]

Another defect in the IPIDA relates to the risk of absolutely empowering a National Assembly Committee —instead of the National Assembly— to perform this role, which is open to easy political influence, manipulation and abuse by the members of the Committee.[1889] This is opposed to the larger members of the National Assembly, which though may also be influenced by a majority party decision or other forces, but still display some level of openness and checks and balances. This defect is noticeable in the area of a split of a decision on the tenure of office of two terms of five years for the office of the Executive Director of IPID, which may or may not be renewed by the National Assembly Committee on Police.[1890]

In 2019, confirmed reports indicate the irrationality of the majority of the members of the National Assembly Committee on Police on the renewal of appointment of the former

---

[1887] Section 6(1) & (2) of the IPIDA

[1888] Section 6 (1) & (2) of the IPIDA; The Times 'DA has Police Chief McBride in its Sights' http://news.howzit.msn.com/da-has-police-chief-mcbride-in-its-sights (Date of use: 5 March 2014) (The Times http://news.howzit.msn.com/da-has-police-chief-mcbride-in-its-sights (Date of use: 5 March 2014)**;** DA 'Parties Not Happy With McBride Recommendation' http://news.howzit.msn.com/politics/parties-not-happy-with-mcbride-recommendation (Date of use: 15 November 2013) (DA http://news.howzit.msn.com/politics/parties-not-happy-with-mcbride-recommendation (Date of use: 15 November 2013); Parliamentary Monitoring Group 'Question 842 of 2013/17B Parliamentary Monitoring Group question posed to the Minister of Police' http://www.pmg.org.za/node/36638 (Date of use: 12 December 2013); see Sowetan 'Nkandla Committee Dissolved for Now' http://www.sowetanlive.co.za/news/2014/04/29/nkandla-committee-dissolved-for-now accessed 30 April, 2014 (Sowetan http://www.sowetanlive.co.za/news/2014/04/29/nkandla-committee-dissolved-for-now (Date of use: 30 April, 2014); Kohn 2013 130 *SALJ* at 816 and 818; Moseneke D 'Striking a Balance between the Will of the People and the Supremacy of the Constitution' 2012 12 *SALJ* at 17; *National Directorate of Public Prosecution and others* v *Freedom under Law* Case No. 67/2014 http://www.saflii.org/cgi-bin/disp.pl?file=za/cases/ZASCA/2014/58.html&query=supremecourtdecisiononrichardmdluli (Date of use: 20 April 2014).

[1889] Bateman C 'Paul O'Sullivan takes anti-McBride MPs on at their own game' https://www.biznews.com/undictated/2019/04/15/paul-o-sullivan-anti-mcbride-mps (Date of use: 15 April 2019).

[1890] Section 6 (1)-(3) of the IPIDA; De Vos P 'Law allowing for extension of McBride's term of office probably unconstitutional' https://www.dailymaverick.co.za/opinionista/2019-03-05-law-allowing-for-extension-of-mcbrides-term-of-office-probably-unconstitutional/ (Date of use:11 March 2019).

Executive Director of IPID —one Mr. Robert McBride— who was contesting the non-renewal of his appointment in court and supported by *amicus curiae*.[1891] In this case, Mr. McBride contests that the power of the Minister of Police not to renew his appointment was unlawful, citing the principle of checks and balances which should place the appointment in the National Assembly Committee on Police as opposed to the Office of the Minister of Police.

The *amicus curie* submits that for the proper application of the principle of checks and balances, the National Assembly —as opposed to the National Assembly Committee— should have the power to appoint or renew the appointment of the Executive Director. However, it could be argued that to prevent any form of favouritism or nepotism towards the end of the first tenure of an incumbent of the position of Executive Director, non-renewable one term of seven years like that of the OPP is an option for legislative adoption.[1892]

Despite the provision of specific grounds for the removal of the Executive Director of IPID,[1893] the grounds for the suspension of the head of IPID[1894] are not stated.[1895] However, the stated grounds for removal could impliedly be used for the suspension of the Executive Director of IPID.[1896]

[1891] Phakathi B 'Bheki Cele has until Monday to give reasons for not renewing Robert McBride's contract' https://www.businesslive.co.za/bd/national/2019-02-14-bheki-cele-has-until-monday-to-give-reasons-for-not-renewing-robert-mcbrides-contract/ (Date of use: 14 February 2019).

[1892] Section 183 of the Constitution.

[1893] Section 6(6) of the IPIDA.

[1894] The Times http://news.howzit.msn.com/da-has-police-chief-mcbride-in-its-sights (Date of use: 5 March 2014)**;** DA http://news.howzit.msn.com/politics/parties-not-happy-with-mcbride-recommendation (Date of use:15 November 2013). Parliamentary Monitoring Group 'Question 842 of 2013/17B Parliamentary Monitoring Group question posed to the Minister of Police' http://www.pmg.org.za/node/36638 (Date of use:12 December 2013). See Sowetan http://www.sowetanlive.co.za/news/2014/04/29/nkandla-committee-dissolved-for-now (Date of use: 30 April 2014); Kohn 2013 130 *SALJ* 816.

[1895] Section 6 (1) of the IPIDA. The Times http://news.howzit.msn.com/da-has-police-chief-mcbride-in-its-sights (Date of use: 5 March 2014)**;** DA http://news.howzit.msn.com/politics/parties-not-happy-with-mcbride-recommendation (Date of use:15 November 2013); Parliamentary Monitoring Group 'Question 842 of 2013/17B Parliamentary Monitoring Group question posed to the Minister of Police' http://www.pmg.org.za/node/36638 (Date of use: 12 December 2013). See Sowetan http://www.sowetanlive.co.za/news/2014/04/29/nkandla-committee-dissolved-for-now (Date of use: 30 April 2014); Kohn 2013 130 *SALJ* 816. Section 6(4) and (6) of IPIDA. Though a repealed law is of no effect for the future, it is however important to show that the repealed s 51 particularly subsection (4) of SAPSA (prior to the 2011 amendment in IPIDA points out the failure or insincerity on the part of government to address an uncompromising stance on the sufficient independence of LEA particularly the police and its affiliates such as HAWKS and IPID. See repealed chapter 10 of SAPSA containing ss 50-54 which have been deleted. These provisions were operational before the enactment of IPIDA.

[1896] Section 6 (1), (4) and (6) and 20 (4) of IPIDA. The Times http://news.howzit.msn.com/da-has-police-chief-mcbride-in-its-sights (Date of use: 5 March 2014); DA http://news.howzit.msn.com/politics/parties-not-happy-with-mcbride-recommendation (Date of use:15 November 2013; Parliamentary Monitoring Group 'Question 842 of 2013/17B Parliamentary Monitoring Group question posed to the Minister of Police' http://www.pmg.org.za/node/36638 (Date of use: 12 December, 2013. See Sowetan

The sole discretion of the Minister of Police to suspend the head of IPID is contrary to the repealed provision in the SAPSA that regulated the former ICD[1897] which was replaced by IPID. The old section 51 (4) of SAPSA —before the 2011 amendment— enabled the Minister of Police to consult with the relevant National Assembly Committees on the guidelines for the removal of the Executive Director of ICD.[1898]

In the case of *Min of Police v McBride*, the court reiterated the principle of separation of powers by holding that the Minister of Police does not have the power to suspend the Executive Director of IPID without the approval of the National Assembly.[1899] Thus, the exclusion of the principles of separation of powers and checks and balances in the suspension of the Executive Director of IPID in IPIDA exposes the weakness in the independence and integrity of the Executive Director of IPID, including the administration of the conduct of an OCI.

Without prejudice to the right of occupation by the substantive Executive Director of IPID to return to work, the independence of IPID and that of the acting Executive Director is threatened where the latter could be retained in the position for an indefinite period.[1900] The indefinite occupation of the position creates insecurity for the acting Executive Director who is susceptible to the whims and caprices of the unseen forces, influence and interference of powers that be in government and the society during the interim period. These vices may directly or indirectly be extended to the administration of the conduct of an OCI.

---

http://www.sowetanlive.co.za/news/2014/04/29/nkandla-committee-dissolved-for-now (Date of use: 30 April 2014); Kohn 2013 130 *SALJ* 816.

[1897] See repealed chapter 10 of the SAPSA containing sections 50-54 which have been abolished. These provisions were operational before the enactment of the IPIDA.

[1898] Though a repealed law is of no effect for the future, it is however important to show that the repealed section 51 particularly subsection (4) of the SAPSA (prior to the 2011 amendment in the IPIDA) points out the failure or insincerity on the part of government to address an uncompromising stance on the sufficient independence of LEA particularly the police and its affiliates such as HAWKS and IPID.

[1899] Section 6(4) and (6) of the IPIDA. Though a repealed law is of no effect for the future, it is however important to show that the repealed section 51 particularly subsection (4) of SAPSA (prior to the 2011 amendment in IPIDA) points out the failure or insincerity on the part of government to address an uncompromising stance on the sufficient independence of LEA particularly the police and its affiliates such as HAWKS and IPID. See repealed chapter 10 of SAPSA containing sections 50-54 which have been deleted. These provisions were operational before the enactment of IPIDA; *McBride v Minister of Police and Another* [2016] ZACC 30 paras 58 (*McBride v Minister of Police*).

[1900] The provision of section 6(4) should not be misconstrued with section 6(5) of IPIDA. The latter deals with the vacancy of the head of IPID which more than a year must not be whereas the former deals with the indisposition of the head which does not have a definite period. The Minister of Police may keep the acting head for as long as he or she wants without declaring the substantive position vacant even where it is obvious that the substantive head is not returning to the position. Save where there is litigation on the occupation of the post, the position should not be left open for an unreasonable period.

In addition, the use of the word 'when' in describing the condition for the unavailability of the substantive head seems very predictive or probable. This provision may play a negative role in the independence of the acting Executive Director of IPID, thus adversely impacts on the effectiveness and impartiality of the investigators.

On the requirement of special knowledge to conduct an OCI, there is no statutory, regulatory or policy provision or advert placement decision[1901] that requires the Executive Director of the IPID to be a specialist or have specialised knowledge in the conduct of an OCI in the recruitment or retention process for this position.

Concerning the members of IPID, provision is made for the appointment of an investigator who must have the knowledge and relevant experience in criminal investigations or any other relevant experience,[1902] be a 'fit and proper person'[1903] and secure relevant security clearance for the job as and when required,[1904] without which there is disengagement from service based on this condition.[1905] These provisions are relatively adequate in the areas of fitness and security clearance of members of IPID because the provisions address the various principles highlighted in this chapter.[1906]

However, although members of IPID are required to have some knowledge of criminal investigations and that the Executive Director of IPID provides guidelines for the general training of members of IPID,[1907] there is no specific statutory, regulatory or professional knowledge and skill requirement for the recruitment or retention for members to conduct an

[1901] Though no advert was placed as at the time of submitting this thesis for the vacated office of the Executive Director of IPID in March 2019, the advert for the position of the provincial head of IPID requires thorough knowledge of criminal and procedural law, law of evidence, investigative systems, and human rights law but the advert does not include the knowledge of the conduct of OCI or information and communication technology, and law, see IPID 'POST 16/28:PROVINCIAL HEAD REF NO: Q9/2019/1' file:///F:/LI-SA-%20ART-%20IPID%20-%20ADVERT%20FOR%20PROVINCIAL%20HEAD%20OF%20IPID%20-%202019.pdf (Date of use: 21 May 2019) (IPID file:///F:/LI-SA-%20ART-%20IPID%20-%20ADVERT%20FOR%20PROVINCIAL%20HEAD%20OF%20IPID%20-%202019.pdf (Date of use:21 May 2019).

[1902] Section 22 (2) of the IPIDA.

[1903] Section 22(1) of the IPIDA. The Times http://news.howzit.msn.com/da-has-police-chief-mcbride-in-its-sights (Date of use: 4 March 2016).

[1904] Section 22(6) of the IPIDA.

[1905] Section 22 (3), (4), (5), (6) of the IPIDA.

[1906] See para 4.1 of this Chapter.

[1907] Section 7(3)(e)(iii) of the IPIDA. It would have been better if the Parliamentary Committee on Police Affairs had some supervisory role in drawing up the training guidelines.

OCI.[1908] Furthermore, drawing on the criticism levelled against the National Commissioner of SAPS —who may not be a career police officer— for determining the training programmes for members of CI-SAPS,[1909] the same opinion is held against the Executive Director of IPID — who may not be a career police officer— for providing guidelines for the general training of members of IPID.

In summary, despite the high level of significance and complexity involved in the techno-legal aspects of conducting an OCI in contemporary society[1910] and the provisions of RICA, there is no specific, published, and the complementary legal framework —including advert placement, decision or policy— that that requires the head and members of IPID in charge of the conduct of an OCI to be specialists or have some level of competence in the field of OCI as part of the requirements for the relevant positions.

4.3.5 Appointment and specialised skill for the State Security Agency in the conduct of online criminal investigation

The President of the RSA solely appoints the Director-General of the SSA who is the accounting officer of SSA,[1911] which is the civilian intelligence agency of the government of the RSA.[1912] The unilateral appointment of the Director-General fails to consider the exercise of the doctrine of separation of powers and principle of checks and balances by the National Assembly. Similarly, the aforementioned principles are also absent in the appointment of the two heads of the ID-SSA in charge of the domestic and foreign divisions respectively who are solely appointed by the Minister of State Security without any recommendation from the

[1908] IPID file:///F:/LI-SA-%20ART-%20IPID%20-%20ADVERT%20FOR%20PROVINCIAL%20HEAD%20OF%20IPID%20-%202019.pdf (Date of use: 21 May 2019).

[1909] See para 4.3.2 of this Chapter.

[1910] See sections 27(3), 31(4), 32, 33(1), 34) (1), 35(1)-(4) and 37(1) &(3) of CCB B6-2017, which are replaced by sections 29(3), 33(4), 34, 35(1), 36(1), 37(1)-(4) and 39 (1) &(3) of the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017.

[1911] Sections 15(D) of the GILAA *II* and 3 of the ISA. Hartley http://www.bdlive.co.za/national/2013/08/08/single-intelligence-body-wields-great-power (Date of use: 28 February 2014).

[1912] Privacy International https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa (Date of use: 25 April 2019).

National Assembly.[1913] These provisions may not guarantee an independent and impartial institutional and structural platform to conduct an OCI.

The independence of the Director-General as the functional and operational head of SSA is eroded by the Minister of State Security who solely creates posts and determines functions in the SSA. However, the Minister of State Security in consultation with the President of the RSA creates the position of Deputy Director-General which is equivalent to the same position in the public service.[1914] The absence of the supervisory role of the National Assembly in the process of creation of top positions and the prescription of functions for the top posts arguably and ultimately undermines the doctrine of separation of powers and principle of checks and balances, given the sensitive and significant role of SSA in State and national security which may be undermined by personal, selfish or political reasons or manoeuvring of or by the authorities concerned which may not be obvious to the public.

However, it may be argued in some quarters that the involvement of the National Assembly in the process of creating some posts in the SSA is tantamount to micro-managing the affairs of SSA or that National Assembly will be usurping the powers of the Executive. Nevertheless, it is submitted that —without casting any aspersion on any authority— the suggestion for checks and balances seems to be adequate and proactive to guard against any form of abuse of power by the appointing authorities.

Although the Director-General has the power to command and control the SSA,[1915] the power is whittled down by the provision of section 22 of the GILAA because the power is subject to the direction of the Minister of State Security.[1916] It is also whittled down because the Director-General has to obtain approval from the Minister of State Security in terms of the issuance of directions on the conditions of service and human resources for SSA and any other matter necessary for the efficient command and control of SSA,[1917] which includes directions on

---

[1913] Sections 20 of the GILAA *II* and 8(1)(a) of the ISA and Hartley http://www.bdlive.co.za/national/2013/08/08/single-intelligence-body-wields-great-power (Date of use: 28 February 2014).

[1914] Sections 16 of the GILAA *II* and section 4(1)(a) and (2) of the ISA.

[1915] Sections 15(D) of the GILAA *II* and 3 of the ISA. Hartley http://www.bdlive.co.za/national/2013/08/08/single-intelligence-body-wields-great-power (Date of use: 28 February 2014).

[1916] Section 22 of the GILAA *II*.

[1917] The Director-General issues directive on the conditions of service and human resources which are submitted for consideration to the Intelligence Council on Conditions of Service (ICCS), in which the Minister of State

communication and computer security.[1918] However, it is submitted that the approval of such conditions from the National Assembly would have been appropriate to ensure the observance of the principles of separation of powers and checks and balances.

In 2018, a move by a Minister of State Security exposes the dangers or risks for lack of provision for the application of the principles of separation of powers and checks and balances in managing the affairs and activities of the SSA, the effect of action or inaction may be controversial.[1919] It was reported that a Minister of State Security allegedly intended to purge the SSA of the alleged loyalists of the former President —Mr. Jacob Zuma— by selectively conducting a fresh security clearance on the loyalists without going through the due process of disciplinary or labour practice in this regard.[1920]

Although the Minister can conduct random security checks on members of SSA in pursuance of the law,[1921] however, if the only consideration for the application of the law is politically motivated and not based on law, then the provision on random security check leaves much to be desired, thus, may amount to an abuse of office or power.

The non-compulsory publication by the Minister of State Security and lack of National Assembly checks of the regulation of the internal rules concerning complaints and consultation on the conditions of service and human resources do not encourage the use of transparent or impartial regulation,[1922] thus impacts on the effective conduct of an OCI in this regard. Nonetheless, the involvement of the JSCI of Parliament is a re-assurance for members of SSA

Security solely appoints members of ICCS on contract. The appointment apparently has the tendency of making the Minister have full control of the affairs of or making the Minister abuse the processes in the ICCS, see ss 22(b) and 34 of the GILAA *II* and sections 10(1) and (2)(a)and (b) and 22 of the ISA (as amended by section 22 of GILAA *II*); Ministry for Intelligent Services 'Regulation 4 -Profile of an Intelligence Officer' Notice No 1505 Regulation No. 7797 Gazette No. 25592 of 2003 http://www.oigi.gov.za/Legislation/IntelServRegs_2003Oct.htm (Date of use: 14 December 2013. Hartley http://www.bdlive.co.za/national/2013/08/08/single-intelligence-body-wields-great-power (Date of use: 28 February 2014).

[1918] Section 10 of the ISA, more particularly s 10(1), (2)(a) & (b), (3) (b) & (c).

[1919] Kgosana C 'The great spook purge: Agents claim move is directed at flushing out 'Zuma's loyalists' https://www.timeslive.co.za/politics/2018-11-11-the-great-spook-purge-agents-claim-move-is-directed-at-flushing-out-zuma-loyalists/ (Date of use: 15 December 2018) (Kgosana https://www.timeslive.co.za/politics/2018-11-11-the-great-spook-purge-agents-claim-move-is-directed-at-flushing-out-zuma-loyalists/ (Date of use: 15 December 2018).

[1920] Kgosana https://www.timeslive.co.za/politics/2018-11-11-the-great-spook-purge-agents-claim-move-is-directed-at-flushing-out-zuma-loyalists/ (Date of use: 15 December 2018).

[1921] Sections 39, 40 and 43 of the GILAA *II* and sections 27, 28(1) and 31 of the ISA.

[1922] Sections 33 of the GILAA *II* and section 21(1), (2) and (3) of the ISA.

to have their grievances concerning the activities and affairs of the SSA re-considered at a different forum.

The re-consideration allays the concerns of members whose interests may adversely be impacted in the fair and conducive working environment for criminal investigation, including the conduct of an OCI. Also, it may be argued that the broad provision which enables the Minister of State Security to make regulations in all issues after consultation with the JSCI of Parliament brings some succour to the concern of partiality and non-transparency of SSA.[1923]

There may not be adequate independence and transparency in the process of demoting or discharging a member of SSA from service arising from their absence from work without leave,[1924] ill-health,[1925] poor performance[1926] and gross misconduct.[1927] This is because, although the doctrine of separation of power is observed, none of the machineries of the principle of checks and balances is vested in the National Assembly. The machineries are all vested within the same cluster; i.e. the Director-General, Minister and Advisory Panel are within the control of the executive arm of government.

The wide powers given to the Minister of State Security to discharge members of SSA on such conditions as he or she may determine lacks the application of the doctrine of separation of powers and principle of checks and balances and makes the Minister unnecessarily and uncontrollably independent.[1928] These statutory provisions in this regard may weaken or threaten the effectiveness of crime investigations if the practice of victimization and nepotism compel some competent and resourceful members to resign unintentionally and inconsequentially.[1929]

The provision preventing the constructive dismissal or unnecessary transfer of members of SSA without consent appears to satisfy the principle of due process and guarantees sufficient independence, transparency and security of conditions of service for members[1930] for effective

[1923] Section 48 of the GILAA *II* and section 37 of the ISA.
[1924] Section 27 of the GILAA *II* and section 15 of the ISA.
[1925] Section 28 of the GILAA *II* and section 16 of the ISA.
[1926] Section 29 of the GILAA *II* and section 17 of the ISA.
[1927] Section 30 of the GILAA *II* and section 18 of the ISA.
[1928] Section 31(c) of the GILAA *II* and section 19(1)(c) of the ISA.
[1929] Hartley http://www.bdlive.co.za/national/2013/08/08/single-intelligence-body-wields-great-power (Date of use: 28 February 2014).
[1930] Section 31(b) and (d) of the GILAA *II* and sections 19(1)(a)(cc) and (2) of the ISA.

investigation without any fear, favour or prejudice in the conduct of an OCI. However, during war, state of emergency or compelling exigencies, consent of such member is not required for secondment[1931] because of the necessity or urgency to ensure the protection of State security and enforcement of crime control through effective investigation in conducting an OCI.

The TFA is compelled to provide training on intelligence matters —as the Minister may prescribe— in the appointment, promotion or transfer of members of SSA in accordance with SAQA requirements.[1932] However, at the 2016 JSCI report submitted to the National Assembly, it was revealed that SSA lacked the required 'intellectual and professional capacity in ICT security.[1933] It will not be surprising therefore to similarly conclude on this issue with regards to the conduct of an OCI by members and head of SSA because they are regrettably not required to possess a qualification in the conduct of an OCI.

However, before the introduction of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, Cybercrime and Cybersecurity Bill made provision for the cooperation of the Minister of State Security with higher institutions within or outside the RSA on the development and implementation of accredited training programmes for members of SSA.[1934] If this provision was not expunged, the training would have given effect to the provision on the development of capacity for cybersecurity and protection of critical information infrastructure in the RSA,[1935] which should include the conduct of an OCI.

In conclusion, despite the high level of significance and complexity involved in the techno-legal aspects of conducting an OCI in contemporary society[1936] and the provisions of RICA, there is no specific, published, and the complementary legal framework —including advert

[1931] Section 47 of GILAA *II* and s 36(1) of the ISA.

[1932] Department of State Security 'Statement on recent developments relating to the management State Security Agency' http://www.ssa.gov.za/Portals/0/SSA%20docs/Media%20Releases/2013/Media%20Release%20Statement%20on%20recent%20developments%20relating%20to%20the%20State%20Security%20Agency%202%20August%202013.pdf (Date of use: 25 February 2014). Sections 13, 17 and 21(a) and (b) of the GILAA *II*; Sections 1, 5 and 9(7) of the ISA (as amended by section 8 of GILAA No. 52 of 2003 'GILAA *1*').

[1933] Parliament of the Republic of South Africa 'Announcement, Tablings and Committee Reports' No 164 -2016 at 21.

[1934] Section 54(1)(a) (iii) of the CCB B6-2017, which is expunged by the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017.

[1935] Section 54(1) (a) (ii) (aa) & (bb) of the CCB B6-2017, which is expunged by the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017.

[1936] See sections 27(3), 31(4), 32, 33(1), 34) (1), 35(1)-(4) and 37(1)and (3) of the CCB B6-2017, which are with replaced with sections 29(3), 33(4), 34, 35(1), 36(1), 37(1)-(4) and 39 (1) &(3) of the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017.

placement, decision or policy— that requires the head and members of SSA in charge of the conduct of OCI to be specialists or have some level of competence in the field of OCI as part of the requirements for the relevant positions.[1937]

4.3.6 Appointment and specialised skill for the Defence Intelligence of the South African National Defence Force in the conduct of online criminal investigation

Under the PSA,[1938] the Minister of Defence solely appoints the head and executive authority of the DI-SANDF who is a member of SANDF, thus, this provision fails to comply with the principles of separation of powers and checks and balances. One would have thought that to prevent political influence, manoeuvring or non-professionalism; the head of DI-SANDF should be appointed by the Chief of SANDF in conjunction with the National Assembly to promote the principles of checks and balances, transparency, impartiality, competence and resourcefulness.

The law creates a discretionary power in favour of the Minister of Defence to establish defence training institutions for purposes of providing specialised instructions and other training for members and employees of the SANDF[1939] while it is the responsibility of the Chief of SANDF to train and develop members of SANDF including the DI-SANDF.[1940] These latter provisions are relatively adequate.

However, granting a discretionary power to the Minister of Defence to establish specialised training institutions is inadequate because specialisation of the military is indispensable. Therefore, the establishment of military training institutions should not be discretionary including the specialisation of the DI-SANDF which serves as the cornerstone for any military warfare, which in the contemporary society includes intelligence on the use of artificially

[1937] Parliament 'Annual Report of the Joint Standing Committee on Intelligence for the Financial Year ending 31 March 2017' 7 and 11-12.
[1938] Sections 1 & 3 (7) of the PSA and sections 5, 13 (2), 14(e) and 82(r) of DA; Section 1 and 9 of the PSA.
[1939] Section 63 and 82(1) (h) (i) &(vi) of the DA.
[1940] Section 14(e) and (i) of DA. Joint Standing Committee on Intelligence at para 4.8 http://www.pmg.org.za/docs/2011/comreports/110921jcintelligencereport.htm (Date of use: 13 October 2013). De Wet P 'From Bully Boys to Wimps: the Decline of SA's Military' http://mg.co.za/article/2012-05-04-lack-of-funds-leaves-sa-vulnerable (Date of use: 12 October 2013) (De Wet http://mg.co.za/article/2012-05-04-lack-of-funds-leaves-sa-vulnerable (Date of use: 12 October 2013).

intelligent and machine learning-driven apparatuses to conduct an OCI such as UAV or drones.[1941]

Furthermore, if the CCB was enacted as a law in its current shape and form concerning the training of LEOs, it would be relatively adequate, however, the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 expunged the provision. The CCB provided that the Minister of Defence must, on an annual basis, report to the Chairperson of Joint Standing Committee on Defence of National Assembly on the progress made on the training of SANDF members on cyber offensive and defence capacity.[1942] This provision is similar to the strategic planning for a cyber offensive by the U.S authorities arising from the alleged cyberwar offensive by China.[1943]

The specialised training in cyber offence and defence capacity should include the conduct of an OCI in the RSA. However, in these provisions above, amongst other requirements, there is no obligation required of the members and head of DI-SANDF to possess any knowledge or skill on the conduct of an OCI during recruitment or retention exercise.

In summary, despite the high-level significant complexity involved in the techno-legal aspects of conducting an OCI in online communication in contemporary society[1944] and aside from the provisions of RICA, there is no specific, published, and complementary legal framework — including advert placement, decision or policy— that requires the head and members of DI-

[1941] See para 2.11.4 of Chapter 2 of this study; Agwu F A *Armed Drones and Globalisation in the Asymmetric War on Terror - Challenges for the Law of Armed Conflict and Global Political Economy* (2017) i.

[1942] Section 54(3)(c) of the CCB B6-2017, which is now expunged by the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

[1943] Cornwell R 'US declares cyber war on China: Chinese military hackers charged with trying to steal secrets from companies including nuclear energy firm' https://www.independent.co.uk/life-style/gadgets-and-tech/us-charges-chinese-military-hackers-with-cyber-espionage-bid-to-gain-advantage-in-nuclear-power-9397661.html (Date of use:12 December 2018); Yi S 'Talk of US cyber war on China ridiculous' http://www.globaltimes.cn/content/1107699.shtml (Date of use: 12 December 2018); Goud N 'Did United States declare a Cyber War on Russia?' https://www.cybersecurity-insiders.com/did-united-states-declare-a-cyber-war-on-russia/ (Date of use:12 December 2018); Nakashima E 'Pentagon launches first cyber operation to deter Russian interference in midterm elections' https://www.washingtonpost.com/world/national-security/pentagon-launches-first-cyber-operation-to-deter-russian-interference-in-midterm-elections/2018/10/23/12ec6e7e-d6df-11e8-83a2-d1c3da28d6b6_story.html?utm_term=.481584E67641 (Date of use:12 December 2018); Cilluffo F J and Cardash S L 'With hacking of US utilities, Russia could move from cyberespionage toward cyberwar' https://mg.co.za/article/2018-08-05-with-hacking-of-us-utilities-russia-could-move-from-cyberespionage-toward-cyberwar (Date of use:12 December 2018).

[1944] See generally Chapter 2 of this study. See sections 27(3), 31(4), 32, 33(1), 34) (1), 35(1)-(4) and 37(1) & (3) of the CCB B6-2017, which are replaced by sections 29(3), 33(4), 34, 35(1), 36(1), 37(1)-(4) and 39 (1) and (3) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

SANDF in charge of the conduct of an OCI to be specialists or have some level of competence in the field of OCI as part of the requirements for the relevant positions.[1945]

4.3.7 Appointment and specialised skill for the Investigating Directorate of the National Prosecuting Authority in the conduct of online criminal investigation

Although there is compliance with the doctrine of separation of powers in the appointment of the head of the ID-NPA by the President of the RSA assisted by the Minister of Justice and National Director of NPA —all of whom tend to be influenced by the concept of collective responsibility in the cabinet or political party politics or loyalty,[1946] there is no adequate compliance with the principle of checks and balances since the appointment process excludes the National Assembly.

Although the head of ID-NPA does not have controlling power over the employment of members who perform services in specific areas in ID-NPA, the trio employment procedure of members of the ID-NPA amongst the National Director of NPA in consultation with the head of ID-NPA and the Minister of Justice[1947] ensures checks and balances in this regard.

While the head of ID-NPA does not have controlling power over the employment of persons who perform services in specific areas in ID-NPA, the National Director of NPA consults with the head of ID-NPA and the Minister of Justice in the service delivery in ID-NPA.[1948]

Not only is the tenure of office of the head of ID-NPA secure as a civil servant, he or she vacates the position or retires at the age of 65.[1949] The security of tenure of office, to some extent in this regard, ensures independence, competence and resourcefulness of the head of ID-NPA.

Apart from the provision for the training of prosecutors who are professionally qualified and the requirement that prosecutors must be 'fit and proper persons',[1950] there is no provision for

[1945] Parliament 'Annual Report of the Joint Standing Committee on Intelligence for the financial year ending 31 March 2017' at 6.
[1946] Section 13(1)(b) of the NPAA; *DA v President* supra 24.
[1947] Section 38 of the NPAA.
[1948] Section 38 of the NPAA.
[1949] Section 16 (4) of the PSA and sections 13(3), 14(1) and (2) of the NPAA.
[1950] Section 38 of the NPAA.

the training of prosecutors and non-prosecutors —including investigators— in the Act[1951] or in any public document[1952] that the head and members of the ID-NPA must be trained or possess the specific or specialised qualification or experience in the field of OCI.

It is however noted that partial reliance may be placed on the provisions of the PSA[1953] which generally regulate the training of public servants[1954] which can be extended to the head and members of ID-NPA especially the OCI investigators who are not lawyers and who do not have adequate knowledge of the substantive and procedural aspects of the conduct of an OCI. However, the general training programme under the PSA may not be sufficient for the specialized area of an investigation involving the conduct of an OCI, if the peculiar training needs of ID-NPA are not met with regards to the conduct of an OCI.

In conclusion, despite the high level of significance and complexity involved in the techno-legal aspects of conducting an OCI in contemporary society[1955] and the provisions of RICA, there is no specific, published, and complementary legal framework —including advert placement, decision or policy— that requires the head and members of ID-NPA in charge of the conduct of an OCI to be specialists or have some level of competence in the field of OCI as part of the requirements for the relevant positions.

4.3.8 Conclusion

Consequently, it is revealed in this segment that the techno-legal framework regulating the affairs and management of the appointment of specialised head and staff and their training in the field of OCI is generally inadequate in the RSA. To ameliorate the *status quo*, the following should be considered.

[1951] See section 7(4) (a) (iii) -(v) & (b) and 22(4)(g)(v) of the NPAA.

[1952] Section 22(4)(g)(v) and (7) of the NPAA. Former Minister of Justice, Mr. Mabunda reiterated the need to have specialized, experienced, talented and skilled investigators in ID-NPA. Between 1994 and 1997, a total of 630 prosecutors resigned which resulted in the engagement of inexperienced and incompetent prosecutors which were questioned by the High Court, Pretoria in 1998, see NPA *Prosecuting service* at 43 and 77. Section 180(a) of the Constitution provides for training of judicial officers only.

[1953] The PSA.

[1954] Sections 4, 7(3) (a) and (b) and 11(2) of the PSA.

[1955] See ss 27(3), 31(4), 32, 33(1), 34) (1), 35(1)-(4) and 37(1) &(3) of the CCB B6-2017, which are replaced by sections 29(3), 33(4), 34, 35(1), 36(1), 37(1)-(4) and 39 (1) &(3) of the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017.

Firstly, the appointment or disengagement of the head of the various LEAs should comply with the basic principles of separation of powers and checks and balances, while adequate measures —such as compulsory, continuous and random objective vetting— should be carried out on the head and members of staff of all the categories of LEAs in their appointment or disengagement as applicants in RICA.[1956] In all of this, competent, transparent, impartial, independent and accountable head and members of the LEAs and LEOs will be guaranteed to engage in the conduct of an OCI.

Secondly, notwithstanding the various degrees or qualifications that the head and members of the various LEAs are required to possess for recruitment, deployment or retention in the conduct of OCI, heavy reliance will be placed on the lessons of the pronouncement of the court in *FAWU v Premier Foods* relating to the qualification in the field of Polygraph Science as a yardstick in conducting an investigation.[1957] While the two experts who carried out a polygraph test had PhDs in Polygraph and Psychology Science respectively as their personal academic feat, the minimum requirement in polygraphic qualification is not a PhD. The court emphasised the need for a polygraph scientist to have minimum required qualifications as part of the requirements to prove the reliability of the use of Polygraph Test as a specialised investigative method,[1958] minimum qualification is required to conduct or supervise the conduct of an OCI in the RSA.[1959]

Thus, in opposition to the decision of the Constitutional Court in *Suzman Foundation v Min of Police* which confirms that investigators should not be required to possess the legal qualification to conduct an investigation,[1960] it is submitted that LEOs who conduct an OCI — as a specialised, delicate and complex investigative procedure— should possess a minimum qualification approved by SAQA in both technical and legal aspects of an OCI. This proposal will guarantee the integrity and security of online communication and the conduct of an OCI. This is also in pursuance of the campaign for the recognition, protection and regulation of an independent professional body of Electronic Criminal Investigators.[1961]

[1956] Sections 39, 40 and 43 of GILAA *II* and sections 27, 28(1) and 31 of the ISA.
[1957] *FAWU v Premier Foods* supra 50.
[1958] *FAWU v Premier Foods* supra 50
[1959] Para 4.6 of this chapter.
[1960] *Suzman Foundation v Min of Police* para 66.
[1961] See para 4.3 of Chapter 4 and para 5.3.3.1 of Chapter 5 of this study.

It is therefore recommended that the curriculum development of such qualification in terms of the modules to be offered may include some, all or more of the following twenty-five modules conducted by accredited institutions: i) Introduction to Information and Communication Technology 1 and 11; ii) Introduction to Law 1 and 11; iii) Constitutional Law 1 and 11; iv) Criminal Law and Procedure 1 and 11; v) Civil Procedure Law; vi) Law of Delict; vii) Law of Evidence 1 and 11; viii) Administrative Law; ix) Domestic and International Territorial Law; x) Law of Contract; xi) Cyber Law 1 and 11; xii) Interception Law 1 and 11; xiii) Domestic and Extra-territorial Interception Law 1 and 11; xiv) Electronic Criminology and Sociology; xv) Accounting for Electronic Investigators; xvi) Online Alternative Dispute Management and xvii) Professional Ethics and Management.

4.4 OPERATION AND FUNDING OF LAW ENFORCEMENT AGENCIES IN THE CONDUCT OF ONLINE CRIMINAL INVESTIGATION

4.4.1 Introduction

This rubric examines the adequacy or otherwise of the regulation of the operation and funding[1962] of the LEAs in conducting an OCI as a specialised method, and unit in the investigative, security or intelligence services cluster.

4.4.2 Operation and funding of the Crime Intelligence of South African Police Service in the conduct of online criminal investigation

Under the SAPS, the CI-SAPS is a division that deals with the operation of crime prevention, provides technical support for the investigation, manages crime intelligence and analyses crime statistics,[1963] the ratings of which are commendable in some instances.[1964]

[1962] Police Executive Research Forum *Cameras* 117-118.

[1963] South African Police Service *Annual report* 2017/2018 at 15, 17, 28, 29, 191; South African Police Service *Annual report* 2008/2009 at 126.

[1964] South African Police Service 'Annual report 2012/2013' at 143-145 http://www.saps.gov.za/about/stratframework/annualreports.ph (Date of use: 6 June 2013 and South African Police Service 'Annual Report 2011/2012' at 117 http://www.saps.gov.za/about/stratframework/annualreports_arch.php (Date of use: 6 June 2013).

Like any other division in the SAPS, the CI-SAPS operates under the control and management of the SAPS,[1965] thus, the operation of the CI-SAPS is not in an independent division or authority of the SAPS or any other department of government. Consequently, the regulation of the conduct of an OCI is dependent on the general operations of investigations by SAPS, which is inadequate for the conduct of an OCI because there is no adequate provision for the conduct of an OCI.

Aside from the provisions of RICA, no law, regulation or policy establishes, neither is there a publication that announces the establishment or operation of a unit or sub-division under CI-SAPS that internally, strictly and holistically administers the conduct of an OCI, which is a significant, complex and delicate method of investigation in electronic communication.[1966]

However, in 2018, the CI-SAPS merely announced the establishment of Cybercrime Steering Committee charged with the responsibility of establishing, capacitating and funding Cybercrime Centre and training of LEOs,[1967] which is one of the aspects of the conduct of an OCI. Thus, the strategy still excludes one of the other aspects of the conduct of an OCI which is the investigation of offences committed offline, because this study posits that the conduct of an OCI is for the investigation of both offline and online offences.

Despite the announcement, the contents of the modalities in the strategy are not in the public domain for implementation or for public scrutiny. It therefore follows that the personnel in charge of the conduct of an OCI will have no choice but to resort or not resort to the general policy on crime intelligence or investigation in the CI-SAPS regarding the operation or administration of the conduct of an OCI as examined in this study.

Given that the personnel in charge of the administration of the conduct of an OCI are members of the CI-SAPS and are not divorced from the general institutionalised, structural and operational imbroglio involving the CI-SAPS,[1968] it is arguably posited that the personnel in

[1965] South African Police Service *Annual report* 2017/2018 at 136.
[1966] See generally Chapter 2 of this study, more particularly paras 2.2, 2.3 and 2.5 - 2.11.
[1967] South African Police Service *Annual report* 2017/2018 at 20, 184-185 and 204 - 205.
[1968] Mbhele https://www.news24.com/Columnists/GuestColumn/professionalise-the-police-and-start-with-its-leaders-20190328 (Date of use: 31 March 2019); Right2Know 2 and 35 'Spooked- Surveillance of journalists in South Africa' https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018) (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

charge of the conduct of an OCI also are affected by some of the following challenges. These challenges range from the suspension of the heads and members of CI-SAPS to the seemingly unending uncertainties and undue political and non-political influence or manoeuvring within and outside the SAPS generally.[1969]

Aside from the possible political influence on the conditions of operation of CI-SAPS,[1970] other operational challenges occur in SAPS which ultimately, may directly or indirectly adversely impact on the administration and conduct of an OCI. These challenges include budgetary constraints;[1971] failure or refusal to modernise police techniques;[1972] incompetence in the identification, collection, processing and utilisation of crime information; lack of protection of information culture[1973] and collection of information in an unlawful manner.[1974]

Other challenges of CI-SAPS include absence of close and mutual working relationships with the community to exchange information;[1975] reluctance by witnesses to give information or

[1969] SAPA http://www.enca.com/south-africa/phiyega-does-structural-change-crime-intelligence (Date of use: 21 February 2014; Goko http://www.bdlive.co.za/national/2013/10/22/crime-intelligence-boss-ngcobo-on-special-leave-credentials-probed (Date of use: 18 January 2014); Faull *ISS* Paper 227 at 10.

[1970] Section 13 of SAPSA; The CI-SAPS does not operate independently and some of the facts concerning CI-SAPS (including its budget) may not be in the public domain in view of the crucial nature of their operations, Oneale L 'Crime Intelligence of South Africa Is a Complete Fiasco' http://guardianlv.com/2014/01/crime-intelligence-of-south-africa-is-a-complete-fiasco/ (Date of use: 20 January 2014) (Oneale http://guardianlv.com/2014/01/crime-intelligence-of-south-africa-is-a-complete-fiasco/ 20 January 2014); Burger J 'To protect and server-Restoring public confidence in the SAPS' (2011) 36 *SACQ* 13 at 13-19(Burger (2011) 36 *SACQ*); Faull A 'When I see them I feel like beating them-Corruption and the South African Police Service' 2010 34 *SACQ* 33 at 35- 39 (Faull 2010 34 *SACQ*); Right2Know 'Spooked- Surveillance of Journalists in SA' at 13-14 and 35 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018) (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use:27 November 2018).

[1971] South African Police Service *Annual report* 2017/2018 at 13; Joint Standing Committee on Intelligence at para 4.9 http://www.pmg.org.za/docs/2011/comreports/110921jcintelligencereport.htm (Date of use: 13 October 2013; Oneale http://guardianlv.com/2014/01/crime-intelligence-of-south-africa-is-a-complete-fiasco/(Date of use:20 January 2014).

[1972] Zinn R 'The Value of Crime Intelligence in Combating Violent Crime' Inaugural lecture delivered at the Department of Police Practice, University of South Africa 2011' at 10 http://uir.unisa.ac.za/bitstream/handle/10500/7649/R_Zinn_Inaugural%20Speech.pdf?sequence=1 (Date of use:12 December 2013 (Zinn at 10 http://uir.unisa.ac.za/bitstream/handle/10500/7649/R_Zinn_Inaugural%20Speech.pdf?sequence=1 (Date of use: 12 December 2013).

[1973] Govender D *The nature and extent of problems experienced by detectives in the collection, processing and utilisation of crime information at the Rustenburg Detective Service* (2008) at 1 (Govender *Nature and extent of problems experienced by detectives* 2008).

[1974] Govender *Nature and extent of problems experienced by detectives* 2008 20.

[1975] Block C, Dabdoub M & Fregly S *Crime Analysis Through Computer Mapping* (1995) at 3 (Block, Dabdoub & Fregly *Crime Analysis Through Computer Mapping* (1995) and Govender *Nature and extent of problems experienced by detectives* 2008 30.

make statements due to fear of reprisal from criminals[1976] and insufficient training and inadequate resources and computer support at station level.[1977]

In addition, the following challenges of CI-SAPS are noted: lack of computer support for detectives to conduct computerised processing and problem of data integrity in computer system[1978] and a number of general police officers in SAPS appear not to understand the value of crime intelligence in police operations.[1979]

It is important to note that, more often than not, the conduct of an OCI involves the offline gathering of information, save in some exceptional circumstances where there is an online detection,[1980] thus, some of these operational challenges that are expressed in the offline world are also relevant to the administration and conduct of an OCI.

[1976] Govender *Nature and extent of problems experienced by detectives* 2008 32 - 33 and Parliamentary Monitoring Group 'Question 720 of 2013/17B Parliamentary Monitoring Group question posed to the Minister of Police' http://www.oigi.gov.za/Legislation/IntelServRegs_2003Oct.htm (Date of use: 14 December 2013).

[1977] Govender *Nature and extent of problems experienced by detectives* 2008 43.

[1978] Govender *Nature and extent of problems experienced by detectives* 2008 45; McKan J 'SAPS wanted to pay R45 million for cell phone spy hardware to fund Zuma' https://mybroadband.co.za/news/government/292800-saps-wanted-to-pay-r45-million-for-cellphone-spy-hardware-to-fund-zuma.html (Date of use: 28 January 2019) (McKan https://mybroadband.co.za/news/government/292800-saps-wanted-to-pay-r45-million-for-cellphone-spy-hardware-to-fund-zuma.html (Date of use: 28 January 2019).

[1979] Zinn at 18 http://uir.unisa.ac.za/bitstream/handle/10500/7649/R_Zinn_Inaugural%20Speech.pdf?sequence=1 (Date of use: 12 December 2013).

[1980] Para 6.6 of Chapter 6 of this study.

There are also reports of lack of capacity by SAPS to deal with corruption within the organisation[1981] and the general offline[1982] and online investigative challenges faced by CI-SAPS,[1983] more particularly in the conduct of an OCI.[1984]

Lack of discipline and disobedience to the lawful order or wilful misconduct of officers contribute to the operational challenges of CI-SAPS.[1985] However, section 199(6) and (7) of the Constitution prohibits LEOs from carrying out unlawful order in their operation or acting unlawfully,[1986] which arguably includes the prohibition of activities involving the conduct of an OCI. It is submitted that this provision guarantees the application of checks and balances in the conduct of an OCI.

[1981] SAPS Civilian Secretariat for Police at 48-49 http://www.policesecretariat.gov.za/downloads/green_paper_policing.pdf (Date of use: 18 September 2013); Faull 2010 34 *SACQ* 35- 38; Faull *ISS* Paper 227 at 10.

[1982] Kruger *Organised crime and proceeds of crime* 5. Govender *Nature and extent of problems experienced by detectives* 2008 1 and 32 - 33 and Parliamentary Monitoring Group 'Question 720 of 2013/17B Parliamentary monitoring group question posed to the minister of police' http://www.oigi.gov.za/Legislation/IntelServRegs_2003Oct.htm (Date of use: 14 December 2013). Block, Dabdoub & Fregly *Crime analysis through computer mapping* (1995) 3 and Govender *Nature and extent of problems experienced by detectives* 2008 2, 20, 30 and 44 and

Ratcliffe J H 2003, "Intelligence-led policing", trends and issues in crime and criminal justice, no. 248, Australian Institute of Criminology, Canberra; SAPA http://www.enca.com/south-africa/phiyega-does-structural-change-crime-intelligence (Date of use:21 February 2014); Zinn at 18 http://uir.unisa.ac.za/bitstream/handle/10500/7649/R_Zinn_Inaugural%20Speech.pdf?sequence=1 (Date of use: 12 December 2103).

[1983] Zinn at 10 http://uir.unisa.ac.za/bitstream/handle/10500/7649/R_Zinn_Inaugural%20Speech.pdf?sequence=1 (Date of use: 12 December 2013); Govender *Nature and extent of problems experienced by detectives* 2008 43 and 45. Goko http://www.bdlive.co.za/national/2013/10/22/crime-intelligence-boss-ngcobo-on-special-leave-credentials-probed (Date of use: 18 January 2014); Section 199(5) of the Constitution.

[1984] McKan https://mybroadband.co.za/news/government/292800-saps-wanted-to-pay-r45-million-for-cellphone-spy-hardware-to-fund-zuma.html (Date of use: 28 January 2019); Pieterse 'Electronic Crime Unit: Directorate for Priority Crime Investigation' 65 and 73.

[1985] Section 47 of SAPSA; SAPS 'National Police Commissioner General Riah Phiyega streamlines the South African Police Service crime intelligence environment' http://www.gov.za/speeches/view.php?sid=43031 (Date of use:21 January 2014) (SAPS http://www.gov.za/speeches/view.php?sid=43031 (Date of use: 21 January 2014); Barnes H 'F v Minister of Safety and Security-Vicarious Liability and State Accountability for the Criminal Acts of Police Officers' 2014 47 *SACQ* 29 at 30-33 (Barnes 2014 47 *SACQ*).

[1986] Section 13 of SAPSA; Oneale http://guardianlv.com/2014/01/crime-intelligence-of-south-africa-is-a-complete-fiasco/ (Date of use: 20 January 2014); Burger 2011 36 *SACQ* 13-19; Faull 2010 34 *SACQ* 35- 39. Section 47 of SAPS Act No. 68 of 1995; Saps http://www.gov.za/speeches/view.php?sid=43031 (Date of use: 21 January 2014); Barnes 2014 47 *SACQ* 30-33. However, there is provision for a high ethical standard in similar institutions such as HAWKS or Chapter 9 Institutions in the Constitution with adequate provisions in this regard, see section 205(2) of the Constitution, ss 181(2), (3) and (4) and 199(7)(b) and (8) of the Constitution and sections 17CA(1)(b), 17E(9) and 17 E of the SAPSA.

The failure of the CI-SAPS to apply high operational standard rules arguably contributes to some of the operational challenges faced by the CI-SAPS.[1987] This is unlike the provision for high ethical statutory standards in similar institutions such as HAWKS[1988] and Chapter Nine Institutions in the Constitution which have adequate provisions on ethical standards[1989] and recently the provisions of the pending the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, which arguably include the regulation of CI-SAPS and HAWKS because they are under the general management of SAPS.

The Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 requires the Minister of Police in consultation with the National Commissioner of SAPS, National Director of Public Prosecution and Minister of Justice to issue and publish in a Gazette an SOP on the investigation of offences in the CCB, which must be observed by other LEAs.[1990]

This provision fills the gap on the provision for an internal procedure on the conduct of investigation in extant laws. However, it is inadequate in the sense that the proposed Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 does not extend the consultation to other LEAs which are not mentioned above to make their contribution to SOP, particularly in their statutorily and operationally specialised areas of law enforcement and crime control expertise.

Like any other division in the SAPS, the CI-SAPS is funded from the allocation made by National Assembly to the SAPS,[1991] which arguably and adversely impact on the independence and competence of CI-SAPS, like any other division in SAPS.

[1987] Section 47 of SAPSA; Saps http://www.gov.za/speeches/view.php?sid=43031 (Date of use: 21 January 2014); Barnes 2014 47 *SACQ* 30-33.

[1988] Sections 17CA(1)(b), 17E (9) and 17 E of the SAPSA.

[1989] Although section 205(2) of the Constitution expects that national legislation shall provide that the SAPS discharge its responsibility effectively, the parameters for the effectiveness are not directly or expressly provided in the Constitution (including chapter 11) as opposed to chapter 9 of the Constitution or section 181(2), (3) and (4) and 199(7)(b) and (8) of the Constitution which guarantee independence of the chapter 9 institutions.

[1990] Section 24(1)(a) & (b) and (2) of the CCB B6-2017, which is replaced by s 26(1)(a) & (b) and (2) of the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017.

[1991] South African Police Service *Annual report* 2017/2018 at 136.

Despite its large budgetary vote, the CI-SAPS encounters budgetary constraints[1992] and financial wastages on non-professional operations and activities[1993] which arguably affect the administration and conduct of an OCI. Such activities include the unlawful uses of resources of CI-SAPS to fight internal factional or political battles[1994] with or without a political party influence or manoeuvring.[1995] However, section 199(7)(a) and (b) of the Constitution prohibits LEAs from using their powers in a partisan or prejudicial manner towards or against a political party.

However, for effective independence of the operations of CI-SAPS in conducting an OCI, the budgetary allocation should be directly sourced from the National Department of Treasury and not under the general budgetary allocation of SAPS. It is also advised that the CI-SAPS should be depoliticised[1996] and reinforced[1997] by generally placing emphasis on procedural operation[1998] including the administration and conduct of an OCI.

4.4.3 Operation and funding of the Directorate of Priority Crime Investigation in the conduct of online criminal investigation

Although with some level of independence as examined below, however, the DPCI or HAWKS generally operates under the control and management of the SAPS.[1999]

[1992] South African Police Service *Annual report* 2017/2018 at 13; Joint Standing Committee on Intelligence at para 4.9 http://www.pmg.org.za/docs/2011/comreports/110921jcintelligencereport.htm (Date of use: 13 October 2013); Oneale http://guardianlv.com/2014/01/crime-intelligence-of-south-africa-is-a-complete-fiasco/ (Date of use: 20 January 2014).

[1993] Harper https://mg.co.za/article/2018-03-02-00-cele-takes-aim-at-crime-intelligence (Date of use: 19 June 2018); ENCA 'Crime intelligence's piggy bank detailed at Zondo Commission' https://www.enca.com/news/crime-intelligences-piggy-bank-detailed-zondo-commission (Date of use: 18 September 2019).

[1994] According to one of the Biblical doctrines in Mathew 12: 25, it says that a house that is divided against itself cannot stand. Right2Know at 2 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[1995] Harper https://mg.co.za/article/2018-03-02-00-cele-takes-aim-at-crime-intelligence (Date of use: 19 June 2018).

[1996] Harper https://mg.co.za/article/2018-03-02-00-cele-takes-aim-at-crime-intelligence (Date of use: 19 June 2018).

[1997] Naidoo http://www.sabcnews.com/sabcnews/saps-boost-crime-intelligence-division-iss/ (Date of use: 18 March 2018).

[1998] Harper https://mg.co.za/article/2018-03-02-00-cele-takes-aim-at-crime-intelligence (Date of use: 19 June 2018).

[1999] South African Police Service *Annual report* 2017/2018 at 15, 18 and 28.

While the SAPS regards the commission of every offence as a serious one,[2000] however, the HAWKS, being a specialised division or unit, prevents, combats and investigates national priority, and more serious organised, commercial and corrupt offences as described by SAPS,[2001] as opposed to the definition of national priority, serious or more serious offence conceptualised in this study.[2002]

The operation of the HAWKS —which replaces the Scorpion— is not based on the *Troika* system implemented by the erstwhile Scorpion under NPA which ignored the application of the principle of separation of powers.[2003] The Scorpion was disbanded because of the fusion of powers it exercised in 'detecting, investigating and prosecuting' crime under the management and control of the NPA, which is primarily concerned with the prosecution of offences.[2004] The application of separation of powers demonstrates fairness and transparency in a criminal investigation, including the conduct of an OCI.

However, it is on record that the HAWKS has not been able to match the successful record created by the defunct Scorpions in combating white-collar and organised crime.[2005] What has become rampant within the HAWKS is the internal rancour or in-fighting in the agency,[2006] which arguably tends to bring the standard of efficiency and effectiveness of operation to a low level, including the conduct of an OCI.

Aside from the provisions of RICA, there is no specific, published, and complementary legal framework that internally regulates the operations, administration, and conduct of an OCI by the HAWKS. Thus, resorts to the implementation of the general frameworks that are used in

---

[2000] South African Police Service *Annual report* 2017/2018 at 19.
[2001] South African Police Service *Annual report* 2017/2018 at 183.
[2002] See para 6.3 of Chapter 6 of this study.
[2003] Section 17J of SAPSA. The *Troika* principles consist of a) intelligence or analysis; b) investigation and c) prosecution, Montesh *Crime investigative system* at 130. *In re Certification of the Constitution of the RSA* 1996 4 SA 744 (CC) 818F-H (par 141); De Vos at 5 http://constitutionallyspeaking.co.za/pierre-de-vos-memo-on-sa-police-service-amendment-bill/ (Date of use: 1 October 2013); and Hoffman http://www.ifaisa.org/Hawks_neither_effective_nor_sufficiently_independent.html (Date of use: 10 December 2013).
[2004] *Glenister* supra 6.
[2005] Section 17CA (21) and (22) of the SAPSA; See Chapter 2 of the CPA. See also the powers and authority of the disbanded Scorpion in Montesh *Crime investigative system* at 129; De Vos 5 http://constitutionallyspeaking.co.za/pierre-de-vos-memo-on-sa-police-service-amendment-bill/ (Date of use: 1 October 2013) and Hoffman http://www.ifaisa.org/Hawks_neither_effective_nor_sufficiently_independent.html (Date of use: 10 December 2013).
[2006] Right2Know at 2 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

other criminal investigative methods or no internal frameworks are used at all, which are not suitable for the complex and delicate operate, administration, and conduct of an OCI.[2007]

However, if the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017 was enacted in the current shape and form it is, the powers of the Minister of Police in issuing a Standard of Operations Procedures will be effective for HAWKS to conduct an OCI provided the National Assembly is consulted in this regard.[2008]

Given that the HAWKS has equal powers in its operation as members of SAPS or peace officers do under the SAPSA and CPA, the HAWKS now exercises some independence including the determination of what constitutes criminal conduct which was hitherto within the purview of SAPS.[2009]

Although the Constitution provides for cooperative governance amongst the organs of state and parastatals,[2010] which means that the HAWKS can cooperate with ID-NPA in the investigation of national priority offences.[2011] However, the statutory provision that enables the HAWKS to make a request to the ID-NPA to investigate national priority offences[2012] may show a sign of incompetence on the part of the HAWKS and dependence on ID-NPA.

Given that the HAWKS has a primary responsibility of conducting investigations, NPA should rather be the one to call upon the HAWKS to conduct some investigations so that the NPA can focus on criminal prosecution that is constitutionally and statutorily mandated to do. In the alternative, the establishment of a joint team between the duo would ensure that both parties significantly play their roles regarding the cooperative investigation. It is however noted that an effective investigation is not dependent on the Troika system that Scorpions applied, rather, it is dependent on strong institutional independence that a LEA practices.

[2007] See generally Chapter 2 of this study, more particularly paras 2.2, 2.3 and 2.5 - 2.11.
[2008] See para 4.4.2 of this chapter and section 24 of the CCB B6-2017, which is replaced by s 26 of CB 2018-Amendments Proposed to Bill B6-2017.
[2009] Sections 16(2) and 17K (7) and (8) of the SAPSA; Kinnes and Newham 2012 39 *SACQ* 33-36; Faull A and Mtsolongo T 'From Stings to Wings-Integrity Management and the Directorate for Priority Crime Investigations' 2009 29 *SACQ* 17 at 17 -22.
[2010] Chapter 3 of the Constitution.
[2011] Section 17D (3) of the SAPSA.
[2012] Section 17D (3) of the SAPSA.

On funding, the HAWKS is not financially independent, as it is tied to the apron of the National Commissioner of SAPS who holds sway in the funding of the unit. However, if the HAWKS is dissatisfied with the allocation by the National Commissioner, the provision allows a lodgement of a complaint by the head of HAWKS,[2013] thus, ensures an effective check and balance and conduct of OCI in this regard.

4.4.4 Operation and funding of the Independent Police Investigative Directorate in the conduct of online criminal investigation

The operational independence of IPID is emphatically and statutorily stipulated to enable it effectively perform its investigative functions[2014] —including the administration and conduct of an OCI— against members of SAPS for wrongdoing.[2015] The fact that IPID members are given equal investigative police powers under the various laws confirms the independence of IPID to investigate members of SAPS without fear, favour or prejudice.[2016]

However, aside from the provisions of RICA, there is no specific, published, and complementary legal framework that internally regulates the operation, administration, and conduct of an OCI by IPID, thus, resorts to the general frameworks that are used in other criminal investigative methods, which are not suitable for the complex and delicate conduct of an OCI.[2017]

In their operations, members of IPID have the backing of the law to reject any unlawful directive that may be given by any authority.[2018] In one of the speeches by a former Minister of Police, he berated the SAPS for interfering in the affairs of IPID[2019] and warned that they should desist from interfering with the operations and work of IPID.[2020] The warning by the

[2013] Section 17H of the SAPSA.
[2014] Sections 4 and 9(d) of the IPIDA; South African Police Service *Annual report* 2017/2018 at 46.
[2015] Sections 22(8) & (9), 24(2), 7(4) & (5) of the IPIDA.
[2016] Sections 22(8) and (9) and 24(2) of the IPIDA; South African Police Service *Annual report* 2017/2018 at 31.
[2017] See generally Chapter 2 of this study, more particularly paras 2.2, 2.3 and 2.5 - 2.11.
[2018] Section 24(1) of the IPIDA.
[2019] Gerber J 'Phahlane must explain why he shouldn't be suspended–Mbalula' https://www.news24.com/SouthAfrica/News/phahlane-must-explain-why-he-shouldnt-be-suspended mbalula-20170601 (Date of use:3 June 2018).
[2020] Harper https://mg.co.za/article/2018-03-02-00-cele-takes-aim-at-crime-intelligence (Date of use:19 June 2018).

Minister reiterates the independence and effective criminal investigations, including the conduct of an OCI.

However, the admonition cannot be said to cut across all ministers of police because a former Minister of Police attempted to whittle down the independence of IPID in some ways, such as suspending the Executive Director of IPID.[2021] Worse still, the National Assembly which should have been seen as a neutral and oversight authority —through its National Assembly Committee on Police— was allegedly reported to have subjectively considered the non-renewal of the appointment of the Executive Director of IPID in 2019.[2022]

According to reports, it was alleged that the Minister of Police and the majority of the Committee members sympathised with their colleagues in some political parties and comrades within and outside the SAPS[2023] that the erstwhile Executive Director of IPID investigated or was investigating,[2024] thus the alleged reason for the non-renewal of his appointment.

Furthermore, the power of IPID to directly refer criminal matters to NPA for the prosecution of SAPS members and only notify the Minister of Police of the decision of IPID demonstrates high-level independence of IPID in policing the police[2025] because the Minister is not required to consent to the prosecution.

The transparency, integrity, and independence of IPID in its operation, including the conduct of an OCI, are assured in some ways. Firstly, the requirement that members should declare any interest in a matter before the Directorate is fundamental and adequate.[2026] Secondly,

---

[2021] *Suzman Foundation v Min of Police* para 66.

[2022] Phakathi B 'Police committee agrees on not renewing Robert McBride's contract as IPID boss- DA MPs have criticised the Committee's decision and boycotted the session during which the report was adopted' https://www.timeslive.co.za/politics/2019-02-28-police-committee-agrees-on-not-renewing-robert-mcbrides-contract-as-ipid-boss/ (Date of use:8 March 2019) **(**Phakathi https://www.timeslive.co.za/politics/2019-02-28-police-committee-agrees-on-not-renewing-robert-mcbrides-contract-as-ipid-boss/ (Date of use: 8 March 2019**)**

[2023] It is noted that though s 199(6) of the Constitution prohibits police officers from being politically partisan, however, on the other hand, the reigning political party, ANC, is in alliance with trade unions comprising police union whose members are regarded as a comrades or colleagues at this level, see Eye Witness News 'Tripartite alliance to work together to ensure 'massive' 2019 election victory' https://ewn.co.za/2018/07/10/tripartite-alliance-to-work-together-to-ensure-massive-2019-election-victory (Date of use: 8 March 2019); Cosatu 'Tripartite Alliance' http://www.cosatu.org.za/show.php?ID=2051 (Date of use: 8 March 2019).

[2024] Phakathi https://www.timeslive.co.za/politics/2019-02-28-police-committee-agrees-on-not-renewing-robert-mcbrides-contract-as-ipid-boss/ (Date of use: 8 March 2019).

[2025] Section 7(4) and (5) of the IPIDA.

[2026] Section 7(3)(d) and 25 of the IPIDA.

undesirable elements are excluded from being part of IPID due to the requirement of continuous and random compliance with security check and clearance and random entrapment or tests of its members, though not at the whims and caprices of the Minister of Police,[2027] failing which such IPID member is discharged from IPID service.

Because IPID receives funding directly from the National Assembly,[2028] it guarantees its independent operations, including the conduct of an OCI.

4.4.5 Operation and funding of the State Security Agency in the conduct of online criminal investigation

In furtherance of its mandate, the SSA through its transformative goal adopts some policies to ensure effective criminal investigation in its operations.[2029]

The offices of the two heads of the ID-SSA in charge of domestic and foreign divisions respectively are, to some extent, regulated under the PSA, which arguably does not cater for the specific or internal operational needs of the SSA including the operation, administration, and conduct of an OCI by ID-SSA save in circumstances where exceptions are granted.[2030] Generally, some cases of in-fighting and rancour have been recorded in the operations of the SSA.[2031] Nevertheless, the regulation of operational policy of SSA in virtually every issue is

---

[2027] Sections 8(3), (4), (5), (6), (7) and (8), 22(3), (4), (5), (6) and (7) and 26 the IPIDA; *Suzman Foundation v President of the RSA in*: *Glenister v President of the RSA* supra 43 and 180.

[2028] Sections 3(3) and 7(1) of IPIDA.

[2029] Sections 17 and 22(e) of GILAA *II* establishes TFA replacing the South African National Academy of Intelligence; SSA 'White paper on intelligence' http://www.ssa.gov.za/Portals/0/SSA%20docs/Legislation/White%20Paper%20on%20Intelligence.PDF (Date of use: 21 January 2014); Section 2(a) and (b) of GILAA *II*; Section 11 (2)(b)(i)-(iv) of ISA No. 65 of 2002; Section 2(1)(b) of the NSIA No. 39 of 1994; Section 2(e) of GILAA *II* and the equivalent provisions in section 2 of NSIA 39 of 1994, section 2 of NSIAA 37 of 1998 and section 2 of NSIAA 67 of 2002; Section 2(e) of the GILAA *II* and the equivalent provisions in section 2 of NSIA No. 39 of 1994, section 2 of NSIA 37 of 1998 and section 2 of NSIA 67 of 2002; Section 2(f) of the GILAA *II* and the equivalent provisions in section 2 of NSIA 39 of 1994, section 2 of NSIA 37 of 1998 and section 2 of NSIA 67 of 2002.

[2030] Section 15 (3), (b), (c)(ii) & (5)(a)(iii)&(iv) of RICA; Sections 4 and 5 of NSIA 39 of 1994 and sections 3 and 4 of ISA 65 of 2002; Ministry of State Security 'Statement on Recent Developments Relating to the Management of State Security Agency' (02 august 2013) which announced the appointment into the offices of Director-General, heads of ID-SSA and other senior positions in SSA http://www.ssa.gov.za/Portals/0/SSA%20docs/Media%20Releases/2013/Media%20Release%20Statement%20on%20recent%20developments%20relating%20to%20the%20State%20Security%20Agency%202%20August%202013.pdf (Date of use: 14 October 2013).

[2031] Right2Know at 2, 10-11 and 35 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

jointly formulated by SSA in consultation with the JSCI of Parliament[2032] which guarantees checks and balances in this regard, which should include the policy on the administration and conduct of an OCI.

However, the approval by the Minister of State Security of the powers of the Director-General to control the operation, superintendence, and functioning of the SSA[2033]—as the central authority coordinating intelligence matters with the support of the National Intelligence Structure—[2034] does not guarantee the operational independence of the SSA, arguably including the administration and conduct of an OCI. The dependence of the SSA on the Minister is due to the fusion of power of the Minister of State Security who formulates operational policies and yet dictates to the Director-General on the execution of those policies.[2035]

Before the introduction of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, the expunged provisions of the CCB stipulated that the Minister of State Security would have been responsible for the establishment, development, security and regulation of operational capacity of critical information infrastructure of government in pursuance of the provision of the Constitution.[2036] These provisions failed to consider the security and operational competence of the Director-General in lieu of that of the Minister. The provisions also fail to consider the principles of separation of powers and check and balances in the powers of the Minister of State Security by excluding the Parliament in the formulation of the regulation.

[2032] Section 7 of the GILAA *II* and section 6 of the NSIA 39 of 1994; ISOA No. 40 of 1994.

[2033] Sections 22 and 24 of the GILAA *II* and sections 10 and 12 of ISA 65 of 2002 as amended by sections 9 and 11 of the ISA 52 of 2003; Hartley http://www.bdlive.co.za/national/2013/08/08/single-intelligence-body-wields-great-power (Date of use: 28 February 2014; Sections 1(b) -(h) and (k), 2,(a),(b), (c) and (e) and section 5 of the GILAA *II*; Department of State Security 'Structure of the State Security Agency' http://www.ssa.gov.za/Branches.aspx (Date of use:18 January 2014).

[2034] Sections 2(a)-(g), 3 and 15 of the GILAA *II*. In section 2(1)(b)(iii) of the NSIA 39 of 1994, SSA supplies intelligence (where necessary) to SAPS on the investigation of any offence allegedly committed, Hartley http://www.bdlive.co.za/national/2013/08/08/single-intelligence-body-wields-great-power (Date of use: 28 February 2014).

[2035] Sections 22 and 24 of the GILAA *II* and ss 10 and 12 of the ISA No. 65 of 2002 as amended by sections 9 and 11 of ISA 52 of 2003; Hartley http://www.bdlive.co.za/national/2013/08/08/single-intelligence-body-wields-great-power (Date of use: 28 February 2014); Sections 1(b)-(h) and (k), 2,(a),(b), (c) and (e) and section 5 of GILAA *II*; Department of State Security 'Structure of the State Security Agency' (Date of use: http://www.ssa.gov.za/Branches.aspx (Date of use:18 January 2014).

[2036] Section 54(1) (a) (i), (ii) & (b) of the CCB B6-2017 is expunged in CB 2018-Amendments Proposed to Bill B6-2017.

In order to ensure a general independent, transparent, impartial and competent investigating authority and specifically ensure the existence of an authority that will effectively conduct an OCI,[2037] the operation of the SSA should implement the policy on the declaration of conflict of interest of members[2038] and execution of initial, continuous and post-service declaration—including restraint of trade after service—[2039] or vetting and confidentiality tests and processes.[2040] This approach is to safeguard the fundamental concept of covert investigation, which should be extended to the operation of an OCI.

Due to the crucial nature of the function of the SSA, the provision for the limitation of the constitutional right of members to strike[2041] complies with the principle of checks and balances of the operations of the SSA. This limitation regulates unnecessary strike actions in a sensitive sector like the SSA such that criminal investigation —including the conduct of an OCI— is not compromised or hampered.

Given that the Minister of State Security makes regulations in consultation with the JSCI of Parliament on the control and administration of funds appropriated to SSA[2042] guarantees the 'check and balance' in the funding of the SSA.[2043] In the report by JSCI of Parliament, it was recommended that the funding module of the SSA be reviewed.[2044] It is submitted that such review should be geared towards guaranteeing the financial independence of the SSA, without ignoring the 'check and balance' principle to prevent a repetition of the financial misappropriation of the secret or slush fund by members of CI-SAPS[2045] in the SSA.

[2037] In South Africa, the danger of abuse of intelligence machinery was revealed in the IGI NIA 'Investigations on Mr. Macozoma' at 8, 13, 18, 19 and 24.

[2038] Section 35 of the GILAA *II* and section 23(3)(a) of the ISA 65 of 2002.

[2039] Sections 39, 40 and 43 of the GILAA *II* and sections 27, 28(1) and 31 of the ISA 65 of 2002.

[2040] Sections 3, 7, 26 and 48(e) of the GILAA *II* and section 14 and s 37(1)(s) of the ISA Act 65 of 2002 and section 2A and 6 of the NSIA 39 of 1994 (as amended by section 3 of the NSIA 67 of 2002 and section 2 of the GILAA *1*). Section 2(f) of the GILAA *II* and the equivalent provisions in section 2 of the NSIA 39 of 1994, section 2 of the NSIA 37 of 1998 and section 2 of the NSIA 67 of 2002, sections 3(c) and (e) and 10(f) of the GILAA *II*.

[2041] Sections 23(2)(c) and 36 of the 1996 Constitution, section 33 of GILAA *II* and section 21(1) of ISA 65 of 2002. IOL News 'SANDF Members protest at the Union Buildings' http://www.iol.co.za/news/sandf-members-protest-at-the-union-buildings-1.676456 (Date of use: 18 June 2012).

[2042] Section 48(c) of the GILAA *II* and section 37(1)(m) of the ISA 65 of 2002 (as amended by section 16 of the GILAA *I*).

[2043] Section 48(c) of the GILAA *II* and section 37(1)(m) of the ISA 65 of 2002 (as amended by section 16 of the GILAA *I*).

[2044] Parliament of the Republic of South Africa 'Announcement, Tablings and Committee Reports' No 164 -2016 4.7.4 at 22.

[2045] Mitchley https://www.news24.com/SouthAfrica/News/crime-intelligence-boss-position-up-for-grabs-20180117 (Date of use: 16 November 2018).

Aside from the foregoing examination and the provisions of RICA, there is no specific, published, and complementary legal framework that regulates the operation, administration, and conduct of FOCI[2046] in RICA, law or policy, thus, opens the door for abuse by the SSA in the conduct of an OCI.[2047]

4.4.6 Operation and funding of the Defence Intelligence of South African National Defence Force in the conduct of online criminal investigation

The DI-SANDF complies with the operational and defence intelligence policy and strategy and the provisions of the NSIA[2048] which ensure checks and balances in its operations, which should include the conduct of an OCI.

For security reasons, the intelligence operations and programmes of the DI-SANDF may not be available to the public.[2049] However, concerns have been raised in some quarters on the need for the intelligence cluster to be transparent and impartial in the publication of their policy[2050] and not abuse their powers under the guise of confidentiality, particularly in the conduct of an OCI, which is being abused by other LEAs.[2051] However, from available reports from the public domain, there is no public complaint against the DI-SANDF thus far for the unlawful conduct of an OCI.

In its operation, a conflict of interest must be declared by senior officials of SANDF as public servants[2052] which arguably, should include a declaration by the head and members of DI-

---

[2046] Parliament 'Annual Report of the Joint Standing Committee on Intelligence for the financial year ending 31 March 2017' 7 and 11.

[2047] Para 2.10 of Chapter 2 of this study.

[2048] Section 34(b)(i) of the DA No. 42 of 2002. Sections 32 and 33 of the DA No. 42 of 2002; Section 1 of NSIA 39 of 1994. The Intelligence Division of SANDF gathers only foreign military intelligence and shall not gather intelligence that is non-military in a covert manner, see section 2(4)(a),(b) and (c) of NSIA 39 of 1994; De Wet http://mg.co.za/article/2012-05-04-lack-of-funds-leaves-sa-vulnerable (Date of use:12 October 2013 and Oxford Analytica 'South Africa Army Incapacity Mars Foreign Policy Goals' https://www.oxan.com/display.aspx?ItemID=DB190015 (Date of use: 15 April 2014) (Oxford Analytica https://www.oxan.com/display.aspx?ItemID=DB190015 (Date of use: 15 April 2014).

[2049] Department of Defence and Military Veterans 'Annual Report FY 2012/13' at 89. http://www.dod.mil.za/documents/annualreports/Annual%20Report%202013%20Final.pdf (Date of use: 12 March 2014).

[2050] Duncan J 'The Politics of South Africa's Intelligence Priorities' http://www.polity.org.za/article/the-politics-of-south-africas-intelligence-priorities-2013-10-01 (Date of use: 2 December 2013). See para 7.5 of this study.

[2051] See the opening statement of para 4.3.2 of this chapter.

[2052] Public Service Commission 'Chapter 3 of the Public Service Regulation 2001' http://www.psc.gov.za/documents/docs/legislation/PUBLIC%20SERVICE%20REGULATIONS.pdf (Date of use: 12 March 2014); Department of Public Service and Administration 'Senior Management Service

SANDF to ensure an impartial administration and conduct of an OCI.

A reasonable level of competence is achieved by the DI-SANDF in the institutionalisation of cybersecurity,[2053] which includes the improvement of the knowledge and understanding of the timeous, relevant and credible electronic vetting processes and intelligence gathering of SANDF members including the DI-SANDF members[2054] when conducting an OCI.

The requirement that regular members including members of DI-SANDF should render full service to SANDF[2055] guarantees competence and resourcefulness which promote effective criminal investigation, including the conduct of an OCI where required.

According to military sources, reports suggest that the DI-SANDF is inadequately funded[2056] which may adversely affect its intelligence-gathering competence, including the conduct of an OCI.

In summary, aside from the general provisions of RICA, there is no specific, published, and complementary legal framework that internally regulates the operation, administration, and conduct of an OCI by the DI-SANDF.[2057]

Handbook Chapter 9 Disclosure of Financial Interest 1/12/2003' http://www.dpsa.gov.za/dpsa2g/documents/sms/publications/CH9_SMS_2003.pdf (Date of use: 12 March 2014); Department of Defence and Military Veterans 'Annual Report FY 2012/13' at 159 http://www.dod.mil.za/documents/annualreports/Annual%20Report%202013%20Final.pdf (Date of use: 12 March 2014).

[2053] Department of Defence and Military Veterans '*Annual Report FY 2012/13'* at 89; National Defence Force Intelligence Division 'Intelligence' http://www.globalsecurity.org/intell/world/rsa/df_id.htm (Date of use: 12 January 2014).

[2054] Department of Defence and Military Veterans '*Annual Report FY 2012/13'* at 89; National Defence Force Intelligence Division 'Intelligence' http://www.globalsecurity.org/intell/world/rsa/df_id.htm (Date of use: 12 January 2014).

[2055] Section 52(5) of DA No. 42 of 2002.

[2056] Department of Defence and Military Veterans 'Annual Report FY 2012/13' at 89 http://www.dod.mil.za/documents/annualreports/Annual%20Report%202013%20Final.pdf (Date of use: 12 March 2014). In April 2014, it was reported that the SANDF lacks the capacity to carry out its mandate due to insufficient funding, De Wet http://mg.co.za/article/2012-05-04-lack-of-funds-leaves-sa-vulnerable (Date of use: 12 October, 2013 and Oxford Analytica https://www.oxan.com/display.aspx?ItemID=DB190015 (Date of use: 15 April, 2014).

[2057] Parliament 'Annual Report of the Joint Standing Committee on Intelligence for the Financial Year ending 31 March 2017' 6.

4.4.7 Operation and funding of the Investigating Directorate of the National Prosecuting Authority in the conduct of online criminal investigation

The ID-NPA[2058] is insufficiently independent in its operations in some ways.

Firstly, the President, on the recommendation of the Minister of Justice and the National Director of the NPA and to the exclusion of the head of ID-NPA, submits its report to the National Assembly on the finalisation of which offences in National Prosecuting Authority Act are set out in the Proclamation.[2059] The exclusion of the head of ID-NPA limits its powers by not having a close opportunity to contribute to the categorisation of offences in the Proclamation regarding the statistics of which serious offences record high commission rate, particularly for the purpose of conducting an OCI.[2060]

Secondly, the National Director of the National Prosecuting Authority and the ID-NPA are not included in the process of making the regulations affecting the NPA.[2061]

Thirdly, in as much as the head of ID-NPA does not need any authorization from the National Commissioner of the SAPS to conduct criminal investigations —including the conduct of an OCI, which is the essence of the independent powers of the six LEAs to conduct an OCI in RICA—[2062] the head of ID-NPA is mandated to inform the National Commissioner of the SAPS in this regard.[2063] This provision is for and against the independence of the ID-NPA.

The argument for the independence of the ID-NPA in this regard is that, though a notice to the National Commissioner of the SAPS is not the same as the words 'approval', consent or 'consultation' which require some agreement, however, the ID-NPA can still exercise this power without any interference by the National Commissioner of the SAPS.

The argument against the independence of the ID-NPA in this regard is that, there is the likelihood of interference of the process by the Office of the National Commissioner of the

[2058] Sections 199(1) and 205 (3) of the Constitution, 26 and 28(1)(d) of NPAA and para 8 of the Prosecution Policy of NPA reiterate the primary function of SAPS.
[2059] Section 7(1), (2) and (3) of the NPAA.
[2060] Para 6.3 of Chapter 6 of this study.
[2061] Section 40(3)(a) of the NPAA.
[2062] See the definition of 'Applicant' in section 1 of RICA.
[2063] Section 28(1) (d) & (2)(a) of the NPAA.

SAPS if there is a vested interest in the investigation by the ID-NPA.[2064] For example, the investigation of some members of the SAPS by IPID is a good example in this regard whereby the information given by ID-NPA to the National Commissioner of SAPS arising from the IPID investigation may be interfered with.[2065]

Fourthly, given that ID-NPA is a directorate under the NPA as opposed to the defunct 'Scorpions' which was sufficiently, largely and relatively independent of the NPA, the general powers of the head of ID-NPA are subject to the control and direction of the National Director of NPA.[2066] In some instances, it is arguable that section 179(6) of the Constitution which vests a mandatory final responsibility of the NPA on the Minister of Justice, is broad and diminishes the independence of NPA as a whole. Worse still, it is argued that the sacrosanct prosecutorial and discretionary independence of the NPA was also diminished when the court compelled the NPA to reinstate the criminal charges against a former president of the RSA, Mr. Jacob Zuma.

Arguably, the court, with due respect, misdirected itself by not jurisprudentially juxtaposing the sacrosanct independence of the NPA to prosecute in this regard and the equally sacrosanct right of a dissatisfied complainant to alternatively embark on a private prosecution, which though is a regrettably expensive venture in terms of time and capital under the current law. In other words, does the decision or jurisdiction of the court not abrogate independence of the NPA; in the alternative, or does this decision constitute another exception to the independence of the NPA?

Furthermore, the ID-NPA conducts investigation based on a request from the DPCI or HAWKS on national priority offences.[2067] This request reiterates the constitutional principle of cooperative governance[2068] and the success story recorded by the defunct Scorpions.[2069]

[2064] Right2Know at 2 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[2065] Chabalala J 'EXCLUSIVE: McBride 'begged' ex-NPA boss to prosecute IPID cases for months, Abrahams denies 'baseless' claims' https://www.news24.com/SouthAfrica/News/exclusive-mcbride-begged-ex-npa-boss-to-prosecute-ipid-cases-for-months-abrahams-denies-baseless-claims-20190302 (Date of use: 14 April 2019).

[2066] Sections 5(2)(a), 7(2)(a) and (b) and (3), 22, 24(2) and 33 of the NPAA.

[2067] See ss 7(3), 26(2) and 28(1)(d) of NPAA; *SAPS v Zim & Dugard* supra 58.

[2068] Chapter 3 of 1996 Constitution. Sections 17D (3) of SAPS Act and 13(1)(c) and 24(7) of the NPAA; In *SAPS v Zim & Dugard* supra 58 and 59, ID-NPA can request SAPS for further investigation of a crime; Sections 32(5), 34(1), (3) & (4) of RICA.

[2069] Schönteich M 'A story of trials and tribulations -The National Prosecuting Authority, 1998 – 2014' *SA Crime Quarterly* No. 50 at 7; IOL 'NPA is the picture of success, says Ngcuka' https://www.iol.co.za/news/politics/npa-is-the-picture-of-success-says-ngcuka-205848 (Date of use: 7

However, it exposes the weakness in the operation and administration of HAWKS, which is a specialised LEA in charge of priority crime, unlike the CI-SAPS which is in charge of general crime investigation. Rather, the establishment of a joint team would ensure that both parties — the ID-NPA and the HAWKS— significantly play their roles regarding the cooperative investigation.

The head of the ID-NPA exercises some powers in the execution of its duty. Firstly, it exercises its discretion to determine the procedure to be followed in the investigation according to each case.[2070] Secondly, the ID-NPA enjoys some degree of independence with the power to enter upon premises, and summon witnesses to give evidence and failure to respond positively constitutes an offence.[2071] Thirdly, the ID-NPA participates in the process of issuing policy directives.[2072]

In order to ensure impartiality and protect its integrity in the operation, the ID-NPA —like any member of the NPA— declares both direct and indirect interests in any business within and outside the country in addition to the enforcement of a declaration on oath of the impartiality of the performance of their duties.[2073]

To ensure competence in their operation, the ID-NPA engages the services of support staff and other persons in consultation with the National Director of NPA and Minister of Justice.[2074]

Since the ID-NPA is a unit under the NPA, its funding is obtained from the appropriation fund approved by the National Assembly to the NPA.[2075] However, this practice does not give sufficient independence to the ID-NPA in this regard.

February 2019). It is however noted that in 2018, the SCA heard an appeal by a former prosecutor of NPA, see *Famanda v State* (930/2017) [2018] ZASCA 139 para 12 (*Famanda v State*).

[2070] Section of 28(4) and (5) of the NPAA.

[2071] Sections 28(6), (7), (8) and (10) and 29 of the NPAA.

[2072] Section 21 of the NPAA and CPA and Commentary Service No 34, 2005 at Prosecuting-41.

[2073] Sections 32 and 39 of the NPAA; Non-compliance with section 32(1)(b) is an offence in section 41 of the NPAA. See Code of Conduct for Members of the NPA under section 22(6) of NPAA 32 of 1998 published under GN R1257 in GG 33907 of December 2010 at paras A, B and C.

[2074] Sections 7(4), 24(2), 37 and 38 of the NPAA.

[2075] Section 36(1) and (2) of the NPAA.

In conclusion, aside from the general provisions of RICA, there is no specific, published, and complementary legal framework that internally regulates the operation, administration, and conduct of an OCI by ID-NPA.

4.4.8 Conclusion

In the operation, administration, and conduct of an OCI by the six categories of LEAs recognised in RICA, none of the LEAs has any specific, published, and complimentary internal policy document that regulates the operation, administration, and conduct of an OCI.

Save for the IPID which receives its funding directly from the appropriation fund approved by the National Assembly; the CI-SAPS, HAWKS, SSA, DI-SANDF and ID-NPA are not independent in their funding. Therefore, there is a likelihood that their dependence will adversely impact the effectiveness and efficiency of these LEAs in conducting an OCI in these regards.

4.5 ACCOUNTABILITY AND OVERSIGHT OF LAW ENFORCEMENT AGENCIES IN THE CONDUCT OF ONLINE CRIMINAL INVESTIGATION

4.5.1 Introduction

Drawing on the belief that says that the possession of power constantly tempts one to want to abuse power absolutely,[2076] this segment examines the adequacy or otherwise of the direct and indirect mechanisms and levels of accountability[2077] and oversight of the six categories of LEAs or LEOs[2078] as specialised investigative, security or intelligence services in the conduct of an OCI. This rubric is in pursuance of the statement of the Constitutional Court in *Suzman Foundation v JSC* which held that all public entities and institutions —which arguably include LEAs— are accountable[2079] provides that:

[2076] Van der Vyver *State secrecy* 48.
[2077] *Primemedia v Speaker, National Assembly* supra 72, 75 and 76.
[2078] Section 199(5) of the Constitution;
[2079] *Suzman Foundation v JSC* supra 64, 65, 66, 98, 187, 211 and 212; *AZAPO v President* para 17 where Mahomed DP says:

> Most of the acts of brutality and torture which have taken place have occurred during an era in which neither the laws which permitted the incarceration of persons or the investigation of crimes, nor the methods and the culture which informed such investigations, were easily open to public investigation, verification and correction.

> The foundational constitutional values of accountability, responsiveness and openness apply to the functioning of the judiciary as much as to other branches of government.[2080]

4.5.2 Accountability and oversight of the Crime Intelligence of South African Police Service in the conduct of online criminal investigation

The Constitution provides for the civilian monitoring of the intelligence services of SAPS and other LEAs by the operation of a multi-party National Assembly structure.[2081] The SAPSA also provides for general oversight function of the SAPS by the Civilian Secretariat of Police Service.[2082] Other bodies which oversee the affairs of CI-SAPS include the IPID[2083] and the A-G.[2084] However, it is arguably presumed that since CI-SAPS is not independent of SAPS, the same oversight authorities oversee the affairs of the CI-SAPS.

The implementation of the National Policing Policy serves as a source of oversight over the operations of CI-SAPS[2085] given the processes that the policy undergoes before implementation. However, the delay in tabling the policy before the Parliament seems to be one of the challenges in the oversight function.[2086]

In the past, the SAPS did not only in its report mislead the oversight body which is the National Assembly Portfolio Committee on Police on the decrease in police corruption —without facts—[2087] but fallaciously posited that it was impossible to compare its high integrity

---

> Much of what transpired in this shameful period is shrouded in secrecy and not easily capable of objective demonstration and proof. . .. Secrecy and authoritarianism have concealed the truth in little crevices of obscurity in our history.

[2080] *Suzman Foundation v JSC* supra 64, 65, 66, 98, 187, 211 and 212 and *AZAPO v President* supra 17.

[2081] Sections 199 (8) and 210 of the Constitution; Gould 2012 40 *SACQ* 40-41; Parliament of the Republic of South Africa 'Announcement, Tablings and Committee Reports' No 164-2016 at 6 and 15.

[2082] Section 3(1)(c) of SAPSA.

[2083] Section 2 of the IPIDA; Maphumulo 'Phiyega facing criminal charges' http://www.iol.co.za/news/crime-courts/phiyega-facing-criminal-charges-1.1597315#.U2jYZ08aLMw (Date of use:13 March 2014).

[2084] Bruce D 'Measuring Output, Neglecting Outcomes-The Auditor-General's Role in SAPS Performance Assessment' 2011 38 *SACQ* 3 at 7-9; In the 2017 JSCI report, although there was no identification of the non-compliance with statutory provisions, the Auditor-General assessed the account of CI-SAPS as a qualified account, Parliament 'Annual Report of the Joint Standing Committee on Intelligence for the Financial Year ending 31 March 2017' 17-18.

[2085] Section 207 (1) and (2) of the Constitution; Montesh *Crime investigative system* at 118.

[2086] Gould 2012 40 *SACQ* 41.

[2087] Faull *ISS* Paper 227 at 10; United Nations Office on Drugs and Crime *Handbook on police accountability, oversight and integrity* (2011) at 21-32 and 117 –130 (United Nations Office on Drugs and Crime *Handbook on police accountability, oversight and integrity*).

framework with the international anti-corruption strategy.[2088] However, on the contrary, international standards are available to prove otherwise.[2089] Supplying false information to an oversight body is worrisome, thus it is an indication —no matter how weak the indication might be— that SAPS may not be forthcoming in supplying information to the oversight authorities, which arguably includes information on the conduct of an OCI, particularly the unlawfully conducted OCI.

At the end of every financial year, the Minister of Police submits a report to the National Assembly indicating the: level of progress on the implementation of support for cybersecurity relating to government online structures; the number of offences committed and prosecuted under the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017 and reported to SAPS; the number of unprosecuted cases after reporting to SAPS and number of SAPS members who underwent training.[2090]

Finally, the provisions of RICA specifically apply to all the six categories of LEA in terms of the adjudication and non-adjudication of an OCI application and interception respectively and reporting to the court in the foregoing instances[2091] and the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017. However, the provisions on the accountability and oversight of the CI-SAPS examined above are general provisions which do not cater for the accountability and oversight of the CI-SAPS in the conduct of an OCI. Accordingly, there is no other specific, published, and complementary legal framework that regulates the accountability and oversight of the operation and administration of CI-SAPS in the conduct of an OCI.

4.5.3 Accountability and oversight of the Directorate of Priority Crime Investigation in the conduct of online criminal investigation

The National Assembly is empowered to conduct civilian monitoring of the activities of the DPCI or HAWKS,[2092] which should include the conduct of an OCI.

[2088] This misrepresentation was made in the time of former convicted national commissioner of SAPS, Jackie Selebi, Faull *ISS* Paper 227 at 10.
[2089] United Nations Office on Drugs and Crime *Handbook on police accountability, oversight and integrity* (2011) at 21-32 and 117 - 130.
[2090] Section 54(2)(c)(i), (ii)(aa)-(cc) & (iii) of the CCB B6-2017, which is replaced by s 55(1)(3)(a), (b)(i) -(iii) & (3)(c) of the CB 2018 -Amendments Proposed to Bill B6-2017.
[2091] Sections 7 (3), (4) & (6) and 8 (4) (a) -(c) and 20 of RICA.
[2092] Section 17K (1) of the SAPSA.

Where there is a conflict between the head of the Hawks and National Commissioner of SAPS, the Minister mediates, which is a fair oversight of the activities of the HAWKS by the Minister in the executive circle.

On the financial oversight of HAWKS, although section 17K(2B) of SAPSA allows the head of Hawks to make a presentation to the National Assembly on its budget, section 17H does not give the Hawks sufficient financial independence because it is still tied to SAPS under section 17H (4) of SAPSA.

Finally, aside from the provisions of RICA,[2093] the provisions on the accountability and oversight of the HAWKS examined above are general provisions which do not cater for the accountability and oversight of the HAWKS in the conduct of an OCI. Accordingly, there is no other specific, published, and complementary legal framework that regulates the accountability and oversight of the operation and administration of the HAWKS in the conduct of an OCI.

4.5.4 Accountability and oversight of the Independent Police Investigative Directorate in the conduct of online criminal investigation

Aside from the specific monthly, bi-annual and annual reports submitted by the Executive Director of IPID to the Minister, and the National Assembly on various subject matters;[2094] the Executive Director reports to the Minister of Police, and the National Assembly were required to do so by any of the duo.[2095] It is submitted that this provision mandating a report to be submitted to the Minister is overtaken by the judgement of the court in *McBride v Minister of Police* which reinstates the enforcement of the principle of separation of powers between the duo.[2096]

From the financial aspects of the oversight of the IPID, the Executive Director is responsible under the PFMA to comply with the provisions as may be required while there is an oversight

[2093] See para 4.5.2 of this chapter.
[2094] Section 7(7), 9(j) and (n) and 32(1)-(3) of the IPIDA.
[2095] Section 7(12) of the IPIDA.
[2096] *McBride v Minister of Police* supra 58.

function of the IPID in the Auditor-General's report to the National Assembly.[2097] In a way, the Auditor-General is mandated to make the IPID account for the budget dedicated to the conduct of an OCI.

It is the obligation of the Executive Director to publish the annual financial and audit reports of IPID for public scrutiny.[2098] These provisions are adequate to highlight the accountability and oversight function by the Minister, A-G, National Assembly and the public. It is submitted that since there is a general and adequate accountability provision for IPID, the similar result should be expected in the accountability of the conduct of an OCI by IPID.

However, in overseeing the affairs of IPID, there seems to be a conflict concerning making regulations under the Act. In section 7(3) (e) (i) of the IPIDA, exclusive power is given to the Executive Director to issue guidelines on investigation and management of cases. However, in section 34 of IPIDA, the Minister of Police is empowered, after consultation with the Executive Director and scrutiny by the National Assembly, to make regulations on a wide range of activities by the IPID.

Though a slight conflict may be created in these provisions between the Executive Director and the Minister, the role of National Assembly in section 34 would settle the issues that may arise from any conflict so that criminal investigation is not affected particularly in the conduct of an OCI.

In conclusion, aside from the provisions of RICA,[2099] the provisions on the accountability and oversight of the IPID examined above are the general provisions which do not cater for the accountability and oversight of the IPID in the conduct of an OCI. Accordingly, there is no other specific, published, and complementary legal framework that regulates the accountability and oversight of the operation and administration of the HAWKS in the conduct of an OCI.

[2097] Section 31 of the IPIDA.
[2098] Section 32 (4) of the IPIDA.
[2099] See para 4.5.2 of this chapter.

4.5.5 Accountability and oversight of the State Security Agency in the conduct of online criminal investigation

The oversight function of the SSA is established in the Constitution and legislation including the ISOA,[2100] all of which highlights the adequacy or otherwise of the direct and indirect roles of stakeholders in diverse ways in the respective accountability and oversight of and by the SSA in the National Assembly and other authorities, entities and interests and mechanisms.

Firstly, in carrying out the accountability and oversight function of SSA by the National Assembly, members of the JSCI make an oath of confidentiality, meet in secret for their usual gathering and submission of a report from other bodies and submit an annual report to the National Assembly with expunged classified information.[2101]

Although the confidentiality and secrecy practices in these regards might be considered to be counter accountability because the oversight authorities are secretive, however, for purposes herein, it reiterates the protection of the right to the SOC of individuals whose information must be kept secret despite the conduct of an OCI on such individuals.

Therefore, the practice of accountability does not mean unnecessary publicity, transparency or openness where there is no need to be, more particularly in this instance where the National Assembly members may not need to know the details of targets that an OCI has been conducted on, save in exceptional cases. Accordingly, these provisions are adequate to not only make LEAs accountable to the National Assembly in the conduct of an OCI but to ensure that the oversight authorities are reciprocally accountable themselves as it is further demonstrated below.

Accountability and oversight of the SSA by the National Assembly is strengthened by both the proportional representation of the multi-political party system representing diverse interests[2102] and the stringent conditions required for the membership of the committee including security

[2100] Section 210 of the Constitution and section 3(a)(iii) Intelligence Services Oversight Act 40 of 1994 ('ISOA').

[2101] Hartley W 'Loopholes in Interceptions Law 'Raise Red Flag' available at http://www.bdlive.co.za/national/2014/03/25/loopholes-in-interceptions-law-raise-red-flag (Date of use: 28 March 2014).

[2102] PMG 'Report of the Joint Standing Committee on Intelligence on activities of the Committee after 5 months of establishment, as stipulated in the Intelligence Services oversight Act 40 of 1994, dated 10 February 2015' https://pmg.org.za/tabled-committee-report/2307/ (Date of use: 5 April 2016).

clearance before taking up the appointment as a member, which is reciprocal in a way to ensure that the oversight authorities are also accountable. This is partially because the JSCI does not only receive the report from the SSA, but it is expected to perform oversight functions on other intelligence matters.[2103]

In a way, the proportional representation principle addresses the concern on the over-confidence placement on the National Assembly or their committees as the check and balance in the conduct of an OCI and protection of the right to the SOC. Because of the culture of a broad debate on issues in the National Assembly which should include issues on the regulation of the conduct of an OCI, the principle prevents or reduces the abuse of power by a dominant political party or a coalition of parties. The more the debate, the better the transparency, checks and balances and impartiality in dealing with intelligence issues, including the conduct of an OCI.

However, the proportional representation of members of the political parties in the National Assembly or the JSCI may not always yield a positive result in a debate, and decision.[2104] This is because the dominant party in the National Assembly or Committee may take advantage of its majority membership to out-vote any issue that they are opposed to, including issues relating to the conduct of OCI. For example, at the 2019 consideration of the renewal of the Executive Director of IPID, the majority party, the ANC, used its majority vote to outvote other parties by subjectively refusing to favourably consider the renewal of the appointment of the Executive Director.[2105] Nonetheless, other oversight authorities, entities and mechanisms are available to serve as checks and balances in making the SSA accountable.

[2103] Sections 1(l), 3 and 26 of GILAA *II* and sections 2, 3, 4, 5 and 6 of ISOA 40 of 1994 (as amended by sections 2 and 3 of Act 31 of 1995, sections 2 and 3 of Intelligence Services Control Amendment Act 42 of 1999(ISCAA 42 of 1999), sections 2 and 3 of Intelligence Services Control Amendment Act 66 of 2002(ISCAA 66 of 2002), section 61 of RICA No. 70 of 2002 and sections 4 and 5 of GILAA *I*); section 6 of NSIA 39 of 1994; Joint Standing Committee on Intelligence at para 3.8 http://www.pmg.org.za/docs/2011/comreports/110921jcintelligencereport.htm (Date of use: 13 October 2103); Mukadam S and Van Vuuren H 'Written submission: General Intelligence Laws Amendment Bill [B25-2011]' at 2 and 5 http://db3sqepoi5n3s.cloudfront.net/files/docs/120322iss_1.rtf (Date of use: 3 March 2013); South African History Archives at 4 http://db3sqepoi5n3s.cloudfront.net/files/docs/120322saha_1.pdf (Date of use: 17 July 2013); L Nathan 'Lighting up the intelligence community: An agenda for intelligence reform in South African' African Security Review 18.1 *Institute for Security Studies* at 94 http://www.issafrica.org/uploads/18NO1FULL.PDF (Date of use: 6 June 2013).

[2104] Section 2(1) and (2) of ISOA 40 of 1994.

[2105] Phakathi https://www.timeslive.co.za/politics/2019-02-28-police-committee-agrees-on-not-renewing-robert-mcbrides-contract-as-ipid-boss/ (Date of use: 8 March 2019).

Secondly, the SSA and National Assembly are not only held accountable in the conduct of an OCI as demonstrated in the first point above, the court and other oversight authorities are also held accountable in pursuance of the accountability of the SSA. The interception judge is required to submit a report bothering on the SSA to the National Assembly JSCI,[2106] which should include a report on the conduct of OCI.[2107]

In addition, the authorities in the Public Audit Act are also held accountable through the JSCI which considers reports under the Public Audit Act relating to intelligence,[2108] which should include the report on the conduct of an OCI, keeping in mind that audit is not limited to finance or funding only.

Thirdly, before the introduction of the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017, which expunged the CCB B6-2017, the Minister of State Security —in charge of the SSA— was required to submit a report on the protection of the critical information infrastructure to the JSCI.[2109] It is submitted that the report will include the unlawful conduct of an OCI on the critical information infrastructure.

Fourthly, the provisions of GILAA seem to weaken some of the powers of the Director-General of the SSA or overwhelmingly empower the Minister of State Security in the performance of the oversight function of the latter in some areas.[2110] The Director-General submits an annual report of the activities of the SSA to the Minister of State Security who in turn tables it before the National Assembly.[2111] The report of the Director-General is publicly accessible save for

[2106] Parliament of the Republic of South Africa 'Announcement, Tablings and Committee Reports' No 164-2016 at 15.

[2107] A report was submitted by retired Justice Y Mokgoro to Parliament on the various issues affecting the implementation of RICA. Further, the report also recommends that RICA should be reviewed because it does not respond to technological development and crime commission, see Parliament of the Republic of South Africa 'Announcement, Tablings and Committee Reports' No 164 -2016 at 19-22, more particularly 21.

[2108] Public Audit Act No. 25 of 2004 ('PAA'). Although the nature of the operation of SSA is secretive in nature, the Auditor-General was still able to obtain some of the financial statements, the outcome of which resulted in a qualified audit account, see Parliament 'Annual Report of the Joint Standing Committee on Intelligence for the Financial Year ending 31 March 2017' 20.

[2109] Section 54(1)(c) of the CCB B6-2017, which is expunged in the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017.

[2110] Sections 22(f) of GILAA *II* and section 10(5) of ISA 65 of 2002; Nathan L 'Lighting up the intelligence community: An agenda for intelligence reform in South African' March 2009 18.1 *African Security Review* 91

[2111] Sections 22(f) of the GILAA *II* and section 10(5) of the ISA 65 of 2002; Nathan L 'Lighting up the intelligence community: An agenda for intelligence reform in South African' African Security Review 18.1 *Institute for Security Studies* at 91 http://www.issafrica.org/uploads/18NO1FULL.PDF (Date of use: 6 June 2013) (Nathan http://www.issafrica.org/uploads/18NO1FULL.PDF (Date of use: 6 June 2013).

classified information.[2112] However, the protocol of submitting a report to the Minister of State Security does not avail the Director-General the opportunity of having direct deliberation and transparency with the National Assembly in this regard,[2113] particularly where there is a need for the Director-General to directly, closely and openly relate with National Assembly or its committee.

The approval by the Minister of State Security of the functional directive issued by the Director-General on the applicable conditions of service and human resources of the SSA does not guarantee adequate oversight function on the Director-General despite that the directive is submitted to a different authority which is the ICCS.[2114] This is because these oversight bodies are all within the internal structures of the intelligence cluster and the executive arm of government, in which the Director-General belongs. This is because of the contradictions in these provisions which are as follows.

On the one hand, the law requires that the members of the ICCS function impartially, without bias, fear or prejudice.[2115] However, on the other hand, the members of ICCS are appointed on contract basis solely by the Minister of Intelligence ('SSA') to whom the members of ICCS report their recommendations on the conditions of service of SSA members.[2116] This contradiction seeks to suggest that the Minister of State Security may have a stronghold on the ICCS members or better still, the independence of members of ICCS may not be guaranteed to objectively deal with their oversight function on SSA regarding the directive on conditions of service and human resources of SSA.

This inadequacy or contradiction may adversely impact on the human resource aspect of the conduct of an OCI which is not functionally in existence because, thus far, this study reveals that there is no special, comprehensive and adequate law, policy, directive or regulation on many issues relating to the conduct of an OCI.

[2112] Sections 22(f) of the GILAA *II* and section 10(5) of the ISA 65 of 2002; Nathan 101 http://www.issafrica.org/uploads/18NO1FULL.PDF (Date of use: 6 June 2013).
[2113] Sections 22(f) of the GILAA *II* and section 10(5) of the ISA 65 of 2002; Nathan 101 http://www.issafrica.org/uploads/18NO1FULL.PDF (Date of use: 6 June 2013).
[2114] Sections 22(b) and (c) and section 34 of GILAA *II* and sections 10(1), (2) and (3)(a) of the ISA 65 of 2002.
[2115] Section 22 (6) of the ISA 65 of 2002.
[2116] Section 34 of the GILAA *II* and sections 22 (1), (3) (7) and (8) of the ISA 65 of 2002.

Notwithstanding the foregoing discussion, there is some hope in the oversight of the SSA. Although the Minister of State Security excludes the participation of the Director-General of SSA from the affairs of the Department of State Security in determining the conditions of service of members of ICCS in pursuance of the principle of checks and balances, however the Minister of State Security submits its report to the JSCI and the Minister in charge of Public Service Administration.[2117] As aforesaid, the fact that at least a non-executive arm of government —JSCI, which is a committee of the National Assembly— exercises some oversight authority on the Minister of State Security suffices to ensure accountability of SSA that the minister oversees in this regard.

Fifthly, the office of the Inspector-General also oversees the activities of SSA as an ombudsman in the intelligence community by assisting the JSCI to monitor compliance with the Constitution by the SSA.[2118] The Inspector-General also performs functions that are referred or assigned to it by the President, Minister of SSA or JSCI.[2119] However, it is submitted that the accountability of the Inspector-General itself is compromised if its function is derived on an ad-hoc basis from the trio aforementioned.

Sixthly, in addition to the function of the Inspector-General above, the JSCI serves as the ombudsman for grievances lodged by members of the public on the infringement of rights of their persons or property by the intelligence and non-intelligence authorities.[2120] It is submitted that the rights include the right to the SOC.

[2117] Sections 34 of the GILAA *II*, sections 22 (5) and (9)(a) of the ISA 65 of 2002 and sections 2 and 3 of the ISOA 40 of 1994.

[2118] Section 7 of ISOA 40 of 1994; Joint Standing Committee on Intelligence at para 4.10 http://www.pmg.org.za/docs/2011/comreports/110921jcintelligencereport.htm (Date of use: 13 October 2013); Fazel (2009) 157 *Monograph* 38 and Gould 2012 40 *SACQ* 41.

[2119] Section 7 of the ISOA 40 of 1994; Joint Standing Committee on Intelligence at para 4.10 http://www.pmg.org.za/docs/2011/comreports/110921jcintelligencereport.htm (Date of use: 13 October 2013); Fazel 2009 157 *Monograph* 38 'Who shall Guard the Guards? Civilian Operational Oversight and the Inspector-General of Intelligence' in L Hutton (ed.) To Spy or Not to Spy? 157 *Monograph* 2009 at 38 and Gould 2012 40 *SACQ* 41.

[2120] Sections 1(l), 3 and 26 of the GILAA *II* and sections 2, 3, 4, 5 and 6 of the ISOA No. 40 of 1994 (as amended by sections 2 and 3 of Act 31 of 1995, sections 2 and 3 of the Intelligence Services Control Amendment Act 42 of 1999 (ISCAA 42 of 1999), sections 2 and 3 of the Intelligence Services Control Amendment Act 66 of 2002 (ISCAA No. 66 of 2002), section 61 of RICA and sections 4 and 5 of the GILAA *I*); section 6 of NSIA 39 of 1994; Joint Standing Committee on Intelligence at para 3.8 http://www.pmg.org.za/docs/2011/comreports/110921jcintelligencereport.htm (Date of use:13 October 2103); Mukadam S and Van Vuuren H 'Written submission: General Intelligence Laws Amendment Bill [B25-2011]' at 2 and 5 http://db3sqepoi5n3s.cloudfront.net/files/docs/120322iss_1.rtf (Date of use: 3 March 2013); South African History Archives at 4 http://db3sqepoi5n3s.cloudfront.net/files/docs/120322saha_1.pdf (Date of use:17 July 2013); Nathan L 'Lighting up the intelligence community: An agenda for intelligence reform in South African' African Security

Seventhly, the cooperative function of the SSA with other departments of government including the SAPS and the SANDF particularly in the area of vetting members of the other departments[2121] serves as a standard of assessment and oversight of the SSA by other State organs in this regard.

Finally, the provisions of RICA specifically apply to all the six categories of LEA in terms of adjudication and non-adjudication of an OCI application and interception respectively and reporting to the court in the foregoing instances[2122] and some provisions of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017. However, the provisions on the accountability and oversight of the SSA examined above are general provisions which do not refer to the accountability and oversight of the SSA in the conduct of an OCI. Accordingly, there is no other specific, published, and complementary legal framework that regulates the accountability and oversight of the operation and administration of SSA in the conduct of an OCI.

4.5.6 Accountability and oversight of the Defence Intelligence of South African National Defence Force in the conduct of online criminal investigation

Accountability and oversight directly or indirectly occur in different dimensions in the DI-SANDF, the provisions of which are relatively adequate.

Firstly, the DI-SANDF assists the Chief of SANDF and Secretary of Defence in terms of gathering, collating and evaluating intelligence policy issues subject to the formulation and execution of such policy by Parliament and national executive,[2123] which is adequate because DI-SANDF is involved in this process, where there is a broader consultative forum in this regard.

Secondly, the DI-SANDF is scrutinized by the Inspector-General of the Department of

Review 18.1 *Institute for Security Studies* at 94 http://www.issafrica.org/uploads/18NO1FULL.PDF (Date of use: 6 June 2013).

[2121] Section 2(f) of the GILAA *II* and the equivalent provisions in section 2 of NSIA No. 39 of 1994, section 2 of NSIA 37 of 1998 and section 2 of NSIA 67 of 2002, sections 3(c) and (e) and 10(f) of GILAA *II*.

[2122] Para 4.5.2 of this chapter.

[2123] Section 210 of the Constitution; Sections 2(a), 8(b), 14 (c) and 34 (a), (ii) & (iv) of DA 42 of 2002; Department of Defence and Military Veterans 'Annual Report FY 2012/13' at 178-183 *http://www.dod.mil.za/documents/annualreports/Annual%20Report%202013%20Final.pdf* (Date of use: 12 March 2014); Section 18(5) of DA No. 42 of 2002. It is noted that section 4 of DA 42 of 2002 provides for the oversight of the Secretary for Defence and Chief of Defence Force by Parliament; Section 2(a) of DA 42 of 2002.

Defence, Inspector-General for Intelligence, NICOC and JSCI of Parliament.[2124] Although this provision is adequate to the extent that diverse oversight authorities hold the DI-SANDF accountable, however, because there seem to be many oversight authorities holding the DI-SANDF responsible makes the oversight process complex to serve the purpose it seeks.

Thirdly, the DI-SANDF co-operates with any other intelligence or non-intelligence services or bodies created by or under any other law such as the SAPS, Hawks, Department of Home Affairs, amongst others,[2125] failing which other LEAs and departments will find it difficult to indirectly oversee the activities of DI-SANDF and vice versa.

Fourthly, before the introduction of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, the CCB provided that the Minister of Defence must, on an annual basis, report to the Chairperson of the JSCD of the National Assembly on the progress made regarding the establishment and maintenance of cyber offensive and defence capacity of SANDF and the numbers of SANDF members who have undergone training on cyber offensive and defence capacity.[2126] Although this is an adequate provision because the scope of its functions arguably and substantially caters for the conduct of an OCI, however, the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 expunged this provision.

Finally, the provisions of RICA specifically apply to all the six categories of LEA in terms of adjudication and non-adjudication of an OCI application and interception respectively and reporting to the court in the foregoing instances[2127] and some provision of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017. However, the provisions on the accountability and oversight of SSA examined above are general provisions which do not cater for the

---

[2124] See Le Roux L 'The Post-Apartheid South African Military: Transforming with the Nation' *Evolution and Revolutions* at 259 http://www.issafrica.org/pubs/Books/Evol_Revol%20Oct%2005/Chap9.pdf (Date of use: 6 March 2014). Although the sensitive nature of the operation of the DI-SANDF prevented the Auditor-General from accessing some evidence which gave it a qualified audit, however, the financial statement was fair, Parliament 'Annual Report of the Joint Standing Committee on Intelligence for the Financial Year ending 31 March 2017' 14-15.

[2125] Sections 201 of the Constitution, 35 of DA 42 of 2002 and Department of Defence and Military Veterans 'Annual Report FY 2012/13' at 89 http://www.dod.mil.za/documents/annualreports/Annual%20Report%202013%20Final.pdf (Date of use: 12 March 2014); Sections 19, 29, 35, 92 and 93 of DA 42 of 2002 and Department of Defence and Military Veterans 'Annual Report FY 2012/13' at 89 http://www.dod.mil.za/documents/annualreports/Annual%20Report%202013%20Final.pdf (Date of use: 12 March 2014).

[2126] Section 54(3)(c) of the CCB B6-2017 is expunged by Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017.

[2127] Para 4.5.2 of this chapter.

accountability and oversight of DI-SANDF in the conduct of an OCI. Accordingly, there is no other specific, published, and complementary legal framework that regulates the accountability and oversight of the operation and administration of SSA in the conduct of an OCI.

4.5.7 Accountability and oversight of the Investigating Directorate of National Prosecuting Authority in the conduct of online criminal investigation

The head of the ID-NPA submits its annual report to the National Director of NPA who in turn includes it in its composite report to the National Assembly through the Minister of Justice who has the final responsibility over the NPA,[2128] who should not be responsible for the management of the affairs and activities of the NPA in this regard. Given the seemingly endless crisis in the NPA, it is submitted that the ID-NPA should be statutorily empowered to directly submit its report to the Chairperson of JSCI to ensure the independence and accountability of the ID-NPA.

On behalf of the NPA, the Minister of Justice consults the National Assembly on the determination of the regulation of the NPA.[2129] However, the fact the NPA is not statutorily required to be part of the consultation makes the consultation defective. Furthermore, thus far, there is no publication by the Minister of Justice or any internal authority of ID-NPA on the administration and conduct of an OCI.

Finally, the provisions of RICA specifically apply to all the six categories of LEA in terms of the adjudication and non-adjudication of an OCI application and interception respectively and reporting to the court in the foregoing instances.[2130] However, the provisions on the accountability and oversight of the ID-NAP examined above are general provisions which do not cater for the accountability and oversight of the ID-NPA in the conduct of an OCI. Accordingly, there is no other specific, published, and complementary legal framework that regulates the accountability and oversight of the operation and administration of SSA in the conduct of an OCI.

[2128] Sections 33, 34 and 35 of the NPAA.
[2129] Section 40 of the NPAA.
[2130] Para 4.5.2 of this chapter.

4.5.8 Conclusion

The provisions of RICA specifically apply to all the six categories of LEA in terms of the adjudication and non-adjudication of an OCI application and interception respectively and reporting to the court in the foregoing instances.[2131] However, the provisions on the accountability and oversight of the six LEAs examined above are general provisions which do not cater for the accountability and oversight of the LEAs in the conduct of an OCI.

Accordingly, there is no other specific, published, and complementary legal framework that regulates the accountability and oversight of the operation and administration of SSA in the conduct of an OCI. However, if specific, internal and adequate provisions regulating the accountability and oversight of the LEAs in the conduct of an OCI exist, the full implementation is yet to be seen in the public domain.

4.6 RECOGNITION, PROTECTION AND REGULATION OF THE PROFESSION OF ELECTRONIC CRIMINAL INVESTIGATORS IN THE MANAGEMENT OF THE AFFAIRS AND ACTIVITIES OF ONLINE CRIMINAL INVESTIGATION

The general investigation of crime is a core training programme and service that every LEO goes through and provides respectively,[2132] covering both overt and covert investigations.

In pursuance of the issues addressed thus far in this chapter, an OCI is a specialised and an advanced method of covert investigation that deserves or requires special recognition, protection and regulation in furtherance of the high ethical, professional and technocratic standards required in the techno-legal complex and delicate conduct of an OCI.[2133] These standards set the pace for the effective and efficient conduct of an OCI and the protection of online communication.

Save for the provision of the requirement that cryptographic providers must register with the Director-General of the Department of Communications,[2134] there is an absence of or

[2131] Para 4.5.2 of this chapter.
[2132] SAQA 'Resolving of crime' http://regqs.saqa.org.za/showQualification.php?id=59989 (Date of use: 9 May 2019).
[2133] See generally Chapter 2 of this study, more particularly paras 2.2, 2.3 and 2.5 - 2.11.
[2134] See sections 29-32 or Chapter V of the ECTA.

inadequate constitutional principles or a statutory regime that recognises, protects, and regulates[2135] the activity of online criminal investigators as a specialised, independent and professional body[2136] as opposed to the general investigative, security or intelligence services.

As a result, the *status quo* dually impacts on the conduct of an OCI and the right to the SOC because there is no such authority that regulates the professional and ethical misconduct and reward of investigators in the conduct of an OCI. For example, in section 36A(1)(b) of the CPA, only authorised persons in SAPS and IPID —who have undergone training in drawing buccal sample approved by the Minister of Health under the National Health Act— are permitted to conduct an investigation of this nature on a suspect, which is a form of regulation in this regard.

The point of departure for the recognition of the profession of online criminal investigators —which is a sub-group of the broad electronic criminal investigators—[2137] is to highlight the recognition, protection and regulation of other specialised human resources which are distinguished from the general body of related professionals, which include the following.

Firstly, lawyers specialise and are recognised, protected and regulated as attorneys, advocates and conveyancers under different and independent professional bodies.

Secondly, in the field of accounting, members specialise and are recognised, protected and regulated as cost accountants, auditors, tax practitioners and management accountants under different and independent professional bodies.

Thirdly, in the field of medicine, members specialise and are recognised, protected and regulated as medical doctors, dentists and ophthalmologists, amongst others.

[2135] Section 22 of the Constitution generally provides for the regulation of the practice of a trade, occupation or profession.

[2136] One can draw on the call for the activity of mediators to be professionalised and accredited in the RSA as other noble professions do such as lawyers, accountants, doctors, Marnewick *Mediation in the Magistrates' Courts* 131, 136 and 148; Secretary General 'Report of the Secretary-General on UN United Nations Activities in Support of Mediation (2017) 19.

[2137] Electronic investigation could be covert or overt. Offline electronic criminal investigator is the counterpart of online criminal investigator, see para 2.2 of Chapter 2 of this study.

Lastly, SCM personnel[2138] have been severed from finance or accounts departments of most organisations in the RSA for better efficiency and effectiveness, leading to the establishment of the Chartered Institute of Procurement and Supply Chain Professionals.[2139]

The activity or procedure involved in SCM is constitutionally recognised and protected in procurement by the government at all levels,[2140] which draw on the rationale that the statutory establishment of online criminal investigators is a reasonable, rational and justifiable one, given the impact of the conduct of an OCI on the security of the RSA and the right to the SOC.

In online criminal investigation, there are high levels of professional expertise and responsibility required of investigators in the techno-legal aspects of conducting an OCI.[2141] This necessitates the imposition of various statutory obligations on the investigators in the conduct of an OCI.

The performance of the obligations of an online criminal investigator is assessed in terms of the 'punishment' and 'reward' systems, which serve as some of the bases for the justification of the recognition, protection and regulation of an independent professional body of online criminal investigators. The awareness that an investigator will be punished or sanctioned[2142] or rewarded by an independent professional body in the conduct of an OCI is one of the attempts at striking a balance in the conflict between the protection of the right to the SOC and the conduct of an OCI.

On the one hand, one of the reasons for the proposed establishment of an independent professional body for online criminal investigators is to empower a public authority to establish and maintain high professional and ethical standards, which include the capacity to impose sanction on investigators for non-compliance or non-performance of an obligation in the conduct of an OCI. Punishment ranges from an option or combination of a fine, suspension

[2138] Department of National Treasury *Public sector supply chain management review* (2015) 24.
[2139] Bizcommunity 'Africa's first professional body for supply chain management launched' https://www.bizcommunity.com/Article/196/760/178600.html ((Date of use: 27 February 2019); CIPS 'Charted Institute of Procurement and Supply' https://www.cips.org/en-za/ (Date of use: 29 January 2019).
[2140] Section 217 of the Constitution.
[2141] Watney *Cybercrime and investigation* 336; Department of National Treasury *Public sector supply chain management review* (2015) 24.
[2142] See generally para 3.10 of Chapter 3 of this study.

from practising the profession to a term of imprisonment against juristic and non-juristic agents under a criminal code in the RSA.[2143]

The enforcement of punishment by a professional body is a measure that is not meant to supplant the recourse to civil action by the SIU,[2144] for example or criminal sanctions by the State against an investigator for wrongdoing[2145] in the conduct of an OCI[2146] but to complement the criminal mandate of the State. For instance, where criminal proceedings or sanctions may not be initiated, given that only a few known prosecutions have been reported,[2147] a professional body will intervene to mitigate the damages from the breach by an online communication investigator.

Another illustration is that, given the fast pace at which technology creates new, risky and compelling opportunities for crime commission that the existing law does not cover, there may not be a legislative criminal liability provision against an investigator for wrongdoing[2148] but a professional body may address the misconduct.

Finally, where there are no criminal proceedings and civil recourse against an investigator in court, a victim of online communication breach becomes a victim of 'double jeopardy' in this regard, because a victim finds himself or herself in a remedial *cul-de-sac* which prohibits him or her from protecting his or her right to the SOC. To avert a 'double jeopardy' in the remedial process for a victim of a breach of the right to the SOC, an independent professional body of online criminal investigators should be established and regulated in the RSA in the same way that other professional bodies are regulated.

[2143] See generally para 3.10 of this chapter.

[2144] Special Investigating Units and Special Tribunal Act, Act 74 of 1996 (SIU Act); Anti-Corruption Authorities 'PROFILEs: South Africa' https://www.acauthorities.org/country/ZA (Date of use: 12 December 2016).

[2145] See the conviction of a prosecutor in an offline bribe scandal, *Famanda v State* supra 12.

[2146] Defenceweb 'Former police crime intelligence officer guilty of phone spying https://www.defenceweb.co.za/security/national-security/former-police-crime-intelligence-officer-guilty-of-phone-spying/ (Date of use: 27 September 2018) (Defenceweb https://www.defenceweb.co.za/security/national-security/former-police-crime-intelligence-officer-guilty-of-phone-spying/ (Date of use: 27 September 2018).

[2147] In an unreported case of first successful prosecution of a LEO contravening the provisions of RICA, a member of the Crime Intelligence of SAPS was convicted in August 2017 of unlawful online spying, see Defenceweb https://www.defenceweb.co.za/security/national-security/former-police-crime-intelligence-officer-guilty-of-phone-spying/ (Date of use: 27 September 2018).

[2148] In 2015, the CCB was published for public comments, which has been replaced by the 2017 version of the bill and again by the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017, but it has not been passed into law. The delay in passing this vital law highlights the likelihood of an investigator being criminally exonerated.

On the other hand, the absence or inadequacy of a framework for the meritorious reward for law enforcement officers ('LEOs') who diligently comply with the requirements for conducting an OCI or LEOs who contribute to the development of the conduct of an OCI creates a vacuum in the effective and efficient conduct of an OCI. For example, the High Court in *State v Miller* commended the LEO who was on the side of caution for not making available to the public or for not unrestrictively using the digital data found in the mobile cellular telephones, which were voluntarily handed over to the LEO by the suspects.[2149]

Although the LEO was executing his job as required by law, however, it is reasonable for the professional body —if there was one— to motivate the LEO by nominating him for recognition or an award, if his or her conduct was deserving recognition or award. In other illustrations, professional bodies like lawyers and accountants honour their members as senior counsel and fellows respectively for their contribution to their professions.

In conclusion, without an intention to express any form of derogatory remark about the recognition, legalisation and protection of the oldest profession —which is sex work— it is submitted that the activity of conducting an OCI is openly taxable as opposed to sex work, which is not. This is because the latter does not seem to have a reasonable and public measure of a standard to determine or trace the taxable income in sex work.

Notwithstanding the differences in the tax philosophy between the bodies of Electronic Criminal Investigators and sex workers, the latter party has gained legal recognition in the Supreme Court of Appeal[2150] and is gathering momentum towards winning the war on the legalisation of sex work, thus a step away from the establishment of a professional body[2151] and a comparative justification for the establishment of a professional body of Electronic Criminal Investigators.

The establishment of an independent professional body of Electronic Criminal Investigators — comprising both offline electronic and online criminal investigators— will achieve two main

[2149] *State v Miller* supra 72.

[2150] The SCA in 1985 overturned the conviction of the prostitutes in *S v Horn* (62/87) [1988] ZASCA 46 (17 May 1988) at pages 3, 14 and 15.

[2151] Van der Watt M 'Decriminalisation of sex work in South Africa will only bring more harm' https://www.dailymaverick.co.za/opinionista/2019-04-17-decriminalisation-of-sex-work-in-south-africa-will-only-bring-more-misery/ (Date of use: 15 May 2019).

cumulative objectives concerning online criminal investigators, which is the gravamen of this study.

Firstly, an independent professional body of Electronic Criminal Investigators will, as it is the goal of non-electronic offline investigators, encourage, promote, and enhance increased credibility, industry recognition, employer confidence, continued professional growth, career advancement, professional opportunity, greater adaptability,[2152] public confidence, peer-group review mechanism, and professional discipline amongst others. Secondly and consequently, the establishment of an independent professional body of Electronic Criminal Investigators will strike a balance between and promote the integrity and security of online communication and the conduct of an OCI.

4.7 CONCLUSION

There are general statutory, regulatory, and policy frameworks for the appointment of specialised staff and training; operation and funding and accountability and oversight of LEAs. However, the provisions are generally not adequate to address the institutional, structural and operational independence, competence, capacity and transparency of the employment, operation and funding and accountability and oversight of the LEAs and LEOs and oversight authorities in the conduct of an OCI in the unique, complex and delicate online communication, both of which require specific provisions to address the issues raised in this study.

[2152] McAfee 'Certified Professional Criminal Investigator (CPCI') https://www.mcafeeinstitute.com/products/certified-professional-criminal-investigator-cpci (Date of use: 1 February 2018).

> Although a bird is free to fly in the sky, however, the wings of a *pelagornis chilensis* cannot overgrow to impede the flight of other birds with equal right to fly. Alas, an eagle, as the watchdog of the jungle, is on patrol to proportionately clip the long wings of the *pelagornis chilensis* according to the level of trespass.

CHAPTER 5: LIMITATION OF THE RIGHT TO THE SECRECY OF ONLINE COMMUNICATION

5.1 INTRODUCTION

Having laid the foundation for the two sides of the coin in this study which are the techno-legal nature and features of the right to the SOC[2153] and the management of the affairs and activities of LEAs or LEOs in the conduct of an OCI,[2154] this chapter applies the limitation principles to this study, with greater emphasis on the constitutional limitation of the right to the SOC.[2155] In addition, this chapter does not only serve as a direct or indirect way of limiting the powers of LEAs in the conduct of an OCI, but also provides guidelines for the effective examination of subsequent chapters in this study.[2156]

5.2 INFRINGEMENT OF THE RIGHT TO THE SECRECY OF ONLINE COMMUNICATION

The infringement of the right to the SOC is considered from the common, statutory and constitutional law perspectives.

[2153] Chapters 2 and 3 of this study.
[2154] See paras 2.5–2.11 of Chapter 2 and Chapter 4 of this study.
[2155] In *Jwara v State* supra 11, there was no contention on the constitutionality of section 36 of the Constitution in limiting the right to privacy.
[2156] See chapters 6 and 7, more particularly paras 6.3 - 6.9 and 6.12 - 6.16 of Chapter 6 and paras 7.2, 7.4, 7.5 and 7.8 of Chapter 7 of this study.

5.2.1 Common law infringement of the right to the secrecy of online communication

In establishing the limitation of the right to the SOC in common law, a single enquiry is made which is, whether the infringement of the right to the SOC is unlawful.[2157] However, two elements are required to prove unlawfulness in common law.[2158] Firstly, for unlawfulness to occur in the conduct of an OCI, the conduct of LEAs must be 'subjectively contrary to the will of an individual'[2159] or against the subjective expectation of the SOC of an individual.[2160]

Secondly, the occurrence of wrongfulness in the conduct of an OCI requires that the infringement must be objectively unreasonable in terms 'of being contrary to the contemporary *boni mores* and the general sense of justice of the community as perceived by the court.'[2161]

5.2.2 Statutory infringement of the right to the secrecy of online communication

5.2.2.1 Introduction

Generally, the infringement of the right to the SOC occurs where LEAs attempt to breach[2162] or intentionally breach the administrative, legal and technical requirements in the provisions of RICA, the POPIA,[2163] the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017[2164]

[2157] Currie and De Waal *Bill of rights* 295.

[2158] *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451(A) 462G (*Financial Mail v Sage*); Neethling et al *Neethling's law of personality* 2nd ed. (2005) 221 (Neethling et.al. *Neethling's law of personality*); Currie and De Waal *Bill of rights* 296.

[2159] *Bernstein v Bester NO* supra 75; McQuoid-Mason *Privacy I* 118-122 and McQuoid-Mason *Privacy II* 12-03 at 38-4; Roos A 'Data Protection' in D Van der Merwe et al *Information and communication technology* (2008) 355 (Roos 'Data Protection'); Neethling J, Potgieter JM and Visser P J *Law of delict* (1994) 332-335 (Neethling, Potgieter and Visser *Law of delict*); *Financial Mail v Sage* supra 462G; Neethling et al. *Neethling's law of personality* 221; Currie and De Waal *Bill of rights* 295-296.

[2160] See para 3.6.2 of this study on the subjective expectation of online communication.

[2161] Neethling, Potgieter and Visser *Law of delict* 332-335; *Financial Mail v Sage* supra 462G; Neethling et.al *Neethling's law of personality* 221; Currie and de Waal *Bill of rights* 295- 296; McQuoid-Mason *Privacy 2* 38-4.

[2162] See sections 2, 49 and 50 of RICA; Section 88 of the ECTA. See Neethling, Potgieter and Visser *Law of delict* 116-119.

[2163] Section 6 (1)(c)(ii) of the POPIA makes provision for the exclusion of the protection of the right to personal information where there is need to detect and investigate crime. See also sections 37(1) and 38(1) of the POPIA.

[2164] The Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.

and other laws, which result in the conduct of an OCI.[2165] The intention of a LEA or LEO takes place in form of *direct eventualis*, *indirect eventualis* and *dolus eventualis*.[2166]

The infringement of the right to privacy in section 14(d) of the Constitution,[2167] concerning the SOC[2168] occurs at four stages in an OCI which create different causes of action in the enforcement of the emerging right to the SOC.

5.2.2.2 Statutory infringement of the right to the secrecy of online communication at the pre-online criminal investigation stage

The infringement of the right to the SOC at pre-interception stage is the first stage of the intrusion of the SOC[2169] which is identified in and prohibited by RICA and the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.[2170] It is the stage where in general practice, save where a ROCI is conducted; non-online information is gathered about an online communication user, upon which an OCI may be conducted if the relevant reasonable grounds standards are satisfied.[2171]

The information gathered is infringed in the following ways. The first set of data that is infringed is the data supplied by a user of online communication before or at the time of activation of or registration for an online communication service. The supply of this data may be offline, such as information required for SIM card registration for mobile cellular telephone,[2172] and online, such as the activation of social media communication. The second set of data that is infringed is the offline information gathered by a LEA under any of the reasonable grounds standards for the commission or attempted commission of an offence necessitating the conduct of an OCI.[2173]

[2165] Other law includes the ECTA and ECA.
[2166] Neethling, Potgieter and Visser *Law of delict* 116-119. Intention may generally occur in the following provisions which have direct and indirect impacts on the right to the SOC: Sections 49, 50 and 51 of RICA; Sections 86(1)-(2) and 87(1) of ECTA and Section 74 of ECA.
[2167] Currie and De Waal *Bill of rights* 133- 149, particularly 136.
[2168] In section 51 of RICA, other types of infringement of the right to the SOC occur indirectly, for example section 51(1)(ii) of RICA.
[2169] Neethling 'The Protection of the Right to Privacy against Fixation of Private Facts' 2004 121 *SALJ* 524 (Neethling 'Fixation of Private Facts'). *State v Naidoo* supra 531.
[2170] Section 42 of RICA and section 37 of CCB B6-2017, whereas the latter is replaced by s 39 of Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[2171] Paras 6.4-6.6 of Chapter 6 of this study.
[2172] Sections 39, 40, 52, 53 and 55 of RICA.
[2173] Paras 6.3-6.6 of Chapter 6 of this study.

It is submitted that the definition of the term 'interception', which is 'disturbingly wide',[2174] covers the pre-OCI stage. Arguably, the wideness incorporates the pre-OCI activities in online communications, which include 'attempted' conduct of an OCI[2175] and the gathering of information in the offline world before an OCI occurs. The pre-OCI activities include circumstances where LEAs or LEOs do not have sufficient fact or do not comply with the usual preliminary requirements at the traditional investigative stage —including lack of relevant reasonable ground standard[2176] before embarking on an OCI, thus resulting in unjustified conduct of an OCI, for example, through the use of a predictive and conscriptive software application.[2177]

5.2.2.3 Statutory infringement of the right to the secrecy of online communication at the online criminal investigation stage

The first leg of section 49(1) of RICA identifies the conduct of an OCI at the actual stage of execution of an online investigation, which makes it unlawful for anyone to intentionally conduct an OCI.[2178] The mere fact that LEAs or LEOs embark on unlawful conduct of an OCI in any of the six online communication devices[2179] is an intrusion of the right to the SOC.[2180] At this stage, LEAs or LEOs have access to both real-time and archived communications of an individual in online communication.[2181]

5.2.2.4 Statutory infringement of the right to the secrecy of online communication at the post-online criminal investigation stage

It is submitted that an infringement of the right to the SOC at the post-interception stage entails a situation where an OCI occurs and LEAs or LEOs acquire, possess or have knowledge of the

[2174] Sections 1 of RICA; Van Der Merwe *Criminal law* 79-80.
[2175] Section 2 and 49(1) of RICA and section 12 of the CCB B6-2017.
[2176] *Web Call v Botha* supra 18; Paras 6.4 - 6.6 of Chapter 6 of this study.
[2177] A predictive software application captures the data or identity of everyone who uses the target words, symbols, signs or forms of communication online and unnecessarily exposes an individual to the risk of wrongful identification or misidentification, Larsson *Telecom operator's incident investigations* 235-240; Para 2.3.3 of Chapter 2 of this study.
[2178] Section 49(1) of RICA. The U.S. law recognizes both interception and post interception and distribution stages, Sloan *Law of privacy in a technological society* 55.
[2179] See Glossary of Acronym.
[2180] Section 49(1) of RICA.
[2181] See s 1 of RICA for the definition of the terms 'interception' and 'monitoring'. See also sections 85-87 of the ECTA.

communications or make some or all of the communications available after recording such communications.[2182] This stage also includes post-decryption of information into an intelligible form by a decryption key-holder.[2183]

5.2.2.5 Statutory infringement of the right to the secrecy of online communication at the distribution stage

Infringement of the right to the SOC occurs at the distribution stage where there is distribution, disclosure or provision of information obtained from the conduct of an OCI by LEAs or LEOs to unauthorized persons or for unauthorized purposes,[2184] resulting in the abuse or misuse of such information.[2185]

5.2.3 Constitutional breach of the right to the secrecy of online communication

In determining the constitutional breach of a right, two enquiries are made, which are the breach of the right to the SOC and its justification.[2186]

5.2.3.1 Breach of the right to the secrecy of online communication

The constitutional breach of the right to the SOC using a limiting measure entails the understanding of two threshold components which inquire about the content and scope of the right to the SOC, on the one hand, and the meaning and effect of the limiting measure-OCI, on the other hand.[2187]

Firstly, the enquiry on the contents and scope[2188] of the SOC is to probe to what extent can the

[2182] Sections 1, 49, 50 and 51 of RICA.
[2183] Sections 1, 49, 50 and 51 of RICA.
[2184] Sections 1, 42, 43, 50 and 51(1)(a) of RICA, sections 37 and 42 of the CCB B6-2017 (which are replaced by sections 39 and 44 of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017) and section 84 of ECTA; Watney *Cybercrime and investigation* 340-341.
[2185] *State v Miller* supra 72.
[2186] See *Ex-Parte Minister of Safety and Security and Others: In Re S v Walters and Another* (CCT28/01) [2002] ZACC 6, 2002(4) SA 613, 2002 (7), BCLR 663 paras 26-27 (*Ex Parte Minister of Safety and Security and Others: In Re S v Walters and Another*).
[2187] *Ex Parte Minister of Safety and Security and Others: In Re S v Walters and Another* supra 26-27.
[2188] Botha H and Woolman S 'Limitations' in Chaskalson M et. al. *Constitutional Law of South Africa* 2ed. (2002) Chapter 36 34.17 - 34.18 (Botha and Woolman 'Limitation'); De Vos (ed) *South African constitutional law in context* (2014)356 ('De Vos (ed) *Constitutional law'*). See Chapter 3 generally, more particularly paras 3.4.4, 3.4.5, 3.5, 3.6, 3.7 and 3.8 of this study on the content and scope of the right to the SOC.

core and peripheral aspects[2189] of an online communication be interpreted and whether the contents and scope of online communication are worthy of constitutional protection.[2190] In response to this query, the contents and scope of the concept of the SOC can be interpreted to protect the extent of the innermost or core (for example, sending a will or trade secret to 'dropbox') and the outer sancta or peripheral (for example, belonging to a social media forum which is open to the entire public) aspects of the reasonable continuum of SOC interests.[2191]

In addition, aside from the existing rights in the concept of privacy,[2192] the contents and scope of the concept of the SOC protect personality rights, therefore, it is invaluable, genuine and serious to constitutionally protect the right to the SOC.[2193] This protection is in accordance with the values that protect an individual in an open and democratic society in furtherance of the unity of values of human dignity, equality and freedom[2194] in an online communication.

It is further submitted that although the protection of the right to the SOC must not be interpreted narrowly or too generously,[2195] nevertheless, it must be interpreted concerning the nature, type and uses of online communication devices, technologies, networks, software applications and services which are dynamic in the contemporary society. In this regard, internal modifiers or limits of the protection of the right to the SOC in such peculiar online communication devices, technologies, networks, software applications and services must first be considered by the court before considering the application of the limitation clause in section 36 of the Constitution, which is external[2196] and generic.

Therefore, using an external or generic modifier may not necessarily address the uniqueness of the protection of the right to the SOC as the internal modifier will do according to the nature, types and uses of online communication devices, technologies, networks, software applications

[2189] *Bernstein v Bester NO* supra 77; De Vos (ed.) *Constitutional law* 374-375.
[2190] Botha and Woolman 'Limitations' 34.17-34.18; De Vos (ed) *Constitutional law* 356.Serious infringement of privacy was described in the Canadian case of *R v Kokesch* 1990 50 CRR 285(SCC) 5, 23 and 26-28 (*R v Kokesch*).
[2191] Paras 3.5.7.2 - 3.5.7.14, 3.7 and 3.8 of Chapter 3 of this study.
[2192] Paras 3.2, 3.3, 3.4.3 and 3.4.4 of this study.
[2193] Chapters 2 and 3 of this study.
[2194] *Ex Parte Minister of Safety and Security and Others: In Re S v Walters and Another* supra 26; De Vos (ed.) *Constitutional law* 26-27, 355- 357; Paras 3.3 and 3.4.4 of this study.
[2195] De Vos (ed.) *Constitutional law* 357.
[2196] De Vos (ed.) *Constitutional law* 357-358 and 382-384; Section 14(d) of the Constitution protects the right to privacy of communications. Only sections 9, 15, 24, 25, 26, 27, 30, 31 and 32 of the Constitution have some forms of internal limitations. See para 5.3.6.1 of this chapter for another examination of internal modifier.

and services.

For example, online conscription[2197] is an automatic and inherent infringement of the right to the SOC that must first be considered internally with regards to the limitation of the right to the SOC before considering any of the external infringement clauses in section 36 of the Constitution. The internal modifier in this regard is the consideration of the specific permissible instances of online conscription, where, although online conscription is an automatic and inherent infringement of the right to the SOC, this study goes further, in its conceptualisation, to submit that the right to the SOC is limited in at least five instances of online conscription.[2198]

These five instances attempt to strike a balance in the conflict in section 35(5) of the Constitution between the outright inadmissibility of online conscripted evidence and the admissibility of all forms of online conscripted evidence.[2199]

Secondly, in the examination of the meaning and effect of the limiting measure enquiry,[2200] the limiting measure in this study is the conduct of an OCI, which is a covert online method of investigation. The practical meaning and effect of the conduct of a covert investigation are described by the pronouncement of the Constitutional Court in the offline context in *Bernstein v Bester No* as an 'extra-ordinary mode' of obtaining information.[2201]

The court further states that the covert offline method, when used, catches an individual unawares and does not entitle an individual who is being investigated to know what is going on in the investigation.[2202] It follows therefore that the meaning, nature and effect of the conduct of an OCI is similar to the description of an 'extra-ordinary mode' of obtaining offline information, in addition to the complex,[2203] delicate and risky nature and effect of the conduct of an OCI.[2204]

[2197] Paras 2.3.3.1-2.3.3.8 of Chapter 2 of this study.
[2198] Para 2.3.3.7 of Chapter 2 of this study.
[2199] Paras 2.3.3.1 and 2.3.3.7 of Chapter 2 of this study.
[2200] De Vos (ed) *Constitutional Law* 359-360; *Ex Parte Minister of Safety and Security and Others: In Re S v Walters and Another* supra 26-27; Para 5.3.4 of this study.
[2201] *Bernstein v Bester No* supra 37 and 38.
[2202] *Bernstein v Bester No* supra 37 and 38.
[2203] See the complex enquiry made in *State v Jordan* supra 80-81.
[2204] Paras 2.5–2.10 and 2.11.4 of Chapter 2 of this study.

The High Court in the digital context in *Absa v Moller*[2205] held that the conduct of an OCI is '*highly evasive, oppressive and draconian in nature*'. In this case, an *Anton Piller* order was obtained and executed covertly against online communication devices such as cloud-based storage system, cellular phones and iPads.[2206] The limiting measure —that is, the conduct of an OCI— must consider that online communication devices are modern-day devices that individuals use in recording their 'most intimate details' and 'closely personal matters' with 'obvious potentially adverse' privacy and dignity implications for an individual and others with whom such individual has had communications with.[2207]

Furthermore, the meaning and effect of the limiting measure[2208] or the 'nature and breadth of the limiting measure' on the right[2209] to the SOC considers whether the conduct of an OCI 'strikes at the core of the right' to the SOC —that is, content data— or its periphery[2210] —that is, meta or traffic data? Arguably, relying on various authorities in the offline world,[2211] the right to the SOC is not capable of partial infringement[2212] —including meta or traffic data according to its own category— where an OCI is executed. The meaning and effect[2213] of the conduct of an OCI relates to the investigation of serious offences[2214] in RICA and the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, which accurately, comprehensively, irreversibly and intrusively infringe on the right to the SOC[2215] in the non-

[2205] *Absa v Moller* supra 2, 13 and 18.
[2206] *Absa v Moller* supra 2, 13 and 18. Italics mine.
[2207] It is noted that though the search warrant issued in *Absa v Moller* related to a house, however, the application and order were ambiguously framed in such a way that they which included both the search of a home and online communication devices, *Absa v Moller* supra 2, 3, 13 and 18. Chapter 2 of this study, more particularly paras 2.2, 2.3 and 2.5- 2.11.
[2208] *Ex Parte Minister of Safety and Security and Others: In Re S v Walters and Another* supra 26-27; *Beinash & Another v Ernst & Young & Others* (CCT12/98) ZACC19, 1999 (2) SA 91, 1999 (2) BCLR 125 and *Mistry v Medical and Dental Council* supra 28; *State v Jordan* supra 28-29. De Vos (ed) *Constitutional law* 356.
[2209] De Vos (ed.) *Constitutional law* 359-360; *Ex Parte Minister of Safety and Security and Others: In Re S v Walters and Another* supra 26-27. The nature and breath of the limiting measure is also examined in para 5.3.4 of this study; *State v Jordan* supra 80-81; *Bernstein v Bester NO* supra 67.
[2210] *State v Jordan* supra 80-86; De Vos (ed.) *Constitutional law* 373- 374 and 376.
[2211] De Vos (ed) *Constitutional law* 374. See paras 5.2.3.1 of this study. In *R v Collins* 1987 crr 122 (SCC) 138 per Lamer J para 138, the court held that evidence could have been obtained without the violation of the Bill of Rights; Van der Merwe S E 'Unconstitutionally obtained evidence' in Schwikkard P J and Van der Merwe S E *Principles of evidence* 3ed (2012) 257 (Van der Merwe *Unconstitutionally obtained evidence*). *Bernstein v Bester No* supra 37 and 38.
[2212] Para 3.5.7.6 of Chapter 3 of this study.
[2213] Botha and Woolman 'Limitation' 34.17-34.18; De Vos (ed.) *Constitutional law* 356. *State v Terrence Brown* supra 6 and 27-31; See Chapter Three particularly para 3.5.7.2 - 3.5.7.14 of this study on the threshold or level of risks and protection of digital privacy.
[2214] It is noted that though RICA permits the use of an OCI in serious offences, however, some offences which are not serious offences but pose actual or potential threats to the State or public can be conducted using an OCI, see para 6.3.3 of Chapter 6 of this study.
[2215] See *State v Miller* supra 48 and 61 and *Riley v California* and *US v Wurie* para 2-4 of the Syllabus and 4, 7, 9, 17, 19, 20, 21 and 25 of the Opinion.

compartmentalised, non-passworded compartmentalised, conscriptive, interoperable, dynamic, complex and risky online communication devices.[2216]

5.2.3.2 Justification of the breach of the right to the secrecy of online communication

The justification stage, which asks the question, whether the limiting measure can be justified in the infringement of the right[2217] to the SOC, entails two independent criteria?[2218]

Firstly, a law —RICA, the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 etc. — must have a character of law, that is, it is derived from a lawful authority[2219] and must be a law of general application[2220] such as RICA and other Acts while the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 does not have the mandate of National Assembly yet simply because it is a Bill.

Secondly, the infringement of the right to the SOC by LEAs must be reasonable and justifiable in an open and democratic society based on 'human dignity, equality and freedom'.[2221] In the South African Constitution, justifiable limitation requires that the purpose of the limitation must be regarded by most people in the society as compellingly important.[2222] Essentially,

---

[2216] In *State v Miller* supra 57, there was unfettered access to the cell phone which was 'willingly handed' over by a suspect to LEAs which had no PIN number. *Riley v California* and *US v Wurie* 2-4 of the Syllabus and 4, 9, 16, 17, 18, 19, 20, of the Opinion. See para 3.5.7 of this study on the threshold for the levels of risks and protection of privacy in the five channels of privacy communications. See Watney *Cybercrime and investigation* 334. See paras 2.2, 2.3 and 2.5–2.11 of Chapter 2 of this study.

[2217] Currie and De Waal *Bill of rights* 150-155. De Vos (ed) *Constitutional law* 360; Para 5.2.3.1 of this study where these constitutional values are considered; *Christian Education South Africa v Minister of Education* CCT13/98, [1998] ZACC 16, 1999(2) SA 83, 1998(12) BCLR 1449 27(*Christian Education v Minister of Education*);*Veldman v Director of Public Prosecutions* (*Witwatersrand Local Division*) (CCT19/05)[2005]ZACC 22, 2007(3) SA 210(CC), 2007 (8) BCLR 827(CC) (*Veldman v DPP*) did not consider the second stage of the limitation enquiry; De Vos (ed) *South African Constitutional Law in Context* (2014) 354-355 ('De Vos (ed) *Constitutional Law'*).

[2218] Currie and De Waal *Bill of rights* 150-155. De Vos P (ed.) *Constitutional Law* 360 See para 5.2.3.1 and (2) of this study where these constitutional values are considered.

[2219] Section 8(3)(b) of the 1996 Constitution; *Dawood v Minister of Home Affairs* 2000 (3) SA 936 paras 39 and 47 (CC) (*Dawood v Home Affairs*); Currie and de Waal *Bill of rights* 155-161; De Vos (ed) *Constitutional Law* 360-362; *President of the Republic of South Africa v Hugo* 1997 (4) SA 1 (CC) 76, 99, 103 and 104; *De Lille v Speaker of the National Assembly* 1998 (3) SA 430 (C) 37; Bawa *ROICA* 306-307; Van der Merwe D 'Telecommunications law' in Van der Merwe D et al *Information communications and technology law* (2008) 27-28 (Van der Merwe *Telecommunications law*); Sections 4-8, 10-11, 16 and 23 of RICA; *State v Nkanbinde* supra 996; *State v Makwanyan*e supra 156; *S v A* supra 293, 297 and 299.

[2220] *State v Naidoo* supra 505 J.

[2221] Currie and De Waal *Bill of rights* 151- 152, 155 and 162. See paras' paras 5.2.3.1 and 5.3.2 of this study where these constitutional values are considered.

[2222] Currie and De Waal *Bill of rights* 151-152; Paras 6.3.3, 6.4-6.6 of Chapter 6 of this study. Section 38(1) of the POPIA.

exceptionally strong or good reasons must be adduced to justify the limitation of the right[2223] to the SOC,[2224] which is herein meant to conduct an OCI in serious offences and other special categories of offences only.[2225]

According to the principle in *Bernstein v Bester No*, which is applied to this study, the limitation of the right to the SOC can be valid where it would not be injusticeable, oppressive, vexatious, unfair or injurious to an individual.[2226]

It is submitted that there is an inherent (first) and an inevitable technical online conscription in online communication[2227] before a second infringement occurs.

The second infringement is legally and compellingly motivated to conduct an OCI, which must be reasonable and justifiable, provided there is strict compliance with the requirements of RICA and other law and recommendation made in this study. The legal and compelling motivation is premised on the fact that given that the conduct of an OCI is an alternative method of investigation, it requires strict compliance with some conditions, mainly the justification by LEA for not applying the alternative method of investigation.[2228] Where there is strict compliance, the effects of the technically inherent, injusticeable, oppressive, vexatious, unfair or injurious[2229] online conscription would have been addressed. The justification enquiry is set out in section 36(1)(a)-(e) of the Constitution[2230] and examined below.

5.2.3.3 Conclusion

Where there is a breach of the right to the SOC which cannot be justified under section 36 of the Constitution, it is submitted that such breach may attract both statutory and non-statutory criminal and non-criminal sanctions and measures to address the breach. Criminal sanctions are imposed in RICA[2231] which prevent the application of the indemnity from prosecution of

[2223] Currie and De Waal *Bill of rights* 151; *State v Manamela* 2000 (3) SA 1 (CC) para 32 (*State v Manamela*).
[2224] Paras 6.4-6.6 of Chapter 6 of this study.
[2225] See paras 6.3.2 and 6.3.3, particularly 6.3.3.2-6.3.3.5 of Chapter 6 of this study.
[2226] *Bernstein v Bester No* paras 17 and 24.
[2227] Para 2.3.3 of this study.
[2228] See paras 6.4-6.6 of Chapter 6 of this study, amongst other conditions.
[2229] *Bernstein v Bester No* paras 17 and 24.
[2230] De Vos (ed.) *Constitutional Law* 366.
[2231] Paras 3.10 and 7.8.5.3-7.8.5.7 of this study.

LEO who maliciously engages in an unlawful OCI[2232] while this study conceptualises non-criminal measures such as the application of the specific permissible instances of online conscription,[2233] ADM mechanism[2234] and voidability and voidness of unlawfully obtained evidence.[2235]

5.3 APPLICATION OF SECTION 36 OF THE CONSTITUTION IN THE LIMITATION OF THE RIGHT TO THE SECRECY OF ONLINE COMMUNICATION

5.3.1 Introduction

Given the established constitutional jurisprudential practice of law in the RSA,[2236] greater emphasis is placed on section 36 of the Constitution which generally makes provision for five criteria in the general limitation of rights. These criteria are applied in the examination of the limitation of the right to the SOC as follows.[2237]

5.3.2 The nature of the right to the secrecy of online communication

In interpreting the nature of the right to be limited, which is the first limitation clause stipulated in the Constitutional provision,[2238] the right to the SOC is a unique, delicate and complex one[2239] that must be considered when a LEO is conducting an OCI.

Notwithstanding the express denial by the Constitutional Court of the existence of the hierarchy of rights in the South African constitutional law jurisprudence,[2240] the same court held that the

[2232] Para 6.16 of this study.
[2233] Para 2.3.3.7 of this study.
[2234] Para 7.7 of this study.
[2235] Paras 7.8.4 and 7.8.5 of this study.
[2236] Nugent *Commission of Inquiry into tax administration and governance by SARS -Final Report* at 116-117.
[2237] See paras 5.3.2–5.3.6 of this chapter for the five constitutional limitation clauses provided in section 36 of the Constitution.
[2238] Section 36(1)(a) of the Constitution.
[2239] Paras 2.2 and 2.3 of Chapter 2 and generally see Chapter 3 of this study.
[2240] *Johncom Media Investments Limited v M and Others (CCT08/08)* [2009] ZACC 5 para 19; De Vos (ed) *Constitutional Law* 373-374.

nature of a right[2241] must be interpreted contextually.[2242] The Constitutional Court also held that special consideration must be taken in the evaluation of the limitation of a particular right,[2243] which means that certain values have greater importance than the others when interpreting the content and scope of a constitutional right.[2244]

For example, the value of human dignity is significant because it is a non-derogable right in the Constitution,[2245] which places the significance of a right above other rights such as the broad right to privacy and lately, the right to the SOC, the composition of which rights is premised on the right to dignity. In other words, it is submitted that the nature of the rights to privacy and SOC seem to be placed on a higher hierarchy than other rights except for the right to dignity.

Relying on the hierarchical principle formulated by the Constitutional Court above, it is submitted that in the nature and features of the five channels of privacy or data communication,[2246] the levels of risks in and protection of online communication channel are higher than the risks and protection in the other channels of privacy communications.[2247]

It therefore follows that a compelling reason[2248] must be established for the limitation of the right to the SOC, which is unique, delicate and complex in nature.[2249] The compelling reason seeks to strike a balance in the conflict between the right to the SOC and the limiting

[2241] Section 36(1)(a) of the Constitution.

[2242] *Bernstein v Bester NO* supra 79. *South African National Defence Union v Minister of Defence* (CCT/27/98) [1999] ZACC 7; 1999(4) SA 469; 1999(6) BCLR 615 25-27.

[2243] *Gay and Lesbian v Min of Home Affairs* supra 34; De Vos (ed) *Constitutional Law* 373-374; *Laugh It Off Promotions CC v South African Breweries International (Finance) BV t/a Sabmark International and Another* (CCT42/04) [2005] ZACC 7; 2006(1) SA 144(CC), 2005(8) BCLR 743(CC); *State v Mamabolo* (CCT44/00) [2001] ZACC 17; 2001 (3)SA 409(CC); 2001(5) BCLR 449(CC) 41; *State v Makwanyan*e supra 144. Similarly, the Constitutional Court in *Bhe and Others v Khayelitsha Magistrate and Others* (CCT 49/03) [2004] ZACC 17, 2005 (1) SA 580, 2005(1) BCLR 1 (CC) at para 71 acknowledges the rights to equality and dignity as important rights.

[2244] De Vos (ed) *Constitutional Law* 357 and 373-374. See paras 5.2.3.1 and 5.3.2 of this study.

[2245] See ss 10 and 37 (Table of Non-Derogable Rights) of the Constitution.

[2246] Para 2.2.1 of Chapter 2 of this study.

[2247] See para 3.5, more particularly paras 3.5.7.2 - 3.5.6.14 of Chapter 3 of this study which is generally on the concept of SOC and particularly on the level of protection for the channels of privacy communication. Communication occurs 24-hour and 7-days- a-week, see Watney *Cybercrime and investigation* 334.

[2248] Section 205(3) of the Constitution provides for the power to investigate crime on behalf of the public, amongst others; See *State v Makwanyane* supra 185; Currie and De Waal *Bill of Rights* 151-152 and 166; Paras 6.4-6.6 of Chapter 6 of this study.

[2249] Paras 2.2 and 2.3 of Chapter 2 of this study.

measure,[2250] which, in this study, is the conduct of an OCI.

5.3.3 The importance of the purpose of the limitation of the right to secrecy of online communication

This principle is examined in two parts. The first part deals with the purposes of the limitation of the right[2251] to the SOC while the second part examines the clause: 'the importance of the purpose of the limitation' of the right[2252] to the SOC.

5.3.3.1 Purpose of the limitation of the right to the secrecy of online communication

The purpose of the limitation of the right to the SOC, which must be legitimate,[2253] justifiable,[2254] reasonable and worthwhile,[2255] is to investigate serious offences and other special categories of offences *only*[2256] for reasons of urgency and public safety[2257] through the use of an OCI which is based on human dignity, equality and freedom, carried out in an open and constitutional democracy.[2258]

In addition, the purpose of the limitation of the right to the SOC through the conduct of an OCI of serious offences must not be 'frivolous, vexatious or made in bad faith'.[2259] For example, there is no justification in the intrusion of the right to the SOC by journalists or for artistry or literary expression as provided in section 7 of the POPIA where such public criminal interest[2260] is not founded, in the first place, on criminality and second, on the commission of

---

[2250] Sections 1(a) and 36(1) of the 1996 Constitution; See sections 16, 17, 18, 19, 20, 21, 22, 23, 26, 29, 30 and 39 of RICA; Currie and De Waal *Bill of rights* 151-152 and 164-165.
[2251] See also para 5.2.3.1 of this study.
[2252] Section 36(1)(b) of the Constitution ; De Vos (ed) *Constitutional law* 369.
[2253] See *State v Makwanyane* supra 185; Currie and De Waal *Bill of rights* 151-152 and 166. There was no legitimacy in the use of an OCI to investigate Mr. Macozoma, see NIA 'Investigations on Mr. Macozoma' 6 and 17-18.
[2254] *State v Makwanyane* supra 185; Currie and De Waal *Bill of rights* 151-152 and 166. See para 5.2.3.1 of this study on the justification for the limitation of a right.
[2255] For example, s 51(1)(b)(ii) of RICA; In *Soobramoney v Minister of Health (Kwazulu-Natal)* (CCT 32/97) 54, the court held that the societal right must not be protected at the detriment of an individual right. Section 38(1) of the POPIA.
[2256] For some of these instances, see sections 1, 7, 8 and 16(5)(a)(ii) - (v) of RICA; Para 6.3.2 of Chapter 6 of this study.
[2257] *State v Hena* 2006 2 SACR 33 (SE) para 42 a-b, *State v Madiba* 1998 1 BCLR 38(D) and *State v Mkhize* 2 SACR 632 (W); Van der Merwe *Unconstitutionally obtained evidence* 251-256; Section 37 of the POPIA.
[2258] Para 5.2.3.1 and 5.3.2 of this study where the Constitutional values are considered.
[2259] *Simataa v Magistrate of Windhoek* supra 20.
[2260] Section 37(2) and (3) of the POPIA. Para 3.1 of Chapter 3 of this study.

a serious offence.

To achieve the purpose of the limitation of the right to the SOC through the conduct of an OCI, offences to be investigated must be classified to achieve the exact purpose of the limitation, which RICA generally classifies as serious offences and potentially and threatening offences *only*.[2261]

However, aside from serious offences being generally and controversially categorised as the only form of offences recognised to be investigated in RICA,[2262] the provisions of RICA and the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 do not have any established or known regulations that specifically classify serious offences into sub-classifications[2263] for purposes of limiting the right to the SOC.

Also, the Constitutional Court of the RSA[2264] and the U.S. Supreme Court[2265] do not specifically classify offences into the six categories of serious offences conceptualised and examined in this study[2266] or into other well-defined forms of classifications to meet the public safety and urgency needs or interests of the government in the investigation of a crime.[2267] The non-specific classification is in contrast with the CPA,[2268] which, in its various schedules, unequivocally and specifically classifies offences for various purposes, for example, the CPA categorises offences, using the bailability criterion.[2269]

[2261] Section 1 for the definition of a serious offence and 16(5)(a)(ii) of RICA.

[2262] Paras 6.3 of chapter 6 of this study, more particularly para 6.3.2 and 6.3.3.2-6.3.3.5.

[2263] Para 16.1(b) and 16.3 of the National Cybersecurity Policy Framework No. 39475 of 2015. The Supreme Court of Appeal in *State v Malgas* (2001) 1 *SACR* 469 (SCA) 14 (*State v Malgas*) held that sentencing rests upon the specific classification of offences. Emphasis is placed on the latter part of paragraph 14 of section 1 of the only Schedule to RICA, which is too broad, which states that RICA applies to an offence whereof the punishment of which a period of 'imprisonment exceeds five years without an option of a fine'. Section 20A (9) of the Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007. *State v Malgas* supra 14. See para 6.3.3.3 of Chapter 6 of this study for the effect of para 14 of s 1 of the Schedule to RICA.

[2264] *State v Makwanyane* supra 156, 159, 160, 161, 163, 164 and 166; *Magajane v North West Gambling Board* supra 50.

[2265] *Riley v California* and *US v Wurie* supra 14-16, 20, 23-24 and 22 -24 of the Opinion. 'The degree of probable cause required can vary according to the level of intrusion of a search, to the importance of the crime it aims at investigating, even to the imminence of the crime it is aimed to prevent.' *Griffin v Wisconsin* 483 US 868 at 887(1987), see Ruiz *Privacy in telecommunications* 232-233.

[2266] Para 6.3.3.2 of Chapter 6 of this study.

[2267] *Magajane v North West Gambling Board* supra 50 and 54.

[2268] The CPA has eight schedules, which unequivocally identify various offences for different purposes.

[2269] Para 6.3.3.2 of Chapter 6 of this study.

Relying on an offline classification of offences by the Constitutional Court,[2270] the non-specific classification of serious offences creates some inconsistency and arbitrariness[2271] in the formulation of an objective guideline[2272] in the investigative threshold requirements in conducting an OCI in the unique, delicate and complex nature of the right to the SOC.[2273]

Furthermore, the non-specific classification of serious offences in RICA,[2274] the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 and other law unwittingly and controversially defeats one of the purposes for which RICA was enacted, which is to limit the right to the SOC in RICA when serious offences are committed, which on its own, RICA classifies only serious offences.

In this regard, should a serious offence be investigated through the conduct of an OCI and conviction is secured with an imposition of a sentence lower than what is prescribed in RICA,[2275] the non-specific classification of serious offences in RICA, the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017 and other law unconsciously re-classifies a serious offence which was initially investigated through an OCI.

Thereafter, it is consequently and unintentionally categorised into a less serious offence. This categorisation is done under the exercise of the 'onerous, monstrous and sometimes lonely'[2276] discretion of either the trial or appellate court where a lesser sentence is ultimately imposed[2277]

[2270] *Estate Board v Auction Alliance* 42. Italics mine.

[2271] *State v Makwanyane* supra 156, 159, 160, 161, 163, 164 and 166.

[2272] 'The degree of probable cause required can vary according to the level of intrusion of a search, to the importance of the crime it aims at investigating, even to the imminence of the crime it is aimed to prevent.' *Griffin v Wisconsin* 483 US 868 at 887(1987), see Ruiz *Privacy in telecommunications* 232- 233.

[2273] Paras 2.2 and 2.3 of Chapter 2 and para 3.5.7 of Chapter 3 of this study.

[2274] Emphasis is placed on the latter part of paragraph 14 of s 1 of the only Schedule to RICA; Section 20A (9) of the Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007. *State v Malgas* supra 14.

[2275] Paragraph 14 of section 1 of the only Schedule to RICA. See also para 6.3.2 of Chapter 6 of this study.

[2276] Hogarth J *Sentencing as a human process* (1971) 5 cited in Stockdale E and Devlin K *Sentencing* (1987) 8.

[2277] *State v Dodo* (2001) 1 *SACR* 594 (CC) paras 1, 3, 8, 9, 29 and 34 (*State v Dodo*); *State v Malgas* paras 1,8, 9, 12, 13 and 25; Section 51 (3)(a) and (6) of the Criminal Law Amendment Act No. 105 of 1997 enables a court to generally use its discretion to reduce the minimum sentence and more particularly in favour of children under the age of 16 years where there are substantial and compelling circumstances to do so by the court, see *Veldman v DPP* supra 17; *N v The State* (469/2007) [2008] ZASCA 30 paras 20 and 44 (*N v The State*). It is submitted that a lesser sentence does not only occur based on the discretion of the court, it may also be imposed where, as a substitute for a serious offence, a less serious offence, is introduced in a trial due to lack of evidence, thus, invasion of online communication would ultimately have become inevitable; *S v Joseph Arthur Walter Brown* (681/2013) [2014] ZASCA 217 paras 98 and 100 (*State v Joseph Brown*). Aside from the cases highlighted above and below, it is noted that there is no recorded or published case law in which an OCI was used to investigate a serious offence which later attracted a lesser sentence and consequently re-classifies the offence into a less serious offence.

below what is stipulated in RICA,[2278] arising from a combination of many factors.[2279] The initial use of an OCI to investigate a non-specific or general serious offence which later attracts a lesser sentence[2280] would have led to the unconstitutional obtainment of evidence in online communication by LEAs, thereby defeating the purpose for which an OCI may be conducted. The consequential lesser sentence is fluid and conceptualised as 'descending serious offence' in terms of criminal conviction and sentencing relating to the conduct of an OCI.[2281]

Thus, it is submitted that a LEO may be expected to comply with some threshold requirements to investigate serious offences based on the display of their knowledge of precedent on sentencing concerning the serious offence that is being investigated.[2282] This is one of the justifications for the call that LEOs should possess a techno-legal qualification in the conduct of an OCI[2283] and that there should be a recognition of the professionalism in the conduct and

[2278] See the latter part of paragraph 14 of s 1 of the only Schedule to RICA.

[2279] *State v Dodo* 1, 3, 8, 9, 29 and 34. The other factors, in form of classification of sentencing are explained below. *State v Makwanyane* supra 158-161, 163-166, 173-174 and 177,199 and 297; Section 51 of the Criminal Law Amendment Act 1997; Bekker P M *Criminal procedure handbook* 9 ed. (2009) 288-290. See *Veldman v DPP* para 17; *N v The State* paras 1, 2, 3, 8, 9, 15 and 43; The exercise of discretion also considers the following: a) sentence must be proportionate to the offence, *Veldman v DPP* supra 4, 32–33, 36 and 38; b) sentencing must not infringe on other rights, *Veldman v DPP* supra 23 and 45 and *State v Tshilo* 2000 (4) SA 1078 (CC) (*State v Tshilo*) ; 2000 (11) BCLR 1252 (CC). *State v Makwanyane* supra 44, 177, 197, 273*; State v Malgas* supra 4, 8, 9, 12, 13, 19, 22, 23, 25 and 34; *N v The State* supra 11; *State v Ivan Andries Muller* CASE NO: 2SH98/2005 paras 1, 2, 79-82 and 112 (*State v Muller*); Criminal Law (Sexual Offences and Related Matters) Amendment Act, No. 32 of 2007 (SORMAA), see more at: NRSO 'FAQ: National Register for Sex Offenders (NRSO)' http://www.justice.gov.za/vg/nrso.html#sthash.l1ApZaBz.dpuf (Date of use: 12 June 2016); Section 51 (3)(a) and (6) of the Criminal Law Amendment Act No. 105 of 1997; *State v Joseph Brown* supra 44, 100, 108 and 112; Section 51(2)(a)-(c) of the Criminal Law Amendment Act.

[2280] See *State v Dodo* supra 29. It is submitted that the trial court should not assume that in order to prevent the appellate court from raising the issue that evidence was unconstitutionally obtained through the conduct of an OCI in a serious offence which later becomes less serious offence by virtue of the imposition of a lesser sentence, it should unreasonably and unjustifiably impose a heavy sentence in order to keep a matter within the ambit of the requirement in the latter part of para 14 of s 1 of the only Schedule to RICA. Unconstitutionally obtained evidence is examined in paras 2.3.3.7 and 7.8 of this study.

[2281] See the latter part of paragraph 14 of s 1 of the only Schedule to RICA and para 6.3.2 of Chapter 6 of this study.

[2282] See para 14 of s 1 of the only Schedule to RICA. In the Constitutional Court case of *Veldman v DPP* supra 36, 38 and 39, the court warned that the prosecution should have known in advance the seriousness of an offence to determine which court to institute the prosecution for appropriate sentencing in a serious offence instead of instituting a serious offence in a court that does not have a higher penal jurisdiction. The court further warned that instituting a case at the wrong court would prohibit effective criminal prosecution. It is submitted that there must be a proportionality between the seriousness of the offence and severity of the punishment, see para 39 of *Veldman v DPP* supra. Similarly see also *State v Joseph Brown* para 119. *Veldman v DPP* supra 36, 38 and 39. *State v Malgas* supra 8 and 25. The need for LEAs, prosecutors and judges who play a role in the conduct of an OCI to have requisite skills in general cyber law and security has been emphasised, see paras 6 (p 6), 1.6, 2.7, 4.1.4, 5.3.6(f) and 12.2 (a)-(d) of the National Cybersecurity Policy Framework No. 39475 of 2015.

[2283] Although the Court in *Suzman Foundation v Min of Police* supra 66 held that LEOs are not required to possess a legal qualification to conduct an investigation in the offline world, however, the HC proves otherwise in *State v Naidoo* supra 521 B-E, see para 4.3.3 of Chapter 4 of this study. See also para 5.4.3 of this chapter.

administration of an OCI in the RSA.[2284]

5.3.3.2 Importance of the purpose of the limitation of the right to secrecy of online communication

In the second leg of section 36(1)(b) of the Constitution, one important purpose of the limitation of the right to the SOC through OCI is found in *State v Miller* where the court observed that a speedy investigative step should be used to access digital information in the fight against crime.[2285] The court held that the step in such an investigation should not be bureaucratic in its operation, otherwise the essence of the procedure would be counter-productive.[2286]

Another important purpose for the limitation of the right to the SOC through the conduct of an OCI is to obtain comprehensive and unrestricted evidence in the non-compartmentalised, non-passworded compartmentalised, interoperable and conscriptive online communication through the inherently covert use of an OCI.[2287]

5.3.4 The nature and extent of the limitation of the right to the secrecy of online communication

The nature and extent of the limitation of the right to the SOC under section 36(1)(c) of the Constitution is the third limitation clause, which has been partially examined under the enquiry that addresses the 'meaning and effect of the limiting measure' or the 'nature and breadth of the limiting measure' on the right to the SOC.[2288] However, the following is examined in pursuance of this limitation clause.

5.3.4.1 Proportionality test

Section 36(1)(c) entails an assessment that is done by the court in the way in which a limiting

[2284] Paras 4.3.8 and 4.6 of Chapter 4 of this study.
[2285] *State v Miller* supra 51.
[2286] *State v Miller* supra 51. Sections 15(2), 16(6)(d), 17(2)(f), 17(5)(d), 18(2)(b)(iii), 18(3)(b), 19(5)(c), 20(1),(2)(b),(4) and (6), 21(5)(e), 22(1)(b), (6) and (8), 23(4)(b), 23(8)(b), 24(b) and 25 of RICA. Hubbard, Brauti and Fenton *Wiretapping* at 16-1.
[2287] See generally Chapter 2 of this study.
[2288] See para 5.2.3.1 of this chapter.

measure —such as the conduct of an OCI— affects the right[2289] to the SOC. The assessment inquires whether the limitation measure —an OCI— is 'a serious or relatively minor infringement' of the right[2290] to the SOC. This enquiry is considered in terms of the principle guiding the proportionality test.[2291]

The test requires that the limitation of the right to the SOC by a limiting authority (that is, LEAs or LEOs) must not extend beyond the purpose it seeks to serve,[2292] which is in line with the principle laid down by the Constitutional Court in *State v Makwanyane* which states that '…if the harm is disproportionate to the benefits, the limitation is not justified.[2293] Borrowing from the principle in *State v Manamela*, the proportionality test requires that the conduct of an OCI or the provisions of RICA, the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017 and other law must not be 'used as a sledgehammer to crack a nut'[2294] or used disproportionally.

Arguably, the proportionality test is considered according to the specific nature and features of both the content and meta or traffic data, given that various unique forms of these two types of data exist, some of which, if infringed, constitute a serious invasion. Proportionality also means that, for example, 'reasonable ground' standards differ in the investigation of an offence and identity of an individual concerning the investigation of an offence.[2295]

In order not to make the limitation of the right to the SOC disproportionate, two issues are considered —amongst others— in the proportionality analysis by the Constitutional Court in *Magajane v North West Gambling Board*.[2296]

Firstly, the court has to consider the 'concentric circle', 'continuum of privacy' or better still,

[2289] Currie and De Waal *Bill of rights* 151-152, 168 and 273.
[2290] Currie and De Waal *Bill of rights* 168. 'It is only too normal that certain searches and seizures are thought to require a higher degree of probable cause than others in order to be considered reasonable. The degree of probable cause required can vary according to the level of intrusion of a search, to the importance of the crime it aims at investigating, even to the imminence of the crime it is aimed to prevent.' Though the Supreme Court of US does not subscribe to lessening the level of application of the probable cause requirement, it however speaks of excepting the application of the probable cause by replacing it with 'reasonable suspicion' which is the likelihood of facts justifying the search, *Griffin v Wisconsin* supra 887, see Ruiz *Privacy in telecommunications* 232-233.
[2291] Currie and De Waal *Bill of rights* 168.
[2292] Currie and De Waal *Bill of rights* 168, 276, 282; *State v Makwanyane* supra 236.
[2293] *State v Makwanyane* supra 236; Currie and De Waal *Bill of rights* 168; Section 37 (1)(a) & (b) of POPIA.
[2294] *State v Manamela* supra 34; Currie and De Waal *Bill of rights* 151-152 and 166.
[2295] Hubbard, Brauti and Fenton *Wiretapping* 3-6 and 3-13; Paras 6.3.2, 6.3.3.1- 6.3.3.5, 6.4 and 6.5 of Chapter 6 of this study.
[2296] *Magajane v North West Gambling Board* supra 50.

the 'expectation of privacy' of an individual[2297] concerning the seriousness of the offence. In this regard, the court held that 'A court has to consider an applicant's expectation of privacy and the breadth of the legislation, among other considerations'[2298] in the limitation of the right to the SOC. The expectation of privacy —in this study, the SOC— will be more attenuated the more the matter is made public.[2299] In interpreting the decision of the court, the more serious an offence, the more intrusive a LEA can conduct an OCI in the SOC.[2300]

Secondly, consideration is given to the breadth of the legislations[2301] —which are mainly the ECT, ECTA, RICA, POPIA and Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017— that seek to protect the right to the SOC and at the same time, limit the right —through the conduct of an OCI— where the need arises. However, it is submitted that the breath of these main legislations is relatively inadequate to effectively protect this right and conduct an OCI in contemporary society.

5.3.4.2 Incremental principle

Drawing on the principle established in the Constitutional Court in *Magajane v North West Gambling Board*,[2302] the incremental limitation of the right to the SOC is possible, and permissible in the conduct of an OCI.[2303] The principle occurs where there is incremental or progressive intrusiveness or intensity of the conduct of an OCI on the continuum of the SOC interests or the rights[2304] in other subject matters, devices, technologies, networks, applications and services that are capable of being incrementally limited.

However, the incremental principle does not occur in the right to life which is not subject to incremental limitation or invasion[2305] because death is different,[2306] and '…the effect is total and irreversible' according to the Constitutional Court case of *State v Makwanyane*.[2307] While

[2297] *Magajane v North West Gambling Board* supra 50 and 59; Para 3.6 of Chapter3 of this study.
[2298] *Magajane v North West Gambling Board* supra 50, 53 and 59.
[2299] *Magajane v North West Gambling Board* supra 50, 53 and 59.
[2300] *Magajane v North West Gambling Board* supra 50, 53 and 59.
[2301] *Magajane v North West Gambling Board* supra 50.
[2302] *Magajane v North West Gambling Board* supra 50.
[2303] *Magajane v North West Gambling Board* supra 50.
[2304] Paras 3.7 and 3.8 of Chapter 3 of this study.
[2305] *State v Makwanyane* supra 351.
[2306] *State v Makwanyane* supra 351.
[2307] *State v Makwanyane* supra 351.

the enjoyment of life can be qualified, its incremental existence cannot.[2308] Life cannot be diminished for an hour, a day, or 'for life'.[2309]

Arguably, the application of the incremental principle in the conduct of an OCI is that *ab initio*, an OCI generally and incrementally or progressively commences with the relative conduct of an OCI in traffic data[2310] —regardless of its duration— which is not as risky as content data. Thereafter, LEAs may later incrementally or progressively resort to the relative conduct of an OCI in the broad riskiest meta and content data[2311] —if reasonable and justifiable— in response to the seriousness of an offence.

However, there is arguably an exception to the incremental principle in which the traffic, content and other forms of data are simultaneously used in the conduct of an OCI without first conducting an OCI in meta or traffic data. This exception constitutes an advance conduct of an OCI because there is no progression or step-by-step movement in the relative conduct of an OCI from the narrow traffic data, through metadata and finally to the broad content data. This exception arguably applies to the following, amongst others, where:

a) two categories of offences occur or may occur, one of which is a general serious offence while the other is a more serious offence, both of which must be investigated simultaneously, necessitating the use of both progressive and advance conducts of an OCI against the same perpetrator;

b) the commission of an offence involves or may involve the safety or security of the Republic or general public;[2312]

c) the effect of the commission of an offence is absolutely or partially irreversible;[2313]

[2308] *State v Makwanyane* supra 351.
[2309] *State v Makwanyane* supra 351.
[2310] Para 2.6.2.1, 2.6.2.3 and 2.6.2.4 of Chapter 2 of this study. See generally para 2.3.3 on the concept of online conscription. The fact that art 30(1) of CoE CoCC enables the Republic to grant expeditious access to traffic data in a preservative order where an OCI application has not been formally submitted by a state to the Republic indicates the relative lesser threshold when using traffic or meta data to conduct an OCI. However, the real-time traffic data requires higher threshold, see art 33(1) of Council of Europe 'Chart of Signatures and Ratifications of Treaty 185-*Convention on Cyber Crime*-Status as at 02/06/2017 (CoE CoCC).
[2311] Paras 2.6.1 and 2.6.2.2 of Chapter 2 of this study.
[2312] Paras 6.3.3.2(a)-(f) of Chapter 6 of this study. Another example is the control and management of corona virus that has been declared as pandemic by the World Health Organisation.
[2313] Para 6.3.3.4 of Chapter 6 of this study.

d) there is a need for the investigation of an offence using a ROCI in a robotic environment;[2314]

e) there is an exceptional circumstance to depart from the general principle or where the court deems it fit in cases where the conduct of an OCI in traffic data may be disproportionate to the nature, seriousness and effect of the commission of an offence.

5.3.4.3 Reverse proportionality principle

In further considering section 36(1)(c) of the Constitution, it will be appropriate for LEAs to use the 'reverse proportionality enquiry' or the 'notion of reasonable accommodation' in the limitation of the right[2315] to the SOC. While the latter is further examined in this chapter,[2316] the former enquiry requires the limiting authorities —such as LEAs, in pursuance of section 7(2) of the Constitution, to consider not only whether the limiting authorities have 'gone too far in restricting the enjoyment of the right'[2317] to the SOC, which is negative protection but whether positive steps could have been taken by the limiting authorities —LEAs— to protect the right to the SOC, which is positive protection.[2318] This study has proven otherwise in terms of the protection of the right to the SOC by LEAs.

[2314] Paras 2.11.3 and 2.11.4 of Chapter 2 of this study.

[2315] De Vos (ed) *Constitutional law* 372-373. Para 5.3.6.1 of this chapter.

[2316] The notion of reasonable accommodation is also examined in para 5.3.6 of this study.

[2317] Citing section 22 of RICA as example, it is submitted that the provision goes too far in restricting the right to privacy. The position of section 22 has not been amended in RICA despite the amendment of some provisions and the case of *S v A* supra 293, 297 and 299; *Bernstein v Bester NO* supra 65, 67 and 77; *Mistry v Medical and Dental Council* supra 16 and 27; *Investigating Directorate v Hyundai and Smit No* supra 557; Currie and De Waal *Bill of rights* 298-300 and 304; See section 1 of RICA for the definition of the term 'premises'; Section 27 of RICA regulates the execution of entry warrant which allows LEAs to enter the premises at any time without prior notice to the owner or possessor and perform any purpose for which the warrant was issued. See also para 5.3.6 of this study on the proportionality test. Sections 20-22 of the CPA; Section 82(3) of the ECTA; Van der Merwe *Criminal law* 83-86; Section 25(4)(b) of the Constitution; Basdeo 2012 2 *SACJ* 205. Section 5 and Chapter 5 of the ECA; Sections 2, 30, 32, 50 and 54 of the Telecommunications Act No 103 of 1996; Sections 56-57 of RICA regulate licensing of electronic networks; Yacoob and Pillay *Licensing* 132-171, particularly 133-134 and 171; See para 3.4.5.3 of this study. It is noted that 'Electronic network possession' is perceived as an intangible, immaterial or intellectual property which is capable of being possessed and this position cannot be over-emphasized, see paras 2.3, 2.7.3, 6.2.3, 8.4.1 and 8.4.2 of Popoola *Liability of ISPs* where emphasis was laid on the invaluability of signal in Internet protocol as a property. In the American context, interception of electronic communications is regarded as search and seizure, Ruiz *Privacy in telecommunications* 63.

[2318] Section 7(2) of the Constitution; De Vos (ed.) *Constitutional law* 372-373; See para 5.3.6.1 of this study on the 'reverse proportionality enquiry'.

5.3.5 The relation between the limitation of the right to secrecy of online communication and its purpose

Section 36(1)(d) of the Constitution is the fourth limitation clause. It stipulates that for the limitation of a right to be reasonable and justified, there must be a relation between the limitation of a right —that is, the intrusive invasion of the right to the SOC through OCI— and the purposes of the limitation,[2319] which are the investigation of crime to protect the public criminal interest,[2320] other instances examined earlier[2321] and the preservation of evidence.[2322]

Applying the view of Currie and De Wall, reasonableness and justifiability also mean that the harm caused by the infringement or the use of an OCI in the limitation of the right to the SOC must be proportional to the beneficial purpose that the law —the ECA, ECTA, RICA, POPIA, Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 and other law— seeks to achieve.[2323] The provisions of RICA seek to achieve effective investigation of serious offences that cannot ordinarily be investigated in the conduct of non-OCIs.[2324]

According to the principle in *State v Makwanyane*,[2325] there must be satisfactory evidence establishing a causal link between the means (that is, the conduct of an OCI) and the ends (that is, the effective investigation of serious offences). On the one hand, if the provisions of a law —such as RICA and Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017— do not serve the purpose of conducting an effective investigation of serious offences at all, there cannot be any reasonable justification for the limitation of the right[2326] to the SOC under such law.

On the other hand, if the provisions of a law —such as the ECA, ECTA, RICA, POPIA and Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017— partially serve their purposes,

---

[2319] Section 36(1)(d) of the 1996 Constitution.
[2320] Para 3.1 of Chapter 3 of this study.
[2321] Sections 4-11 of RICA that justify the purpose of using OCI procedure in the investigation of crime. *Web Call v Botha* supra 13.
[2322] See s 37 of RICA*; Web Call v Botha* supra 13; See also Van der Merwe 'Unconstitutionally obtained evidence' 255-256 and 265.
[2323] Currie and De Waal *Bill of rights* 169.
[2324] *Web Call v Botha* supra 5 and 12. The devices dealt with by the court were online communication devices.
[2325] *State v Makwanyane* supra 184; Currie and De Waal *Bill of rights* 151-152 and 169-170; De Vos (ed) *Constitutional law* 371.
[2326] *State v Makwanyane* supra 184; Currie and De Waal *Bill of rights* 169-170; De Vos (ed) *Constitutional law* 371.

there cannot be adequate justification for the limitation of the right[2327] to the SOC.

Essentially, the provisions of the ECA, ECTA, RICA, POPIA and Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, amongst others, through the conduct of an OCI, must fully serve the purpose of investigating serious offences. However, from the practical point of view, according to De Vos, in most cases, a limiting measure does not fail this rational connection requirement.[2328]

5.3.6 Less restrictive means to achieve the purpose of limiting the right to secrecy of online communication

In the fifth and last limitation clause, section 36(1)(e) of the Constitution provides for the principle of 'less restrictive means' in the limitation of the right to the SOC. According to De Vos, two alternate enquiries are set out in section 36(1)(e) which are the 'less restrictive alternative means' and 'well-tailored' enquiries which are considered before the proportionality test is applied.[2329]

5.3.6.1 Less restrictive alternative means enquiry

In the 'less restrictive alternative means' enquiry, consideration is given to the 'possibility of a hypothetical, alternative measure that is less restrictive of the right'[2330] to the SOC. Section 36 of Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 stipulates that the powers of LEAs to investigate an offence must be based on the severity of such offence and the rights, legitimate interests and responsibility of other parties.[2331] This section is in pursuance of the use of less restrictive means to carry out an investigation.

Borrowing from the Namibian case of *Simataa*, which deals with digital data, LEAs should embark on an OCI in 'the least evasive manner with regards to digital data in computers,

[2327] *State v Makwanyane* supra 184; Currie and De Waal *Bill of rights* 169-170; De Vos (ed.) *Constitutional law* 371.
[2328] De Vos (ed) *Constitutional Law* 371. However, in *National Defence Union v Minister of Defence* supra 615 the blanket ban on the formation of union in the defence force was irrational.
[2329] De Vos (ed) *Constitutional Law* 371-373.
[2330] Section 36(1)(e) of the 1996 Constitution; De Vos (ed) *Constitutional law* 371- 372.
[2331] The CCB B6-2017.

laptops and other devices which contain personal data as well as data relevant to the investigation'.[2332]

The decision of the Canadian Court in *R v Kokesch* relates to the admissibility of evidence in section 24 (2) of the Canadian Charter which is equivalent to section 35(5) of the Constitution of the RSA.[2333] However, persuasively drawing on this case, the relevance and interpretation of the dictum below cannot be overemphasised to *mutatis mutandis* serve a second, dynamic, progressive and compelling purpose of espousing it under the less-restrictive principle in s 36(1)(e) of the Constitution of the RSA:

> '[o]f course, the reason why other investigative techniques were unavailable is that the police did not have the requisite grounds to obtain either a search warrant or an authorization to intercept private communications pursuant to the Criminal Code… the *unavailability of other, constitutionally permissible, investigative techniques is neither an excuse nor a justification for constitutionally impermissible investigative techniques…Where the police have nothing* but suspicion *and no legal way to obtain other evidence*, it follows that they must *leave the suspect alone, not charge ahead* and *obtain evidence illegally* and *unconstitutionally*. Where they take this latter course, the *Charter* violation is plainly more serious than it would be otherwise, not less'. [2334]

However, a means does not have to be less restrictive provided it is proportionate.[2335] The use of a less restrictive means might not, on balance, be proportionate due to the consideration of other circumstances or factors in the issue.[2336] It is submitted that even where the conduct of an OCI is not less restrictive to the right to the SOC, it must be proportionate to the level of seriousness and nature of the offence that is being investigated.[2337] Furthermore, although intrusive; the invocation of an oral application in section 23 of RICA or section 43 of the

---

[2332] *Simataa v Magistrate of Windhoek* supra 40 and 49; See also *Investigating Directorate v Hyundai and Smit No* supra 35-38 Per Langa.

[2333] Admissibility or exclusionary rule in section 35(5) of the Constitution is clearly examined in paras 2.3.3.7 and 7.8 of this study.

[2334] Italics mine. *R v Kokesch* supra 5, 23 and 26-28. See also paras 6.5.3, 6.5.6 and 6.5.7 of Chapter 6 of this study.

[2335] De Vos (ed) *Constitutional Law* 372.

[2336] De Vos (ed) *Constitutional Law* 372. Other circumstances or factors in issue include costs and other rights that may be infringed, see *Three Cities Investment Ltd & other v Signature Life (Pty) Ltd & others* 2011 BIP 352(KZD) para 18 where an order to search a cellphone of an individual in an *Anton Piller* order was extended to the wife, children and visitors of the target.

[2337] De Vos (ed) *Constitutional law* 372; *State v Nombewa* 1996 2 *SACR* 298(G) para 423 c-e (*State v Nombewa*); As proportionality is used in this regard, it is the concern of the court that public opinion is affected by the seriousness of crime, see Van der Merwe *Unconstitutionally obtained evidence* 188 and 213. Admissibility of evidence obtained unconstitutionally is examined in Chapter 6 of this study.

Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017[2338] to investigate more serious offences or cybercrime —such as high treason, terrorism and cyber warfare— is proportionate because of the very likely serious irreversible consequences of the commission of these offences, such as the risk of death.[2339]

The choice of an investigative method must not be made in bad faith[2340] and less restrictive means are always easily and possibly identified.[2341] On the one hand, it is not the duty of the court to find the least restrictive means in limiting the right[2342] to the SOC. The non-availability of lawful methods other than an OCI is not a justification for the intrusion of the right[2343] to the SOC. On the other hand, Currie and De Waal support the belief that the State has the discretion to embark on an alternative investigative procedure,[2344] however, it is submitted that the broadness of the discretion of LEAs or the internal policy guideline on the use of an OCI by LEAs should be subject to the proportionality test.[2345]

The court may ask a question about the failure or refusal to use a conventional procedure or less invasive procedure[2346] in the investigation of serious offences. However, the courts should not usurp the role of policymakers in looking for a less restrictive means while asking questions concerning a less invasive procedure.[2347]

The proportionality test considers the balance of different interests by 'weighing up of competing values'[2348] which include the costs of the limitation.[2349] The costs in this perspective are the effects or consequences of the limitation, which are established in *State v*

[2338] The CCB B6-2017, which is replaced with the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[2339] See the later part of this rubric where this principle is examined under a different principle.
[2340] *R v Feeney* 1997 44 CRR 2d 1 (SCC) para 37; Van der Merwe *Unconstitutionally obtained evidence* 257.
[2341] *R v Kokesch* supra 5, 23 and 26-28.
[2342] De Vos (ed) *Constitutional law* 372. Currie and De Waal *Bill of rights* 170; Van der Merwe *Unconstitutionally obtained evidence* 257.
[2343] *R v Kokesch* supra 5, 23 and 26-28; Van der Merwe *Unconstitutionally obtained evidence* 257.
[2344] Van der Merwe *Unconstitutionally obtained evidence* 257; *State v Pillay* supra 89, Schwikkard *Arrested, detained and accused persons* 810.
[2345] Currie and De Waal *Bill of rights* 163, 276 and 282; *Web Call v Botha* supra 19-20; See paras 3.2.3 (b) and 4.3.4 of this study.
[2346] *Web Call v Botha* supra 19. Currie and De Waal *Bill of rights* 151-152, 163-164 and 170. Van der Merwe 'Unconstitutionally obtained evidence 203 and 244; Canadian case of *R v Stillman* (1997) 1 S.C.R 607 para 224 and 234.
[2347] De Vos (ed) *Constitutional Law* 372-373.
[2348] Currie and De Waal *Bill of Rights* 163.
[2349] Currie and De Waal *Bill of Rights* 163 and 170. See also the examination of cost from the reasonable accommodation perspective in this paragraph.

Makwanyane[2350] where the court held that the cost of having to impose a death penalty as a form of deterrence was too grievous, extensive, and costly.[2351] In this study, the cost of limitation relates to the intrusive, extensive, comprehensive and irretractable invasion of the non-compartmentalisation, non-passworded compartmentalised, interoperable, and conscriptive online communication.[2352]

'The more serious the impact of' a limiting measure —such as the conduct of an OCI— on the right to the SOC, 'the more persuasive or compelling the justification must be'[2353] to conduct an OCI. In this study, the impact that the conduct of an OCI will have on the right to the SOC is determined by the justification of the threshold requirements of relevant standards of proof for each of the category of serious offences to be met by LEAs.[2354] It is meaningless to consider a 'balancing process' in a limiting measure —such as the conduct of an OCI— if such measure has been 'found either not to be rationally connected to the constitutionally acceptable purpose' —which is the duty of the investigation of serious offences— or if it can be achieved 'through other, less restrictive means'.[2355]

After considering the proper balancing exercise, which is to fulfil the minimal internal threshold requirement, LEAs must consider the external aspects of the conduct of an OCI.[2356] One such factor is the consideration of the aims and objectives of the ECA, ECTA, RICA, POPIA, Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 and other law in an open and democratic society based on freedom, equality and dignity.[2357] The consideration of the ECA, ECTA, RICA, POPIA, Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 and other law will assist LEAs in striking a balance in the conflict between the right to the SOC and the conduct of an OCI.

[2350] *State v Makwanyane* supra 123 and 128 (Chaskalson P); Currie and De Waal *Bill of rights* 170-172.
[2351] *State v Makwanyane* supra 123 and 128 (Chaskalson P); Currie and De Waal *Bill of rights* 170-172.
[2352] Chapter 2 of this study.
[2353] *Web Call v Botha* supra 18; *Lock International Plc v Beswick and Others* [1989] 1 WLR 1268 (Ch) at 1280-1283; *CBS Butler Ltd v Brown & Ors* [2013] EWHC 3944 (QB) 32; (CCT25/99) [2000] ZACC 5; 2000(3)SA; 2000(5)BCLR 491 32; Du Plessis M and Penfold G 'Bill of rights jurisprudence: Operational provisions of the bills of rights (2008) *Juta's Annual Survey of South African Law* 50; De Vos (ed) '*Constitutional law'* 375.
[2354] De Vos (ed) *Constitutional Law* 375 ; Paras 6.4-6.6 of Chapter 6 of this study.
[2355] De Vos (ed) *Constitutional Law* 375 and 384; *R v Collins* supra 138 and *R v Feeney* supra 37.
[2356] See another version of the examination of this principle in para 5.2.3.1 of this chapter.
[2357] *Christian Education v Minister of Education* supra 43; *Islamic Unity Convention* supra 42-43; De Vos (ed) *Constitutional Law* 375.

Another factor to be considered is the prevailing or frequent state of the commission of serious offences in the balancing and proportionality process[2358] while conducting an OCI. It is submitted that where there is an increase in the commission of a serious offence or where more people become victims of a minor offence, there is a higher tendency to also embark on an OCI at an early stage of the commission of such minor offence, thus elevating such minor offence to temporarily be regarded as a serious offence.[2359]

For example, statistics show that there is an increase in the organised crime of dealing in hard drugs —which is a serious offence anyway— in South Africa,[2360] thus the more frequent use of an OCI may be more justifiable in this regard than before. Another example where a minor offence is temporarily elevated to be a serious offence is where the commission of such a minor offence may temporarily lead to the declaration of a state of emergency or where such minor offences *actually* and potentially threaten the State or public safety and security.[2361]

The 'less restrictive alternative means' can also be expressed in terms of the adequate formulation of the notion of 'reasonable accommodation'.[2362] In applying the notion, it is submitted that the notion generally inquires about and supports the view that reasonable accommodation of less restrictive means is usually or generally available and possible to use[2363] in the investigation of serious offences without resorting to the conduct of an OCI. It is however submitted that though less restrictive means might be available and possible to use in some most serious offences —for example, in terrorism and high treason cases, it is not proportionate to use a non-OCI in the investigation of these two serious offences since it may not meet the desired expectation of the investigation of these two serious offences.[2364]

Arguably, it is better for an invasion of the right to the SOC to occur where the consequences of the intrusion of online communication are irreversible than to protect the right to the SOC where the consequences —of the commission of the offences of terrorism and high treason, for example— are most likely to be irreversible particularly where lives and property are involved.

[2358] *S v Nombewa* supra 396 (E) 423 c-e.
[2359] Paras 6.3.2 and 6.3.3.2 (e) of Chapter 6 of this study.
[2360] Hosken G et. al. 'SA blows Nigeria away as drug capital-Organised crime rampant, Statistics show' *The Times* September 30, 2015 1-2.
[2361] Para 6.3.2 and 6.3.3.2 (a) – (f) of Chapter 6 of this study.
[2362] De Vos (ed) *Constitutional law* 372. Para 5.3.4.3 of this chapter.
[2363] De Vos (ed) *Constitutional law* 372.
[2364] De Vos (ed) *Constitutional law* 372. See the early part of this rubric where similar explanation was made but under a different principle.

This is because there is no degree of the limitation of the right to life,[2365] given that the more likely effect of the commission of terrorism and high treason is irreversible neither can it be done in layers as opposed to the right to the SOC which can be proportionately limited according to the continuum of secrecy interests in online communication.

Furthermore, the Constitutional Court gives serious consideration to the principle of reasonable accommodation in the *Christian Education v Minister of Education*[2366] wherein its inquiry on how far democracy should allow religious societies obey or not obey the law of the land. In its response, the Court held that the law of the land should not force a religious believer to choose between the law of the land and the law of their belief, thus the former should reasonably accommodate the latter.[2367]

In applying this principle to this study, it is submitted that where it is 'reasonably possible' in limiting the right to the SOC, LEAs should not force individuals into 'extremely painful and intensely burdensome choice of putting' information either in online communication or into other channels of privacy communications.[2368] In other words, an individual should have the absolute freedom of choice of channel of privacy communication. In a case reported by an investigative journalist, it was revealed that the team that worked on a corruption 'made as little use of electronic communication as possible' because the team did not see any safety or security in the use of online communication.[2369]

The 'reasonable accommodation' notion, which is a unique concept is an exercise in the 'reverse proportionality' process.[2370] It shifts the emphasis from negative protection to positive protection.[2371] LEAs should, in the process of using an extensive or far restricting means (such as the conduct of an OCI, which is a negative approach), also consider the protection of the

[2365] *State v Makwanyane* supra 351.
[2366] *Christian Education v Minister of Education* supra 35.
[2367] *Christian Education v Minister of Education* supra 35; De Vos (ed) *Constitutional law* 378.
[2368] *Christian Education v Minister of Education* supra 35; *MEC for Education: Kwazulu-Natal and Others v Pillay* (CCT/5106) [2007] ZACC 21;2008(1) SA 474(CC), 2008(2) BCLR 99(CC) 73 (*MEC Education: KZN v Pillay*); De Vos (ed) *Constitutional law* 378.
[2369] Right2Know 'Spooked- Surveillance of journalists in SA' at 7 and 9-11 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018) (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).
[2370] De Vos (ed) *Constitutional law* 378. Para 5.3.4.3 of this study.
[2371] De Vos (ed) *Constitutional law* 378. Para 5.3.4.3 of this study.

right to the SOC which essentially implies that limiting authority —such as LEAs— must use a less restrictive alternative means -positive approach.[2372]

Essentially, the question is, whether LEAs have done enough to reasonably accommodate those rights that the ECA, ECTA, RICA, POPIA, Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 and other law infringe?[2373] In other words, the shift in responsibility arises from the shift from the justifiability of the use of an OCI —that is, whether LEAs have gone too far in limiting the right to the SOC— to the justifiability of the effect of the conduct of an OCI on an individual or society, that is, whether LEAs should have taken steps to protect the right to the SOC in contemporary society.[2374]

Where a reasonable accommodation can be understood as a 'reverse proportionality' enquiry, the question is not whether a limiting authority —such as LEAs— can find a less restrictive means,[2375] but whether the less restrictive means should be employed keeping in mind all the requirements which include the cost to society?[2376]Arguably, in addition to the earlier consideration of cost, the cost to society can be divided into two. Firstly, the cost to LEAs, which is the cost of conducting an OCI. Secondly, the cost to the individual, which is the comprehensive and irreversible consequence of intrusion of the right to SOC.

Finally, despite the difficulty in drawing a line around the workability of 'reasonable accommodation' test, the courts have set some guiding principles in form of enquiries.[2377]

First of all, according to the decision of the Constitutional Court in *MEC Education KZN v Pillay,*[2378] the enquiry is, whether a school authority would reasonably accommodate a pupil to put a nose ring in school in pursuance of his religious belief?[2379] In applying this principle, an OCI will reasonably be accommodated to investigate various categories of offences based on the observance of the continuum of secrecy of online communication interests and vice

[2372] Section 7(2) of the Constitution; De Vos (ed) *Constitutional law* 372- 373; See also para 5.3.4.3 of this study on the 'reverse proportionality enquiry'.
[2373] De Vos (ed) *Constitutional law* 380.
[2374] *Christian Education v Minister of Education* supra 32; De Vos (ed.) *Constitutional law* 378.
[2375] De Vos (ed.) *Constitutional law* 372-373. Section 7(2) of the Constitution. See para 5.3.4.3 of this study.
[2376] De Vos (ed.) *Constitutional law* 373. See also the earlier examination of cost from the proportionality test perspective in this rubric.
[2377] *MEC Education KZN v Pillay* supra 79; De Vos (ed) *Constitutional law* 379.
[2378] *MEC Education KZN v Pillay* supra 79; De Vos (ed) *Constitutional law* 379.
[2379] *MEC Education KZN v Pillay* supra 79; De Vos (ed) *Constitutional law* 379.

versa.[2380]

The second enquiry is, what is the importance of the practice of putting on nose ring by a pupil and how does the permission of the use of a nose ring 'cause undue burden upon the school'?[2381] In applying this principle, the importance of the uses of online communication devices is economically and socially indispensable, and inevitable in contemporary society[2382] which does not cause any undue burden to the society except where individuals misuse or abuse the usage of online communication devices.[2383]

Furthermore, turning the reasonably accommodating principle around amid all investigative procedures, the use of an OCI will not create an undue or unnecessary burden on the individual who enjoys the right[2384] to the SOC provided an OCI is conducted in accordance with the level of seriousness of an offence.

5.3.6.2 Well-tailored enquiry

In the 'well-tailored' enquiry;[2385] it considers whether the choice of a limiting measure —such as the conduct of an OCI— by LEAs is well-tailored —proportionate— for the purpose[2386] of investigating all classes of serious offences which, to some extent, is answered in the affirmative.

However, it is submitted that it would be very 'well-tailored'[2387] to achieve an effective investigation if an OCI was conducted according to the specific degree of serious offences.[2388] This enquiry is made possible where all relevant factors are considered and not only when the effect of the measure on the right is considered.[2389] Usually, if the limiting measure —such as

[2380] See the Continuum of privacy interest at para 3.4 of Chapter 3 of this study.
[2381] *MEC Education KZN v Pillay supra* 79; De Vos (ed.) *Constitutional law* 379. *R v Collins* supra 138; Van der Merwe *Unconstitutionally obtained evidence* 257.
[2382] *Riley v California* and *U.S v Wurie* supra 9, 16-17 and 28 of the Opinion and p 6 of the minority decision by Alito J.
[2383] *Riley v California* and *U.S v Wurie* supra 25.
[2384] *MEC Education KZN v Pillay* supra 85, 112, 162 and 156; De Vos (ed.) *Constitutional law* 379.
[2385] De Vos (ed.) *Constitutional law* 372.
[2386] De Vos (ed.) *Constitutional law* 372; See also submission on the similar statement on reverse proportionality enquiry in para 5.3.6.1 of this study.
[2387] See the earlier part of this paragraph where 'tailored-made' enquiry is examined; See para De Vos (ed.) *Constitutional law* 377.
[2388] See para 6.3.3 of this study on the specific classification of serious offences.
[2389] De Vos (ed.) *Constitutional law* 372.

an OCI— fails, it is not because it is disproportionate to the protection of a right —including the right to the SOC, instead, it is because a limiting measure —such as an OCI— is not well-tailored to achieve an effective purpose[2390] in the criminal investigation of all the serious offences.

5.4 FORMS OF PROPORTIONALITY TEST IN THE RIGHT TO THE SECRECY OF ONLINE COMMUNICATION AND CRIMINAL INVESTIGATION

5.4.1 Introduction

This study conceptualises five forms of proportionality tests —amongst others— that are applicable to the right to the SOC or the conduct of an OCI or simultaneously applicable to both.

5.4.2 Proportionality of continuum of secrecy of online communication principle

The proportionality of continuum of the SOC principle is derived from one of the core aspects of the concept of the SOC examined in this study titled 'Reasonable continuum of secrecy of online communication interests'.[2391] This form of proportionality test operates where an individual exercises the liberty to place information in any of the sanctum in the continuum of SOC according to his or her subjective expectation of the right to the SOC, which is subject to the objective reasonableness of the SOC by the society. For example, if a user places a 'will' or 'testament' in a 'dropbox' without the intention of sharing the information with anybody, such 'will', or 'testament' is presumed to be placed at the innermost sanctum of the SOC where the information is not shared with other people.[2392]

In applying the proportionality of continuum of SOC principle to this study, a LEA is allowed to proportionately intrude into the innermost sanctum to investigate the state of emergency

[2390] *National Defence Union v Minister of Defence* supra 11; De Vos (ed) *Constitutional law* 377.
[2391] Paras 3.7 and 3.8 of Chapter 3 of this study.
[2392] Para 3.8.2 of Chapter 3 of this study. Dropbox is an online communication that basically enables one to save an information in the cloud, though has an option that enables one to share the information saved in a Dropbox with other people.

offences and offences that constitute an actual or potential threat to the sovereignty of the RSA and public safety and health of the people of the RSA.[2393]

5.4.3 Proportionality of the investigator capacity-based principle

Given the high-level risks that online communication is exposed to, there is no classification of authority and competence of the members and officers appointed to conduct an OCI[2394] that proportionately correspond with the investigation of the conceptualised six classes of serious offences according to the authority and competence of the appointed LEOs. The non-classification lowers the competence threshold required for the proportionate investigation of the six classes of serious offences by LEOs.[2395] Similarly, Canada, U.K and U.S. do not have designated LEOs for the investigation of the six classes of serious offences according to their level of authority and competence. However, UNODC 'Model Legislative Provisions Against Organised Crime 2012 provides for the employment of senior officials to conduct an OCI,[2396] which is commendable.

In pursuance of the combined effects of the competence requirement stipulating the minimum official designation of LEOs who are qualified to conduct an OCI,[2397] a proportionality of investigator capacity-based principle is required in the specific classification of serious offences[2398] and the standards of proof required to conduct an OCI —amongst other factors. This principle requires that the more serious an offence, the more skilful capacity a LEO

[2393] Paras 6.3.3.2–6.3.3.5 and 6.4-6.6 of Chapter 6 of this study; Sections 6(1)(c)(i) and 37(1) of the POPIA.

[2394] Section 33 of SAPSA, section 1 of the DA, section 1 of the ISA. Any member of IPID is allowed to conduct OCI procedure, see section 22(3)-(9) of IPIDA. Though sections 1, 3, 8, 9 and 19 of the ISA describe who a member is, RICA does not classify the level or seniority of membership despite the identification or recognition of senior member of SSA in the definition section of the ISA, Chapter 1 of Para 1(2) of Regulation 7797 Notice No. 1505 Gazette No 25592 titled 'Ministry for Intelligence Services' Intelligence Services Act No of 65 of 2002. Membership of SSA does not extend to cadet, see Chapter VI Para 5(3) of Regulation 7797 Notice No 1505 Gazette No 25592. Clearance level is provided in Chapter XXVI of Para 2(1) (a), (b) & (c) of Regulation 7797 Notice No 1505 Gazette No 25592. Chapter XXVI of Para 8 of Regulation 7797 Notice No 1505 Gazette No 25592 provides for the withdrawal, downgrading or refusal to grant security clearance by the authorities. The definition of 'law enforcement agency' in section 1 of RICA also does not define who is a member of the National Director of NPA, thus a lacuna on the competence of the applicant in RICA; IPIDA does not define who a member of their institution is, thus creates a lacuna on the competence of the applicant in RICA.

[2395] Alberti A A *Wiretapping: A Complete Guide for the Law and Criminal Justice Professional* (1999) 10 ('Alberti *Wiretapping*').

[2396] Art 16(4) of the UNODC 'Model Legislative Provisions Against Organised Crime' 2012.

[2397] See the definition of applicant in section 1 of RICA.

[2398] Para 6.3 of Chapter 6 of this study.

possess —particularly in the techno-legal qualification—[2399] to conduct an effective and efficient OCI.

For example, a very senior officer of a LEA, whom of course must be highly, formally, professionally and academically qualified to conduct an OCI, is competent to conduct an OCI in a 'state of emergency offence'. Further, an ordinary officer or the equivalent as defined in section 1 of RICA[2400] with the relevant academic qualifications in the conduct of an OCI, is competent to conduct an OCI of general serious offences.[2401]

It is therefore recommended that the various categories of LEAs should appoint different layers of investigating officers —between the ranks of at least commissioned officers but lower than top management position—[2402] indicating the mandate of each officer according to the seriousness of offences to be investigated,[2403] amongst other criteria. The reason for appointing officers in this category is to ensure that junior officers —who may ordinarily not be techno-legally efficient, competent or qualified— and top management officers —who are usually pre-occupied with strategic issues and meetings— are not involved in the complex and strict operational conduct of an OCI.

5.4.4 Proportionality of the seriousness and class or stage of crime commission principle

In pursuance of the Constitutional Court case of *Investigating Directorate v Hyundai and Smit No*,[2404] the proportionality of seriousness and class or stage of crime commission principle is premised on the proportionality of continuum of SOC principle[2405] because based on minimal facts gathered in the standard of proof required from a LEO, an OCI is conducted earlier in a more serious offence.

[2399] Para 5.3.3.1 of this chapter. Although the Court in *Suzman Foundation v Min of Police* supra 66 held that LEOs are not required to possess a legal qualification to conduct an investigation in the offline world, however, the HC proves otherwise in *State v Naidoo* supra 521 B-E, see also para 4.3.3 of Chapter 4 of this study.

[2400] See the definition of applicant in section 1 of RICA.

[2401] Para 6.3.3.2 (f), 6.3.3.3(b), 6.3.3.4(d) and 6.3.3.5(g) of Chapter 6 of this study.

[2402] See paras (a)-(c) of the definition of 'applicant' in section 1 of RICA and section 33 of SAPS, section 1 of DA and section 1 of the ISA. The purpose of limiting the LEOs to this category is to ensure that low rank members and top managers who may not be competent and who are too busy respectively be involved in the conduct of OCI.

[2403] Paras 7.2, 7.3 and 7.5.4 of this study.

[2404] *Investigating Directorate v Hyundai and Smit No* supra 1, 2, 4, 6, 7, 8, 13, 14, 27, 28, 30, 31, 33, 34, 44, 45, 46, 47, 48, 51 and 52.

[2405] Para 5.4.2 of Chapter 5 and paras 3.7 and 3.8 of Chapter 3 of this study.

For example, an OCI is conducted earlier at the innermost sanctum of the SOC in the commission of a 'state of emergency offence' than other categories of offences, the investigations of which are conducted later with more facts required to be gathered by a LEO or higher standard of proof required from a LEO to conduct an OCI in such latter offences.[2406] This principle further emphasises the significance of the specific classification of serious offences and the substantive and procedural standards of proof required for the conduct of an OCI.[2407]

5.4.5 Proportionality of duration of the conduct of online criminal investigation principle

Three months and five days general statutory duration of the conduct of an OCI are stipulated in RICA and the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 respectively,[2408] in which this study has proven as unreasonable, irrational and unjustifiable in conducting an OCI in all offences despite the seriousness of such offences.[2409] It is also unreasonable, irrational and unjustifiable to conclude concerning this principle that the law, should in all classes or stages of serious crime commission, rigidly adhere to the reduced period of the conduct of an OCI of *two days* in *State v Naidoo,* where an employee of MTN handed over a transcript to a captain in SAPS within two days;[2410] *three days* to access data in the investigation in Macozoma case[2411] and *twenty minutes* in downloading data in an offline device in *State v Terrence Brown*.[2412]

The proportionality of the duration of the conduct of an OCI principle stipulates that the duration of the conduct of an OCI should generally be based on the seriousness of an offence and should not be based on a rigid period of three months or five, three or two days. This principle is to ensure that the intrusion into the right to the SOC is proportionate to the period

[2406] Paras 6.3.3.2 (a)-(f) and 6.4.4 - 6.4.9 of Chapter 6 of this study.
[2407] Paras 6.3 - 6.6 of Chapter 6 of this study.
[2408] Sections 16(6)(d), 17(1), 20(3)(a) and (b), (4), (5) and (6) and 21(5)(e) of RICA and s 20(3)(a) & (b)(i) and (7)(a) of CCB B6-2017, whereas the latter is replaced by ss 21(3)(a) & (b)(i) and (7)(a) of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017. Paragraphs 89-97 of Section III (Explanatory Notes to Model Legislative Text on Interception of Communication) of ITU 'Interception Policy & Legislative Text' (2012).
[2409] Para 6.3 of Chapter 6 of this study.
[2410] *State v Naidoo* supra 521 B-E.
[2411] NIA 'Investigations on Mr. Macozoma' 13 and 20; *Helling v Mag* supra E at 101. See also para 3.5.7.7 of Chapter 3 of this study.
[2412] *State v Terrence Brown* supra 6 and 8.

that LEOs are allowed to conduct an OCI based on the seriousness of an offence, the minimum of which this study recommends as *two-three minutes* of conducting an OCI.[2413]

5.4.6 Proportionality of the use of devices, technologies, networks, applications and services principle

Given that the invention, development and interoperability of devices, technologies, networks, applications and services cannot be controlled or predicted, it is difficult to allocate the investigation of a particular category of a serious offence to the use of a particular device, technology, network, application and service, unlike the other proportionality principles which can be proportionately classified as examined above. However, it is reasonable to propose that the more serious an offence, the more devices, technologies, networks, applications and services are employed to conduct an OCI.

In February 2019, Mark Zuckerberg, the owner of the three most massively used and popular social media platforms on the globe announced the interoperability of 'Facebook', 'WhatsApp' and 'Instagram'.[2414] This interoperability enables the scalability of the three platforms and ensures that a user can communicate with one another on the three platforms without necessarily installing the software application of the other two platforms.[2415]

The interoperability of any of the devices, technologies, networks, applications and services makes the application of the proportionality principle in this regard difficult in terms of the issuance of court direction. This is because before the interoperability concept, a separate OCI direction would proportionately be issued in each of the devices, technologies, networks, applications and services subject to the seriousness of an offence. However, under an interoperability regime, the issuance of an OCI direction in respect of two or more interoperable devices, technologies, networks, applications and services which consider these two or more interoperable devices, technologies, networks, applications and services under one OCI direction will amount to an infringement of the right to the SOC.

[2413] Para 3.5.7.8 of this study.

[2414] Francis J 'Facebook's convergence conundrum- Merging Facebook Messenger, WhatsApp and Instagram is a risky gamble and there isn't a good enough reason to do so.' https://www.itweb.co.za/content/mYZRXv9Ppd8qOgA8 (Date of use: 12 February 2019 (Francis https://www.itweb.co.za/content/mYZRXv9Ppd8qOgA8 (Date of use: 12 February 2019).

[2415] Francis https://www.itweb.co.za/content/mYZRXv9Ppd8qOgA8 (Date of use: 12 February 2019).

This is because the several OCI directions which should have been issued as separate directions according to the seriousness of an offence are lumped up in one or interoperable OCI direction. By so doing, a LEA will be gathering more information than is necessary for the class of a serious offence committed because using all the devices, technologies, networks, applications and services to conduct an OCI of any serious offence will be disproportionate. This is because there may be a greater revelation of data than is necessary for the purpose for which an OCI is conducted.

Therefore, an interoperable OCI direction takes away the right of an individual to benefit from the application of proportionality principle, which should have proportionately considered the objective or meritorious use of the other devices, technologies, networks, applications and services side by side the seriousness of an offence as a basis for the number of devices, technologies, networks, applications and services to use in the investigation of such a serious offence.

However, despite the difficulty in applying the proportionality principle under this rubric, the court will still reasonably, justifiably and generally consider the fact that the more serious an offence, the more devices, technologies, networks, applications and services will be applicable to conduct an OCI. For example, it is submitted that in state of emergency offences,[2416] it is reasonable and justifiable to proportionately conduct an OCI in all interoperable devices, technologies, networks, applications and services.

5.5 CONCLUSION

In pursuance of the provision of section 36 of the Constitution, the right to the SOC —as opposed to the right in non-online communications— is limited by the need for LEAs to conduct an OCI in serious offences enumerated in the only schedules of RICA, Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 and other law. The extent to which LEAs conduct an OCI is determined mainly by the proportionality[2417] and incremental[2418] principles, which integrate and summarise other principles in s 36 of the Constitution.

[2416] Paras 3.7, 3.8, 6.3.2, 6.3.3.2(e), 6.3.3.3(e), 6.3.3.4(d), 6.3.3.5(e) and 6.4.5 of this study.
[2417] *State v Makwanyane* supra 104.
[2418] *Magajane v North West Gambling Board* supra 50.

In applying these principles, the more serious an offence, the more intrusive LEAs are allowed to invade the continuum of the SOC interests of an individual in the complex and delicate non-compartmentalised, non-passworded compartmentalised, interoperable and conscriptive online communication devices, technologies, networks, applications and services comprising both content and non-content data.

> Even in the aves kingdom, an eagle, as a watchdog representing the public interests in the kingdom, is, according to the rules of natural justice, required to systemically invade the secrecy of the affable, flaccid and orderly bee hummingbirds who are mating, save in emergencies and other special circumstances which do not require a knock at the door to intrude.

CHAPTER 6: APPLICATION FOR AND ISSUANCE OF AN ONLINE CRIMINAL INVESTIGATION DIRECTION

6.1 INTRODUCTION

Having arguably established the reality of protecting the right to the SOC[2419] which is limited by the conduct of an OCI[2420] in the protection of the 'public criminal interests'[2421] by LEAs whose affairs and activities are inadequately managed,[2422] this chapter examines the substantive and adjectival requirements for the application and issuance of a direction for the conduct of an OCI[2423] in the RSA.

6.2 TYPES OF ONLINE INTERCEPTION

6.2.1 Introduction

Save as provided by RICA and other law in the permissible instances below,[2424] there is a prohibition of intentional or attempted interception of online communication by any person in

[2419] Chapter 2 and 3 of this study.
[2420] Chapter 2 and 5 of this study.
[2421] Para 3.1 of Chapter 3 of this study; *Bosasa Operation (Pty) Ltd v Basson and Another* (09/29700) [2012] para 55 (*Bosasa v Basson*).
[2422] Chapter 4 of this study.
[2423] Reed *Internet law: Text and materials* at 106 where it states that lawmakers erroneously believe in the principle that the legal norms which regulate the physical world should, where possible, as well regulate cyberspace. The concept is more usually expressed by saying that both online and offline activities should be treated equally.
[2424] Paras 6.2.2 - 6.2.7 of this chapter.

the RSA in section 2 of RICA.[2425] However, section 2 of RICA is not properly couched because it impliedly does not create express protection of archived online communication by virtue of the use of the expression 'in the course of its occurrence or transmission', though it is impliedly and ultimately protected, drawing on the U.S. principle which dynamically protects archived online communication.[2426]

In the U.S., both real-time and archived communications are protected, though there is a higher burden of proof that is required by LEAs to conduct an OCI of real-time communication than in an archived communication. [2427] LEOs circumvent this requirement by ensuring that real-time communication is stored first and thereafter conduct an OCI immediately a real-time communication is recorded or stored because the standard of proof in archived communication is not as high as that of the real-time communication.[2428] Drawing on the foregoing discussion in the U.S. practice, it is submitted that although the prohibition of the conduct of an OCI in an archived communication may not be protected in section 2 of RICA but it is protected in other provisions of RICA.[2429]

It is finally noted that though the conduct of an OCI is a segment of the broader concept of interception,[2430] some of the following types of interceptions may have some features of an OCI and the general features of an intercept.

6.2.2 Non-consensual party intercept without a direction

Non-consensual intercept occurs where parties to online communication —including a LEO- may, without the intervention of an Online Communication Service Provider— save for the general technical or operational provisioning of an online communication network and Interception Centre[2431] intercept their online communication without any requirement of consent from the other party.[2432] Parties in this rubric are not allowed to intercept online

[2425] Section 2 of RICA. For the definition of interception, see section 1 of RICA.
[2426] Para 2.7.1 of Chapter 2 of this study.
[2427] Para 2.7.1 of Chapter 2 of this study.
[2428] *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d 827, 840 (S.D.Tex. 2010); Crump *Geolocational Privacy and Surveillance Act* 280-281. Para 2.7.1 of Chapter 2 of this study.
[2429] Sections 12, 13, 14, 15, 16, 18, 19 and 20 of RICA, amongst others.
[2430] Paras 2.5.1-2.5.3 of Chapter 2 of this study.
[2431] Section 1 of RICA.
[2432] Section 4 of RICA.

communication for purposes of committing an offence.[2433]

Where a party in the online communication is a LEO, the relevant standard of proof must be complied with as examined in this study to investigate a serious offence[2434] and not following the contradictory rigid standard created in section 4(2)(b) of RICA which strictly locates the standard of proof on 'belief' standard alone as opposed to the other standards of proof examined in this study.[2435] In the case of a private person in section 4, such a person is arguably not bound by the same condition that binds a LEO in the interception of online communication in the other leg of section 4 of RICA.

Although a LEO under section 4(2)(b) of RICA is allowed to conduct an intercept on the grounds referred to in section 16(5)(a) of RICA, section 4 does not require a direction to intercept an online communication. This is because section 4 does not require parties to place a request to an Online Communication Service Provider for an interception as it may be required in other instances where LEOs are involved in an online intercept, neither are parties in section 4 allowed to be in possession of interception device. However, the parties are permitted to record or are capable of recording online communication in which they are privy to, therefore, no direction is required for parties to intercept an online communication in section 4 of RICA.

6.2.3 Consenting party intercept without a direction

Parties in online communication —including a LEO— may, without the intervention of an Online Communication Service Provider —save for the technical or operational provisioning of an online communication network— and the Interception Centre,[2436] intercept their online communication with prior written consent from the other party.[2437] The examination of section 4 of RICA applies *mutatis mutandis* in the remaining part of the examination of section 5 of RICA.[2438]

[2433] Section 4(1) and (2) of RICA.
[2434] Paras 6.3-6.6 of this chapter.
[2435] Paras 6.3-6.6 of this chapter.
[2436] Section 1 of RICA.
[2437] Section 5 of RICA.
[2438] Para 6.2.2 of this chapter.

Section 6 of RICA is another form of consensual interception which occurs where a party may, without the intervention of an Online Communication Service Provider (save for the technical or operational provisioning of an online communication network) and Interception Centre (as defined in RICA)[2439] relating to the conduct of business and with the express or implied consent of a party using the online communication and the system controller, intercept an online communication.[2440]

Section 6 is to ensure that the records of an online communication are monitored and kept to establish that some facts exist, or are meant to investigate or detect the unauthorised use of an online communication system and that the system is securely and effectively operated.[2441] Section 6 is also meant to monitor indirect communication in a confidential free of charge voice telephone communication counselling or support service where a user is anonymous.[2442]

6.2.4 Emergency intercept without a direction

A LEO may, without a direction, intercept an online communication or orally request an Online Communication Service Provider to route the duplicate signals to an Interception Centre to intercept an online communication in a bid to prevent serious bodily harm.[2443] In addition, a party to an online communication —including a LEO— may, without a direction, inform a LEO or cause someone to inform a LEO or 'orally request' or 'cause another' LEO to orally request an Online Communication Service Provider to determine the location of a user of online communication in times of emergency and to intercept an online communication of the rescued party.[2444]

For example, an emergency arguably includes a scenario where a person is on the run for testing positive at a clinical or medical laboratory for the deadly coronavirus pandemic[2445] which does

[2439] Section 1 of RICA.
[2440] Section 6 (1) (a)-(c) and (2)(a)-(d) of RICA.
[2441] Section 6(2)(b)(i) of RICA.
[2442] Section 6(2)(b)(ii) of RICA.
[2443] Section 7(1)(c) and (2) of RICA.
[2444] Section 8(1) (i) &(ii), (2) and (3) of RICA. In the U.S., the authorities may, among other circumstances, intercept an online communication where there is an 'immediate danger of death or serious physical injury to any person' and where a parent gives consent to the interception of the device of a child. However, the law is silent on the regulation of consent concerning 'mental handicaps, developmental abilities, dementia' or someone 'on medication', Cassilly *Geolocational Privacy and Surveillance Act*) 266-268.
[2445] Disaster Management Act 2002: Amendment of Regulations Issued in Terms of Section 27(2) in Gazette No 43148 of 25 March, 2020 (DMA COVID-19 Regulation of 25 March, 2020) and paras 11H(6)(A) and (7) of

not require a direction from the court.[2446] Another instance where a court direction is not required is where there is a self-declaration by a priest who tested positive for COVID-19 which he contracted at a large church gathering.[2447] The LEAs are required to trace and track down other congregants[2448] who attended the mass church service.[2449]

In these two instances, a judge and a designated judge in the oral and written physical application,[2450] including the operation of a designated judge in an emergency intercept without a direction,[2451] oversee the activities of the health and other ancillary departments and workers and,[2452] through Online Communication Service Provider, trace and tract the online communication of corona virus clinical cases as described in this study.[2453]

The only purpose of tracing and tracking[2454] in these scenarios is to ensure the administration of medical solution[2455] and thereafter delete such data not later than six weeks of gathering such data.[2456] This is one of the instances where an interception of the geographic traffic or

---

the Disaster Management Act 2002: Amendment of Regulations Issued in Terms of Section 27(2) in Gazette No 43199 of 2 April, 2020 (DMA COVID-19 Regulation of 2 April, 2020).

[2446] Section 8 of RICA; Para 11H (10) (a) and (b) of COVID-19 Regulation of 2 April 2020.

[2447] SABC News 'ACDP leader Reverend Kenneth Meshoe tests positive for coronavirus' https://www.sabcnews.com/sabcnews/acdp-leader-reverend-kenneth-meshoe-tests-positive-for-coronavirus/ (Date of use: 28 March 2020); Paras 11H(2), (3)(c) and (10)(a) & (b) of COVID-19 Regulation of 2 April 2020.

[2448] SABC News 'ACDP leader Reverend Kenneth Meshoe tests positive for coronavirus' https://www.sabcnews.com/sabcnews/acdp-leader-reverend-kenneth-meshoe-tests-positive-for-coronavirus/ (Date of use: 28 March 2020); Paras 11H(2), (3)(c) and (10)(a) & (b) of COVID-19 Regulation of 2 April 2020.

[2449] Maduna M of Power Digital 'Duduza Clinic remains closed after nurse tests positive for corona virus' https://www.power987.co.za/news/duduza-clinic-remains-closed-after-nurse-tests-positive-for-coronavirus/ (Date of use: 3 April 2020).

[2450] Paras 6.7 and 6.8 of this chapter.

[2451] Para 6.2.4 of this chapter. See section 8 of RICA, more particularly section 8(6).

[2452] The Director-General of the Department of Health is empowered to conduct the track and trace interception, Hunter and Thakur https://www.news24.com/Columnists/GuestColumn/advocacy-new-privacy-rules-for-covid-19-tracking-a-step-in-the-right-direction-but-20200404-2 (Date of use: 6 April, 2020.

[2453] SABC News 'Lamola appoints Justice Catherine O'Regan as COVID-19 designate judge Lamola appoints Justice Catherine O'Regan as COVID-19 designate judge' available at https://www.sabcnews.com/sabcnews/lamola-appoints-justice-catherine-oregan-as-covid-19-designate-judge/ (Date of use: 5 April, 2020; O'Regan K and McKaiser E 'Regulation is clear, information contained will only be used to fight COVID-19'Regulation is clear, information contained will only be used to fight COVID-19'' http://www.702.co.za/articles/379998/regulation-is-clear-information-contained-will-only-be-used-to-fight-covid-19 (Date of use: 6 April 2020) (O'Regan and McKaiser http://www.702.co.za/articles/379998/regulation-is-clear-information-contained-will-only-be-used-to-fight-covid-19 (Date of use: 6 April 2020).

[2454] Para 11H(10)(a) & (b) of COVID-19 Regulation of 2 April 2020.

[2455] Paras 11H (11) (b) of COVID-19 Regulation of 2 April 2020.

[2456] Paras 11H(11)(d) of COVID-19 Regulation of 2 April, 2020; The Director-General of the Department of Health is empowered to conduct the track and trace interception, Hunter M and Thakur C 'Advocacy: New privacy rules for Covid-19 tracking a step in the right direction, but

geo-locus data[2457] can be conducted on such congregants or participants because the convention at a rendezvous, 'assembly, concourse or procession' constitutes an offence under the Regulation.[2458]

It is important to note the contradiction between paragraphs 11H(11)(d) and 11H (16) of COVID-19 Regulation of 2 April, 2020 on the deletion of data of a tracked person and the issuance of a notice of tracking of data of such a person. The contradiction is that, of what benefit or use is it for a tracked and traced person whose tracked and traced data is deleted within 6 weeks of gathering tracked data in paragraph 11H(11)(d)? This is because the tracking could have happened on the first day of the state of disaster while the person tracked is only informed within 6 weeks of the conclusion or termination of the state of disaster in paragraph 11H(16), which could be extended beyond the initial 21 days, which further denies the target the opportunity of knowing the exact details of the data tracked and traced before the deletion.

This is because, without an extension, the Minister of Health might, according to this Regulation, notify a target in the 1st week of the conclusion or termination of the state of disaster, which effectively, is the 7th week of the gathering of the tracked and traced data of a target. Thus, the data will not be available to the target because it is outside the 6 weeks of keeping the data after the tracking and tracing. This regulation denies the target of the track and trace the opportunity of knowing the gathered data, worse still, in an extension of the state of disaster.

This is because the data must have been deleted earlier than the time that the target becomes aware of the tracking and tracing. That is, the data must have been deleted at the eve of the week of the commencement of the period of notification of the gathered data. This, in a way, makes the notice void because there is no data that exists for the target to contest, should there be any need for such contestation, such as, whether the authorities should know the whereabouts of a target who visits a mental health facility as an out-patient —for example— during the state of disaster.

…' https://www.news24.com/Columnists/GuestColumn/advocacy-new-privacy-rules-for-covid-19-tracking-a-step-in-the-right-direction-but-20200404-2 (Date of use: 6 April 2020) (Hunter and Thakur https://www.news24.com/Columnists/GuestColumn/advocacy-new-privacy-rules-for-covid-19-tracking-a-step-in-the-right-direction-but-20200404-2 (Date of use: 6 April 2020).

[2457] Paras 2.6.2.1 and 2.8.3.3 of Chapter 2 of this chapter; Paras 11H (2), (3)(c) and (10)(a) & (b) of COVID-19 Regulation of 2 April 2020.

[2458] DMA COVID-19 Regulation of 25 March, 2020.

It is submitted that the LEAs cannot rely on an interception without a direction in an emergency described under this rubric to conduct a bulk or mass OCI without a court direction where same or similar facts do not exist as described above.[2459]

6.2.5 Online criminal investigation without a direction under the Correctional Services Act

Save in a privileged communication,[2460] an interception by an 'agency' authorised by the legislation[2461] of online communication between an inmate and a member of the public — including an online communication— occurs in any correctional facility in the RSA[2462] based on the rigid reasonable ground to 'believe' standard.[2463] The standard is determined by the Head of the Correctional Centre that the communications being intercepted contain or will contain a proof of an act or omission which will pose a risk to the safety and security of the correctional facility or a person; or the commission of a criminal offence or a plan to commit a criminal offence.[2464] There must also be a 'reasonable ground to believe' that the conduct of an OCI is the least restrictive means to gather evidence of crime committed in the circumstance.[2465]

Although the term 'agency' in the Regulation of the CSA[2466] is broad in this context, however, considering the context in which it should be used in RICA, it excludes the court from this process in terms of the express provision that the head of the prison or a correctional centre may determine the reasonable standard of proof.[2467] Therefore, though contested, a direction from the court is not required for obvious reasons that such a centre may not be placed under the general rule because of the severe security risk levels.

[2459] Para 6.13 of this chapter.
[2460] Para 6.15 of this chapter.
[2461] Agency as described by Regulation 8(4)(a) of Correctional Services Act (111/1998): Promulgation of Correctional Services Regulations with Amendments Incorporated No 35277 of 2012 (Correctional Services Regulation) will include the categories of agencies mandated to conduct an OCI in RICA save the court, see para 7.5.1 of Chapter 7 of this study.
[2462] Section 9 of RICA. See para 6.15.2 of this chapter where there is an examination of privilege communication between an attorney and a client inside and outside a correctional facility.
[2463] Paras 6.4.2.2, 6.4.8 and 6.4.10 of this chapter.
[2464] Regulation 8(4) (a) (i) &(ii) & (b) and (5) of Correctional Services Regulation; Chapter 2 Part 1 of RICA; Para 6.2.4 of this Chapter.
[2465] Regulation 8(4)(b) of Correctional Services Regulation.
[2466] Regulation 8(4)(a) of Correctional Services Regulation; Para 7.5.1 of Chapter 7 of this study.
[2467] Regulation 8(4) (a) (i) &(ii) & (b) and (5) of Correctional Services Regulation.

According to the provisions of RICA, it is arguable that a correctional facility will exclude all police stations or national key points. This exclusion is to ensure that bulk interception does not occur in every part of the RSA because there are many national key points. This impliedly means that almost everywhere that a user of an online communication reaches will encounter a mass intercept, therefore, not all national key points will qualify for protection under a mass interception.[2468]

For example, a mass interception in the National Assembly is not permitted in RICA even where the president of the RSA presents the State Of the Nation Address ('SONA') in the case of *Primemedia v Speaker, National Assembly*.[2469] The court criticised the National Assembly of the RSA for jamming the mobile cellular telephone and broadcast communication signals at the National Assembly precinct which denied public access to online and broadcast communications to the live social and TV broadcasts of the presentation of SONA because of the claimed security threat on the life of the erstwhile President of the RSA.[2470] Also, in *AmaBhugane*, the High Court held that bulk interception was unlawful.[2471]

6.2.6 Technical maintenance and monitoring intercept without a direction

Technical interception monitors signal to install or maintain facilities, apparatus or devices and monitors radio and signal frequency spectrum to manage the radio frequency spectrum.[2472]

The Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 prescribes the duty of Online Communication Service Providers and financial institutions to report the involvement of their computer systems in the commission of an offence to the SAPS not later than 72 hours of the commission of the offence. However, this provision does not impose an obligation on the Online Communication Service Providers and financial institution to monitor the data that is being transmitted or stored or to consciously solicit for information about an unlawful

[2468] Para 6.13 of this chapter.
[2469] *Primemedia v Speaker, National Assembly* supra 84(1)-(4); Para 6.13 of this study.
[2470] *Primemedia v Speaker, National Assembly* supra 84(1)-(4).
[2471] *AmaBhungane v Minister of Justice v Minister of Justice* supra 3, 14, 25, 143, 146, 147, 151, 152, 154, 155, 161, 162, 163, 164, 165, 167 and 168(6).
[2472] Sections 10 and 11 of RICA.

activity in online communication.[2473] Therefore, the duo cannot *suo moto* intercept online communication.

The provision for the reporting system corroborates with the key finding by this author at LL.M degree level which reveals that the liability of Internet Service Providers should not be limited in some circumstances including the protection of sound recording, given the exclusive obligation of an Internet Service Providers to filter, identify and detect an unlawful transmission of sound recording.[2474] This issue is now being addressed in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, which restores the partial liability of Internet Service Providers in the breach of an obligation to filter, identify and detect an unlawful transmission of online communication.[2475]

6.2.7 Online criminal investigation with a direction

As opposed to the above five types of interception which cater for specific instances of online communication interception,[2476] section 3 of RICA is a general or main provision which addresses the broad principle of OCI.[2477] An OCI is titled differently from the other forms of interception because the function that an OCI performs largely motivates the gravamen for the enactment of RICA and the rationale for the conduct of this study.

Section 3 lays the foundation for an interception of communication under an OCI direction to investigate a serious offence, as opposed to some of the other five types of interception which may not require a direction to intercept an online communication and may be used for other purposes other than the investigation of a serious offence.

[2473] Section 52(4)(a) & (b) of CCB B6-2017, which is replaced by section 54(4) (a) &(b) of the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017.
[2474] Popoola *Liability of ISPs* at ii, 1, 2, 6, 16, 17, 18, 85, 86, 90, 91, 92, 94, 106, 144, 184, 185, 192, 206 and 208; Section 79 of ECTA provides for the deviation of liability of Online Communication Service Provider provided in ECTA.
[2475] Section 20 of CCB B6- 2017, which is replaced by section 21 of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[2476] Paras 6.2.2 - 6.2.6 of this chapter.
[2477] Para 2.5 of Chapter 2 of this study.

6.3 SPECIFIC CLASSIFICATION OF SERIOUS OFFENCES AS A REQUIREMENT FOR THE APPLICATION OF PROPORTIONALITY PRINCIPLE IN ONLINE CRIMINAL INVESTIGATION APPLICATION

6.3.1 Introduction

Given the unimaginable and uncontrollable level of intrusion that LEAs or LEOs go in their bid to conduct an OCI in online communication,[2478] the specific classification of serious offences cannot be over-emphasised as a requirement for the reasonable, rational and justifiable application[2479] of the proportionality principle in an OCI application and execution.

6.3.2 Fluidity of the scope of restriction of online criminal investigation application to serious offences

According to the provisions of RICA, the conduct of an OCI is restricted to the investigation of serious offences only. However, the scope of the restriction is fraught with fluidity, uncertainty and contradiction.[2480]

[2478] Paras 2.3, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 3.4.4, 3.4.5, 3.5.7.6, 3.5.7.8, 3.7, 3.8 and 5.2 of this study.

[2479] *Davis v Secretary of State for the Home Department* [2015] EWHC 2092 (17/07/2005) at 114 cited in *AmaBhungane v Minister of Justice* supra 103.

[2480] According to State Security Agency 'About US' http://www.ssa.gov.za/AboutUs.aspx (Date of use: 13 February 2020) the following offences were given attention by SSA: terrorism, sabotage, subversion, espionage and organised crime; Du Plessis 'International Criminal Courts' 191. Since the Security Council regards economic sanction or coercion from other states as a serious violation of state sovereignty under the principle of non-intervention, it may threaten the political independence of the RSA, Resolution 2525 (XXV), Paust J and Blaustein A P 'The Arab-Oil Weapon-A threat to international peace' 1974 68 *AJIL* 410 (Paust and Blaustein 1974 68 *AJIL*), United States Comprehensive Anti-Apartheid Act of 1986 1987 26 *ILM* 111; 1986 Annual Survey 70, Barrie G N 'International law and economic coercion- A legal assessment' 1985-1986 11 *SAYIL* 40, Fergusson-Brown K 'The legality of economic sanctions against South Africa in contemporary international law' 1988-9 14 *SAYIL* 59; Nicaragua case 1986 ICJ Reports paras 244-5, Dugard *International law: SA* 497- 498. Mudaly L *Search and seizure of documents in the investigation of tax-related cases* (M. Tech dissertation Unisa 2011). In the case of *Estate Board v Auction Alliance* supra 42, the court classified and contrasted revenue and custom duties offences as more serious offences than money laundering relating to and financing of terrorist and related activities, without considering the grievous consequences of the latter offences. However, in *Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others* 2008 (2) SACR 421 (CC) paras 50, 124, 140, 142, 151-155, 160, 161, 167 and 221 (*Thint*), the Constitutional Court regards racketeering, corruption, fraud, money laundering and tax offences as serious offences that can be effectively and 'objectively' investigated unilaterally by a small number of senior NPA officials through specially designed search and seizure procedure in s 29 only, instead of section 28 procedure under NPA Act. Sections 28(13) and 28(14) of the NPA Act 32 of 1998, accordingly made provision for the 'preparatory investigation' of three categories of serious, complex and complicated offences via specially designed search and seizure procedure. The offences relate to corruption; organised crime and public safety offences and serious economic offences which are given prioritised and non-subjective investigation, see *Investigating Directorate v Hyundai and Smit No* supra 1, 2, 3, 44, 45, 46, 47, 48, 49, 51 and 53 and *Thint* paras 74, and 115 and 151-155. Section 16 (5)(a)(ii) of RICA.

While the Constitutional Court unanimously held in *SAPS v SAHRLC & Ors*[2481] that there is no distinction in the classification of serious offences in the domestic law of the RSA,[2482] it is submitted that the difficult determination of what constitutes a serious offence in terms of the conduct of an OCI is controversially defined because of the diverse purposes for which offences are classified.

The international definition of a serious offence is no exception because it is also difficult, uncertain, fluid and non-uniform to define a serious offence at this level,[2483] given the specific and deserving diverse societal and sovereign needs and phenomena in each jurisdiction of the comity of nations concerned in addressing the issues in their criminal justice systems.[2484]

See sections 24, 26, 27, 28, 29 and 195(1)(b) and (e) and Chapters 13 of the 1996 Constitution of South Africa, amongst others. Salifu U 'The Nigerian citizen's recent conviction in a Johannesburg high court of 13 terrorism charges confirms South Africa`s commitment to the global fight against terrorism.' https://issafrica.org/iss-today/henry-okah-counter-terrorism-ruling-is-a-judicial-triumph-for-south-africa-and-the-continent (Date of use: 12 June 2016); Paragraphs 2, 5, 6, 8, 9, 10, 15 and 16 of the only Schedule to RICA. Section 16(5)(a)(ii)-(iii) of RICA. The commission of a serious offences impacts on the following rights of the public in ss 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 22, 23, 24, 25, 26, 27, 28 and 29 of the 1996 Constitution; Paragraphs 2, 5, 6, 7, 8, 11, 12, 13, 15 and 16 of the Schedule of RICA. Section 16(5)(a)(ii) and (iii) of RICA.

[2481] *National Commissioner of the South African Police Service, Zimbabwe Exiles' Forum & and another v Dugard and others* CCT 02/14 (*SAPS v SAHRLC & Ors*) para 77.

[2482] Aside from the identification of two classes of serious offences in RICA, which on the one hand, constitute actual and potential threats in the RSA and on the other hand, constitute general serious offences, there is no certainty in the specific classification of serious offences into other categories -such as the specific classes of 'state of emergency', 'most' and 'more' serious offences- to direct the conduct of an OCI in the RSA, section 16(5)(a)(ii)&(iii) of RICA. There are also no criteria for the specific classification of offences in NPA policy, NPA *Lawyers for the People- South African Prosecuting Service* (2011) at 32 - 33.

[2483] Art 2(a) of the UNODC 'Model Legislative Provisions Against Organised Crime' 2012 regards an offence involving organised criminal group as a serious offence. This definition is problematic because the criterion of seriousness is based on the organisation or otherwise of a group in the commission of an offence, whereas a serious could be committed by an individual while a group might also commit a less serious offence. Art 2(b) of General Assembly Resolution 55/25 of 15 November 2000 titled TOCC defines a serious offence as one that has a penalty of not less than 'four years imprisonment or a more serious penalty'. See art 2 (2) of Framework Decision 2002/584/JHA (European Arrest Warrant) Official Journal L 190, 18.07.2002 1-20, Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* at 41; UNODC 'Model Legislative Provisions Against Organised Crime' 2012 at 25.

[2484] For example, while homosexuality is an offence in Nigeria, it is not in South Africa. Although the United Nations guides on the elements of what constitutes international crime, which is one form of classification but it does not guide on the specific classification of international crimes into different categories such as most, more and general crimes, which is a concept developed in this study, see para 6.3.3 of this chapter and UN 'Report of the Preparatory Commission for the International Criminal Court: Part II Finalised Draft Text of the Elements of Crimes' PCNICC/2000/1/Add.2 at 1 - 48 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/724/27/PDF/N0072427.pdf?OpenElement (Date of use: 12 January 2017) wherein many offences are listed but not classified. Further, genocide, crime against humanity, war crimes and aggression are regarded as serious offences by ICC, Du Plessis M 'International Criminal Courts, the International Criminal Court, and South Africa's Implementation of the Rome Statute' in Dugard J *International Law: A South African Perspective* 4th ed. (2013) at 175 (Du Plessis 'International Criminal Courts'). Further, the practice is that the description of an offence does not have to have the same title in the RSA and other states in extradition matters, section 1 of Extradition Act No 67 of 1962, Dugard J et al 'Extradition'' 219-220.

At the foreign level, Canadian law does not provide for any criterion for the choice or inclusion of some serious offences in the statutes through which an OCI is conducted.[2485] These difficulties and fluidity open the floodgates for unreasonable, irrational, disproportionate and unjustifiable conduct of an OCI against individuals domestically[2486] and internationally.[2487] However, the following issues are examined.

Firstly, no case law specifically classifies offences according to their level of seriousness when conducting an investigation in the offline world, let alone create some criteria for classification according to the gravity of the serious offences as a guide in the conduct of an OCI in compliance with the application of the proportionality clause.[2488] This inadequacy creates a form of fluidity or uncertainty in the classification of serious offences in terms of the application of the provisions of RICA.

However, case law —such as the cases of *Investigating Directorate v Hyundai and Smit No* and *Thint*— only generally defines 'specified offences' according to the provisions of National Prosecuting Authority Act,[2489] which includes tax offences, corruption, fraud and money laundering but these cases are themselves not specifically classified according to their various levels of seriousness for purposes of conducting an investigation.[2490]

[2485] In Canada, an OCI can be used to investigate murder, hostage and drug trafficking offences which are regarded as 'relatively serious in nature' on the one hand as well as section 347 of the Code (criminal interest rate), section 372 of the Code (false messages), section 240(1) of the Excise Act (unlawful possession or sale of manufactured tobaccos or cigars) which are arguably less serious offences. However, an OCI cannot be used for less serious offences in Canada, see section 183 of the Canadian Criminal Code and Hubbard, Brauti and Fenton *Wiretapping* 1-6.1 to 1-6.2 and 4-2. In some countries, electronic investigation is conducted in any crime provided that the issuing judge is satisfied with the conditions thereto, see section 184.2(2)(a) and (3) of the *Criminal Code* of Canada, sections 15-16 of the *Listening Devices Act 1984 of the* New South Wales, Australia, see also para 3.6 of United Nations Office on Drugs and Crime 'Current practices in electronic surveillance in the investigation of serious and organized crime' https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf (Date of use: 2 May 2013).

[2486] See Chapter 5 of this study for the principle of disproportionality in online communication.

[2487] There are some difficulties in determining the diverse thresholds in various countries that seek for mutual OCI assistance in the RSA, sections 16(5)(a)(iv)(aa) & (bb) of RICA; A serious offence for which a person can be extradited according to the definition of extraditable offence in the Extradition Act 67 of 1962 is one that the penalty is six months and above.

[2488] See Chapter 5 of this study, more particularly paras 5.3.4 and 5.3.6.

[2489] *Investigating Directorate v Hyundai and Smit No* supra 86 and *Thint* supra 46, 48, 53 and 54. In *Thint* supra 252, a serious offence is defined as 'specified offence' according to the provisions of NPA Act. These offences include tax offences, corruption, fraud and money laundering.

[2490] *Investigating Directorate v Hyundai and Smit No* supra 86 and *Thint* supra 46, 48, 53 and 54.

Secondly, amongst the paragraphs in section 1 of the only Schedule to RICA, paragraph 14 does not stipulate or refer to any specific offence.[2491] However, according to paragraph (a) of the definition of a serious offence in section 1 of RICA, a serious offence is an offence that is listed under section 1 of the only Schedule to RICA (as amended) which identifies fifteen types of serious offences,[2492] all of which is specific, certain and definite in nature, features and application save paragraph 14 which has both positive and negative implications. The specificity of the fifteen types of serious offences does not specifically state the categories or levels of seriousness of these serious offences.

One of the positive aspects of paragraph 14 is that the non-stipulation of specific offences ensures that RICA covers other offences which are not specifically mentioned in RICA, but which may be investigated through the conduct of an OCI in terms of the penological requirement in paragraph 14.

Furthermore, paragraph 14 is the only, overall and more general, common and unequivocal criterion in defining or qualifying all serious offences[2493] in which an OCI can be used to conduct an investigation. The paragraph generally identifies the severity of *three* terms of imprisonment as one of the most effective forms of punishment for the commission of a crime by an individual[2494] as a criterion for consideration in the conduct of an OCI. Consequently, and arguably, any offence that is defined as a serious offence in RICA —which may require the use of an OCI in its investigation—[2495] must attract a punishment of one of the *three* terms

[2491] Paragraph 14 of the only Schedule to RICA makes an omnibus provision that allows the use of an OCI for any offence that is punishable by either: *a*) life term imprisonment; *b*) several terms of imprisonment in terms of section 51 of the Criminal Law Amendment Act. It is noted that the four grounds listed in section 51(3) cannot be regarded as substantial and compelling circumstances, see generally sectually 51(3) and (6) of the Criminal Law Amendment Act No 105 of 1997, *State v Dodo* supra 1, 3, 8, 9, 29 and 34; *State v Malgas* supra 1, 8, 9, 12, 13 and 25; *Veldman v DPP* supra 17; *N. v The State* (469/2007) [2008] ZASCA 30 paras 20 and 44);[2491] *c*) a term of imprisonment exceeding five years without an option of fine.

[2492] Section 1 of the only Schedule to RICA lists fifteen categories of offences in which paragraph 3 is now expunged. A non-serious offence includes 'relatively petty offences like pickpocketing or grabbing the mealie from the fruit-stall', see *Ex Parte Minister of Safety and Security and Others: In Re S v Walters and Another* (CCT28/01) [2002] ZACC 6; 2002 (4) SA 613; 2002 (7) BCLR 663 (21 May 2002) para 41 (*Ex Parte Minister of Safety and Security and Others: In Re S v Walters and Another*).

[2493] A serious offence includes offences in paras 1-2, 4-13 and 15-16 of section 1of the only Schedule to RICA. It should be noted that one should not conflate the broad definition of serious offence in para (b)(i), (ii)& (iii) of s 1 of RICA on the one hand and para 14 of section 1 of the only Schedule to RICA, on the other hand. This is because the latter definition is functional, substantive and to some extent, specific unlike the former which is vague, redundant and not specific.

[2494] See para 6.3.3.3 of this chapter on how and why terms of imprisonment seem to be one of the most recognised forms of punishment for crime commission.

[2495] Any offence includes offences in paras 1-2, 4-13 and 15-16 of section 1of the only Schedule to RICA.

of imprisonment in paragraph 14.[2496]

Amongst these three terms of imprisonment, the last term of imprisonment, which requires that the punishment must exceed five years without an option of fine,[2497] is arguably an outstanding term or criterion to determine what constitutes a serious offence concerning the conduct of an OCI. This criterion is the only and most general, uniform, *least* or *minimal*, common and unequivocal factor in the threshold requirement to refer to an offence as being a serious offence in RICA as opposed to minor or non-serious offences.

However, the negative aspects of paragraph 14 of s 1 of the only Schedule to RICA, which create some fluidity, uncertainty or contradiction, are arguably highlighted as follows:

a) An OCI cannot be used to investigate some of the offences created by RICA and Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 themselves. This is because the duration of punishment for committing such offences in RICA and Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 does not meet the requirement that stipulates that any offence with which an OCI can be used to investigate must be an offence that is punishable with no less than five-year imprisonment without an option of the fine due to the foregoing reasoning.[2498]

   It is ironic that where an offence is committed in the cyberspace,[2499] it is expected that there should be an imposition of a heavier sentence than in non-cyberspace to enable the conduct of an OCI in such offences according to the five-year minimum term of imprisonment requirement in RICA, which is the main law regulating the conduct of an OCI in the RSA.[2500] This is because the object of a protection in the cyberspace is digital data, which is enormous and exposed to greater risks than the data in the non-cyberspace;[2501]

[2496] Para 6.3.3.3 of this chapter for the three types of terms of imprisonment.
[2497] See section 1 of the only Schedule to RICA, particularly the third or last clause in para 14. However, in the definition of extraditable offence in the Extradition Act 67 of 1962, the implied minimum threshold for serious offence is six months imprisonment.
[2498] See sections 51(1)(b)(ii) of RICA and section 14(1) of the CCB B-2017, whereas the latter is replaced by section 14(1) of the Cybercrime Bill 2018 -Amendments Proposed to Bill B6-2017.
[2499] See the fourth criterion at para 3.5.7.11 of Chapter 3 of this study which submits that the penalty for the contravention of the requirements of a search warrant by LEAs is higher in online communications than in non-online communications.
[2500] In *Jwara v State* supra 13, the SCA held that the old interception law in the RSA – Interception and Monitoring Prohibition Act 127 of 1992 was an elaborate law.
[2501] Chapters 2 and 3 of this study. *N v The State* (469/2007) [2008] ZASCA 30 paras 23 (*N v The State*).

b) Aside from the Canadian law, which uses an OCI to investigate both minor and non-serious offences,[2502] international law on the minimum term of imprisonment as a criterion to classify offences for purposes of conducting an OCI is below five years[2503] as opposed to the requirement of a minimum of five-year imprisonment without an option of fine in RICA in the RSA.[2504]

Although some offences are universally acknowledged as serious offences,[2505] however, a serious offence attracts a minimum of one or four-year imprisonment at the international law level to enable the conduct of an OCI.[2506] Based on the diverse variation of jurisprudential definition, description or application of the meaning of the serious offence in the globe, it becomes difficult, if not impossible, for all countries to have a uniform threshold requirement to determine the seriousness of an offence on an individual domestic basis[2507] in this regard, particularly where there is a request for an international mutual OCI assistance.[2508] Even where States have ratified specific treaties, such as the Cybercrime Convention, there are differences in the criminal penalty imposed for the same offences by the States.[2509]

Thirdly, in paragraphs (b)(i)-(iii) of the definition of a serious offence in section 1 of RICA, a serious offence means an offence that "'is allegedly being', 'has allegedly been' or 'will *probably* be' committed" 'by a person, group of persons or syndicate':

[2502] An OCI is used for the investigation of serious offence. See s 183 of the Canadian Criminal Code and Hubbard, Brauti and Fenton *Wiretapping* 1-6.1 to 1-6.2.

[2503] Article 2(b) of the United Nations Convention against Transnational Organised Crime; Chapter III of the UNODC 'Model Legislative Provisions Against Organised Crime' 2012'; Art 2(b) of General Assembly Resolution 55/25 of 15 November 2000 titled TOCC.

[2504] Sections 51(1)(b)(ii) and paragraph 14 of RICA.

[2505] Such offences include hard drug dealing, organised crime or cybercrime, Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 24.

[2506] Article 2(b) of the United Nations Convention against Transnational Organised Crime; For the offences specified in Chapter III of the UNODC Model Legislative Provision 2012, 'no penalties are specified in the provision' but a minimum sentence of one year imprisonment is provided for extradition cases, see and art 3(h) of the UNODC 'Model Legislative Provisions Against Organised Crime 2012; Pieterse N B 'Electronic Crime Unit: Directorate for Priority Crime Investigation' Workshop for Policy Design towards Digital Security, Cybercrime and Cybercrime Prevention (2015) 23 http://www.nstf.org.za/wp-content/uploads/2015/10/BrigPieterse.pdf (Date of use: 27 August 2017) (Pieterse http://www.nstf.org.za/wp-content/uploads/2015/10/BrigPieterse.pdf (Date of use: 27 August 2017).

[2507] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 26.

[2508] Section 16(5) (a) (iv) (aa)&(bb) of RICA.

[2509] The penalty for the hacking of computer is maximum of one year in Czech, maximum of 4 years in Netherlands and between 2-7 years in Romania, Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 26.

i) 'acting in an organised fashion' in at least two incidents with 'same or similar intents, results, accomplices, victims or methods of commission';[2510]

ii) 'acting in the execution or furtherance of a common purpose or conspiracy', incitement or attempting to commit 'any of the offences mentioned herein';[2511]

iii) acting in a way that is likely to result in a 'substantial financial gain' for the actor or other persons.

It is submitted that the definition in paragraphs (b)(i)-(iii) is independent of the definition in paragraph (a) of the definition of a serious offence in section 1 of RICA.[2512]

Arguably, since paragraphs (b)(i)-(iii) of the definition of a serious offence in section 1 of RICA are independent of paragraph (a), the meaning of a serious offence in the former paragraphs —standing alone— does not constitute specific serious offences because they are broad, vague, fluid, redundant and ineffective. Paragraphs (b)(i)-(ii) do not specifically, functionally or substantively and unequivocally define or describe these acts as serious offences neither is there any higher criminal substance or element in any offence to categorise it as a special class of serious offences aside from the already classified general serious offences and offences which constitute actual and potential threats in the RSA.[2513]

Rather, paragraphs (b)(i)-(ii) provide broad and fluid guidelines only on the meaning of serious offences, which may erroneously be applied to minor or non-serious offences[2514] as further examined below.

[2510] See section 1 of RICA for the definition of serious offence.

[2511] *Kaunda v President* supra 129; See the next footnote on the reservation made with regards to this clause. Walden I *Computer Crimes and Digital Investigations* (2007) 71; Meehan E and Currie J H *The Law of Criminal Attempt* 2 ed. (2000) 2 and 15-34; Donnelly-Lasarov B A Philosophy of Criminal Attempts-The Substantive Approach (2015) 7- 86.

[2512] It is noted that the last clause of the definition of serious offence in para (b)(iii) of section 1 of RICA which states 'any of the above-mentioned offences' relates to para (b)(iii) of the definition only but not paragraph (a) of the definition of serious offence.

[2513] See section 16(5)(a)(ii) and (iii) of RICA.

[2514] In *NDPP v Geyser* (2008) ZASCA, the court held that Protection of Organised Crime Act 121 of 1998 (POCA) is applicable to offences that may not be classified as organised crimes; Kruger *Organised crime and proceeds of crime* 6-7.

Essentially, to illustrate the broadness, vagueness, redundancy, and ineffectiveness of paragraphs (b)(i)-(ii), the phrase 'organised fashion or crime'[2515] in paragraph (b)(i) of s 1 of RICA is not a specific, certain or definite offence but it is a method, approach, pattern or system of the commission of a crime.

According to Nugent JA in *NDPP v Vermaak*,[2516] organised crime is a term 'to describe offences that have organisational features of some kind that distinguish them from individual criminal wrongdoing',[2517] thus, the organisational feature impacts only on the number of people but does not arguably impact on the seriousness of an offence. This arguably implies that an individual may still commit a more serious offence that a group of people can commit, or the latter can also commit a less serious offence even where there is a presence of an organisational feature, thus the nature of the commission of the offence matters to determine its seriousness.[2518]

In paragraph (b)(ii), a minor or non-serious offence —such as shoplifting of items with very little value—[2519] can be committed in an organised fashion or as an organised crime, and with common purpose or conspiracy yet, may not be investigated via the conduct of an OCI because the nature and features of shoplifting constitute a minor or non-serious offence.

Commenting on paragraph (b)(iii) of the definition of a serious offence in section 1 of RICA, which is on the constitution of 'substantial financial gain' as a serious offence, the provision is also vague, fluid and ineffective because the value or measurement of substantial gain is very subjective and circumstantial. Paragraph (b)(iii) does not provide for the definition of

---

[2515] Organised crime has been erroneously identified and classified as a serious crime by many authorities including RICA, scholars and the state, which is contested in this study because of its vagueness and redundancy in terms of the definition, features and operations of the offence. The term organised crime is a criterion that determines the seriousness of an offence if considered in relation to a specific offence, as earlier recommended, see the definition of 'serious offence' in sections 1 and 15 (2)(e)(i), (5)(a)(iv) & (5)(c)(i) of RICA. Throughout the contents of the following, organised crime has been erroneously used: Pieterse at 23 http://www.nstf.org.za/wp-content/uploads/2015/10/BrigPieterse.pdf (Date of use: 27 August 2017); Kruger *Organised crime and proceeds of crime*; De Koker L *South African Money Laundering and Terror Financing Law* (1999) and State Security Agency 'About US' http://www.ssa.gov.za/AboutUs.aspx (Date of use: 30 September 2016); Harfield C The organisation of organised crime policing and its international context 2008 8(4) *Criminology and Criminal Justice* 483 - 507; Walsh A and C Hemmens C (eds) *Introduction to criminology : A Text /Reader* (2008) 492.

[2516] *NDPP v Vermaak* 2008 (1) SACR 157 (SCA) para 4; Kruger *Organised crime and proceeds of crime* 7.

[2517] *Mohunran & Another v NDPPP & Others* 2007 (6) BCLR 575 (CC) paras 74 and 140; Kruger *Organised crime and proceeds of crime Law* 7.

[2518] Paras 5.3.3–5.3.6 of Chapter 5 of this study.

[2519] *Ex Parte Minister of Safety and Security and Others: In Re S v Walters and Another* supra 41.

'substantial financial gain'[2520] neither is this clause connected to any form of crime to determine what constitutes 'substantial financial gain' or the level of substantial financial gain,[2521] where different categories of victims are involved who have incomparable and unparalleled financial and socio-economic needs and status in the society.[2522]

What constitutes substantial financial gain differs. For instance, in the case of *Famanda v State*,[2523] the reception of a bribe of R3, 500 by a convicted prosecutor to quash a case before him was not regarded as a serious offence as compared to a bribe that runs into millions of rand under the Prevention of Organised Crime Act. However, arguably, one act of fraudulently obtaining R1, 000 from a job seeker by an individual or group of people, will in this context be a serious offence to the victim. This is because of the worth of the money to an ordinary victim who is seeking for a cleaning job in a government department, for example.

From the general jurisprudential perspective, if there is no clear definition of what constitutes substantial financial gain, it is therefore argued that the principle that states that no authority can punish anyone for a non-existing or specific offence[2524] can also be applied to paragraphs (b)(i)-(iii) of RICA, in which the conduct of an OCI may not be the appropriate method of

[2520] Article 3(b) of UNODC 'Model Legislative Provisions Against Organised Crime 2012 only defines 'financial or other material benefits' as 'any type of financial or non-financial inducement, payment, bribe, reward advantage, privilege, or service (including sexual or other services)'.

[2521] In *Famanda v State* supra 12, the sum of R3500 can impliedly not be regarded as a substantial financial loss.

[2522] Drawing on the Constitutional Court decision that held that corporate entities are protected under a different privacy regime different from private individuals and identifies, this signifies the distinction between different categories of victims whose rights to online privacy require protection while conducting an OCI, *Bernstein v Bester NO* supra 69 and 83. Consequently, this study highlights different victims who bear the impact or effect of crime commission. A victim of crime commission is believed to experience or encounter adverse, diverse, incomparable, unique and profound physical, emotional and psychological experiences, perceptions and well-being subject to the type and degree of serious offences committed against the right-holder. The NPA uses multi-disciplinary and victim-centred approach in its prosecution policy, see NPA *Lawyers for the People-South African Prosecuting Service* (2011) at 52. Victims of the commission of serious offences can be direct, and indirect which impact on the form of electronic interception jurisdiction to be exercised or donated by the RSA. Direct victims in the fifteen categories of serious offences which are listed in the only Schedule to RICA are identified as government, general public, individuals, endangered species (in form of living beings -animals and agricultural species on land, sea and air) and corporate entities and victimless crime alongside the likely related serious offences that have effect on such victims, see Kruger *Organised crime and proceeds of crime* 9; Paragraphs 1, 2, 4 and 10 in the only Schedule to RICA. See the preamble, sections 1, 2 and 235, 237, and Chapter 11 of the 1996 Constitution of South Africa, amongst others; Section 16 (5)(a)(ii) and (iii) of RICA; Convention on International Trade in Endangered Species of Wild Fauna and Flora 2009; Shur E M *Crimes without victims: deviant behaviour and public policy* 169 (1965); Conklin J E *Criminology* 2nd ed. (1987) 84; Stitt B G 'Victimless crime: a definitional issue' *Journal of Crime and Justice* 11 (2): 87-102; Schmalleger F *Criminal Justice today: an introductory text for the 21st century* 3rd ed. 127.

[2523] *Famanda v State* supra 12.

[2524] *State v Naidoo* supra 505 J; Para 5.2.3.2 of Chapter 5 of this study.

investigation to be used because the clause does not provide for the element of a serious offence as examined herein.

In attempting to resolve the broad, vague, fluid, redundant and ineffective definition of a serious offence in paragraphs (b)(i)-(iii) of the definition of a serious offence in section 1 of RICA, the following is therefore recommended. In the first place, paragraphs (b)(i) and (ii) mentioned above should be reviewed and made applicable to specific serious offences in paragraph (a) of the definition of a serious offence in section 1 of RICA instead of relying on its present construction which makes paragraphs (a) and (b)[2525] alternative provisions instead of making the two paragraphs cumulative provisions. In the second instance, since the economic status of victims in the society differs, 'substantial financial gain' in para (b)(iii) should reasonably be definite, and determinable in degrees and concerning the five categories of victims[2526] of the commission of a serious offence.

Fourthly, further to the conceptualisation and examination of the 'descending serious offence' theory,[2527] it allows the conduct of an OCI of a serious offence but later turns out to be a less serious offence because of the sanction of a lesser sentence regarding the determination of penology of serious offence criterion in conducting an OCI.[2528] The imposition of a lesser offence in this regard contradicts one of the requirements for the conduct of an OCI in terms of the penological minimum five-year imprisonment without an option of fine,[2529] in which the fluidity in the restriction of the conduct of an OCI of serious offences is also impacted by the 'ascending serious offence' theory, which applies in two instances, amongst others.

The first instance of the 'ascending serious offence' theory applies where a non-serious offence is elevated to be a serious offence due to the frequency or magnitude of the commission of such less serious offence which compels the authorities —due to moral and social outcry of the society— to rate such a less serious offence to a serious offence[2530] under any of the six classes of serious offences identified in this study.[2531] The second instance of the 'ascending serious

[2525] Paras (a) and (b) of the definition of a serious offence in section 1 of RICA.
[2526] Du Plessis 'International Criminal Courts' 176- 177.
[2527] Para 5.3.3.1 of Chapter 5 of this study.
[2528] Para 6.3.3.3 of this chapter.
[2529] Para 6.3.3.3 of this chapter. See *State v Dodo* supra 29.
[2530] Paras 5.3.6.1 and 6.3.3.2 (e) of this study.
[2531] Para 6.3.3.1 of this chapter; *Investigating Directorate v Hyundai and Smit No* supra 545; Parliament of the Republic of South Africa 'Announcement, Tablings and Committee Reports' No 164 -2016 at 38 (JSCI Report 2016).

offence' theory occurs where an already classified serious offence is elevated to a higher hierarchy of serious offence by virtue of the repeated commission of such an offence by a convicted offender, which in turn elevates the requirements for the conduct of an OCI, particularly the proportionality principle.

In another vein, RICA allows LEAs to intercept an online communication for prosecution in civil proceedings in cases of asset forfeiture, and seizure, which arguably and in another breath involves some foundational element of criminality.[2532] However, it is argued that where such an interception does not have an element of criminality, the evidence obtained should be declared inadmissible and not consider the positive aspect of the interpretation of section 35(5) of the Constitution in favour of the State in this regard.

This is because permitting LEAs to embark on an interception of online communication in purely civil matters takes the right to the SOC of a non-governmental person or entity and defeats the sincere objective of the guideline for interception of online communication and the conduct of an OCI.

Importantly, because the determination of civil proceedings —including ordinary commercial transaction— is based on the preponderance of the evidence, it is overreaching, prejudicial and unjustifiable to allow the State to have an upper hand in a civil matter. The State already has abundant resources to investigate a non-online communication against a non-governmental person or entity who, in most cases, is at the mercy of the State in information gathering. Therefore, the State should be placed on the same footing with private persons or corporate entities who are at liberty to conduct a private investigation for purposes of conducting civil prosecutions.

In summary, the following findings are made on the above four-point perspective of the fluidity, uncertainty of or contradiction in the restriction of the scope of the conduct of an OCI to serious offences only.

Firstly, although, a serious offence may be defined, its application is broad, vague, fluid, redundant and ineffective when it is considered in the conduct of an OCI. This is because it is

[2532] Section 25(5)(a), 29(8) (b) (i) &(ii), 47(1) & (2) and 48 of RICA.

difficult to strictly limit the application of the conduct of an OCI to serious offences only due to the 'descending serious offence' and 'ascending serious offence' theories which basically and respectively state that a serious offence may eventually become a less serious offence and a less serious offence may also eventually become a serious offence in some circumstances. Impliedly, these theories defy the rule that the conduct of an OCI strictly or rigidly applies to serious offences only as defined in RICA and other law.

Secondly, it is difficult but reasonable to specifically classify serious offences in terms of the level of seriousness of an offence, which will serve as a guide in the conduct of an OCI in compliance with the application of the proportionality clause to justify the investigation through an OCI.[2533]

Finally, the gathering of evidence of online communication by the government for civil proceedings against a non-government person or entity is a mockery of the right to the SOC because it is not justifiable and reasonable for the government to do so if there is no element of criminality involved in the purpose for an online interception.

6.3.3 Criteria for specific classification of serious offences in the application of the proportionality principle in online criminal investigation application

6.3.3.1 Introduction

Where there are no thresholds that specifically classify serious offences in the application of proportionality principle, LEAs or LEOs wittingly or unwittingly resort to the unreasonable, irrational and unjustifiable invasion of the right to the SOC when making an application for the conduct of an OCI.

RICA identifies three categories of serious offences, which are: a) general serious offences; offences that are potentially threatening to the State or public safety and security; and c) offences that are actually threatening to the State or public safety and security. However, this

[2533] See Chapter 5 of this study, more particularly paras 5.3.4 and 5.3.6.

identification is fraught with some lacuna for lack of consideration of the application of the various forms of the proportionality principle as follows.[2534]

Firstly, although RICA recognises offences that are potentially and actually threatening to the State or public safety and security, however, it fails to recognise or provide a guide on the constitutionally provided state of emergency offences to proportionately determine how an OCI can be conducted in this regard.

Secondly, RICA fails to categorise the classes of general serious offences, thus creates a vacuum in the application of the proportionality principle in the conduct of an OCI.

Thirdly, RICA identifies a dichotomy between offences that affect the State or its existence and the general public on the one hand and private persons and entities on the other hand. However, RICA fails to identify the specific and coordinated classification of serious offences between the State and private persons and entities in the proportionate conduct of an OCI.

Therefore, six[2535] specific, hierarchical and coordinated classes and stages[2536] of serious offences between the State and general public, on the one hand, and the private persons and entities, on the other hand, are proposed and examined in this study for consideration in the application before the court for a proportionate, effective and practical conduct of an OCI[2537] at:

a) the *lowest* standard of *merely reasonable suspicious ground* to investigate first-class and stage serious offences that pose severe risks to the State or to investigate the state of emergency offences in the RSA;

[2534] Paras 3.4.4, 3.4.5, 3.5.7, 3.8, 5.3.4, 5.3.6, 5.4, 6.3.3.2 – 6.3.3.5, 6.4 - 6.6, 6.8 and 6.13 of this study.

[2535] Finkelstein M O and Levin B *Statistics for lawyers* (2nd ed.) 2001 at x and 36-42 (Finkelstein and Levin *Statistics for lawyers*). The proportion or range in these formulae is 9.9 % which is equal in all the formulae except the 6th formula (belief) which has a proportion or range of 49.9 %.

[2536] Stage is used in a different context in this study other than the general stages that may be connoted.

[2537] Paras 5.3.4, 5.3.6 and 5.4 of this study. For the examination and distinction between suspicion and belief standards of proof, upon which the six standards of proof are considered, see paras 6.4.2.1 - 6.4.2.3, 6.4.3, 6.4.4.1- 6.4.4.3, 6.4.5, 6.4.6.1, 6.4.6.2, 6.4.7.1, 6.4.7.2 and 6.4.8.

b) the '*lower* standard of *merely reasonable suspicious ground* to investigate second class and stage serious offences that actually pose high risks to the sovereignty of the RSA, and the public;[2538]

c) the *low* standard of *merely reasonable suspicious ground* to investigate third class and stage serious offences that potentially pose medium risks to the sovereignty of the RSA, and the public;

d) the *high* standard of *reasonable suspicious ground* to investigate most and fourth class and stage serious offences;

e) the '*higher* standard of *reasonable suspicious ground* to investigate more and fifth class and stage serious offences;

f) the *reasonable belief*' standard to investigate general and fifth class and stage of general serious offences.

While paragraphs (a)-(c) concern the State and general public and paragraphs (d)-(f) relate to private persons and entities, these two sets of classes and stages of serious offences are relatively and effectively inter-applicable, dependent and operational. While the risk levels involved in paragraphs (a)-(c) are arguably likened to the categorisation of risks in the State security realm in the RSA which are *severe*, *high* and *medium* risk assessments; the risk levels in paragraphs (d)-(f) are the general risk assessments that are generally found in the private persons or entities risk assessment realm.

The following four criteria[2539] amongst others are examined in the determination of the degree of serious offences, which in turn, assist LEAs, LEOs and other stakeholders to proportionately apply the provisions of RICA and other law in an OCI application at the appropriate classes and stages of crime commission. The criteria are:

[2538] It is noted that any serious offence can be escalated to be an actual or potential serious offence subject to whether the threat level of the commission or effect of the serious offence is high or medium respectively.
[2539] *Ex Parte Minister of Safety and Security and Others: In Re S v Walters and Another* para 42.

i) The bailability of serious offences;

ii) The penology of serious offences;

iii) The irreversibility or otherwise of the effect of the commission of serious offences and;

iv) The economic harm or loss in serious offences;

all of which may not necessarily and similarly classify serious offences in the same manner based on their nature and features as examined below.

While it is noted that paragraphs (i) and (ii) affect or relate to an offender and paragraphs (iii) and (iv) affect or relate to the victim, it is submitted that it is important for a court to, in an OCI application, consider at least a criterion each from the perspectives of both the victim and offender to ensure a balance between the two sides of the divide.

6.3.3.2 The bailability of serious offence criterion

a. Introduction

According to the provisions of the CPA, there is no offence that is not bailable,[2540] it is only the conditions of bail that are stringent in some offences.[2541] The purpose of whether to grant bail and the required conditions thereof are to ensure the appearance of an accused at a designated time and court or place, as may be directed by the authorities.[2542]

The bailability of an offence is not provided in RICA as a criterion for determining the seriousness of an offence neither is it a criterion for determining the threshold requirements for the conduct of an OCI. However, the condition of bail for an offence in the CPA, the examination of which validity is not covered in the scope of this study, is determined by the

[2540] Sections 58 and 60 (11)(a) of the CPA.
[2541] Section 60(11)(b) of CPA. In U.K., the political offence of 'compelling a government to change its policy' is equivalent to physical revolution against a state, *Schtraks v Government of Israel* [1964] AC 556 at 583 (HL), J Dugard et al 'Extradition'' 223.
[2542] Section 58 of the CPA.

seriousness of an offence,[2543] which ultimately determines the proportionality of the conduct of an OCI. [2544]

The proportionality is in terms of the level of intrusion into the right to the SOC and the stage of crime commission at which an OCI may be conducted,[2545] amongst other requirements provided in RICA or other law. The bail theory, according to the CPA Schedules, is broadly premised on three conditions as follows.

Firstly, it is submitted that where the bail condition requires the principle of 'exceptional circumstances' in section 60 (11)(a) of the CPA, which is the most stringent bail condition stipulated in the CPA, it is arguably an indication that the relevant offences in which such exceptional circumstances occur are likely to be the most serious offences for purposes of this study.[2546]

Secondly, where a bail condition requires the principle of 'interest of justice' in section 60(11)(b) of the CPA, it is arguably an indication that the relevant offences are likely to be the more serious offences for purposes of this study. The 'interest of justice' indicates that the condition is less stringent than the bail condition in most serious offences.[2547] The principle 'interest of justice' seems to be a more accommodating principle, which may consider other factors in the 'interest of justice' other than 'exceptional circumstances'.

Thirdly, where the commission of offences in which bail is granted does not require the proof of the above two principles, it is arguably an indication that the conditions for granting bail for such offences are less stringent than most and more serious offences. Such a bail condition can be referred to as the minimum or general bail condition, which is arguably likely to be applied to general and non-serious offences for purposes of this study. The inclusion of non-serious

[2543] Chapter 9 and Schedules 1-8 of the CPA.
[2544] Sections 58, 59(1)(a), 59A(1),60(4)(a), (5)(e)&(g),(11)(a)&(b) & (11A)(a)&(c) and 63A(1)(a)(ii) of the CPA where reference is made to some schedules (such as 1, part II or part III of Schedule 2, 5,6 and 7) in which bail may be granted with respect to some offences.
[2545] Paras 6.4.2.3 and 6.4.3 of this chapter.
[2546] It is noted that where an offender has committed an offence twice in Schedules 1 and subsequently 5, the offence is automatically escalated to Schedule 6 of CPA. Thus, this caveat should be considered in Schedule 5 offences in the CPA.
[2547] It is noted that where an offender has previously committed an offence in Schedule 1, the offence is automatically escalated to Schedule 5 of the CPA. Thus, this caveat should be considered in Schedules 1 and 5 offences in the CPA.

offences in the minimum bail condition requirement is because it may be *ultra vires* of the jurisdiction of the court to consider other bail conditions in other law other than the CPA, save where equity is applied to consider factors which are external to the provisions of the CPA.

Thus, in applying the 'ascending serious offence' theory, an offence may ultimately be a serious offence,[2548] therefore, minimum or general bail condition will be applied in a less serious offence.

According to the bailability criterion for purposes of this study, below is arguably a consideration of the specific classification of serious offences in paragraphs 1-16 of section 1 of the only Schedule to RICA[2549] into the following six categories of offences. This categorisation is in accordance with the bail condition classification provided in the CPA, in which this study does not examine the jurisprudential justifiability or otherwise of the bail conditions for such offences in the CPA.

b. 'Minimum' bail condition for a *sixth* class and stage of serious crime commission and general serious offence

Given that the least bail condition in the CPA is the broad application of the 'minimum or general bail condition' in the CPA Schedule,[2550] the conditions of which are considered in an OCI application to arguably and proportionately investigate the minimum class and stage of a serious offence, which is the general and sixth class and stage of serious offences.[2551]

The offences in the CPA Schedule in which the 'minimum bail condition' is considered for the conduct of an OCI application arguably include, for purposes of this study, offences such as terrorism; sedition;[2552] loss or serious risk of loss of life[2553] caused by culpable homicide;[2554] any sexual assault against a minor or someone who is mentally disabled or incapacitated;[2555]

[2548] Paras 5.3.3.1 and 6.3.2 of this study.
[2549] Note that para 3 of section 1 of the only schedule to RICA was amended by deletion.
[2550] See para 6.3.3.2(a) of this chapter.
[2551] Para 6.3.3.1 of this chapter.
[2552] See sections 59, 59A and 60 and Schedules 1, parts II and III of 2 and 8 of the CPA.
[2553] Schedules 1, 2 (Parts II and III), 5, 6, 7 and 8 of the CPA.
[2554] Schedules 1, 7 and 8 of the CPA.
[2555] Part 2 of Chapter 3 or the whole of Chapter 4 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act 2007 and Schedules 1 and 2(Part II) of the CPA.

assault when a dangerous or grievous bodily harm or wound is inflicted[2556] and torturing, all classified in the CPA Schedule as such.[2557]

Other general serious offences in the CPA Schedule in which the minimum or general bail condition is considered for the conduct of an OCI application arguably include fraud,[2558] corruption,[2559] theft[2560] and extortion[2561] in other circumstances other than Schedule 5 of the CPA, forgery and uttering,[2562] kidnapping,[2563] arson,[2564] malicious damage to property,[2565] breaking or entering any premises[2566] and public violence.[2567] Other general offences are offences relating to Intimidation Act[2568] and offences under Diamond Act and other related acts;[2569] criminal gang activities involving acts of violence which may be likened to some offences under the Intimidation Act;[2570] offences in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017 (committed locally or internationally) which are similar to offences cited in Schedules 1, 2 (Parts 1-III), 7 and 8 of the CPA.

c. 'Interest of justice' bail condition for a *fifth* class and stage of serious crime commission and more serious offence

Given that the broad application of the 'interest of justice' bail condition in the CPA Schedules is a condition that is more stringent than the 'minimum bail condition',[2571] the former condition

[2556] Schedules 1, 2(Part II), 7 and 8 of the CPA.
[2557] Section 4(1) and (2) of the Prevention and Combating of Torture of Persons Act No 13 of 2013 and Schedules 1, 2 (Parts II and III) of the CPA.
[2558] Schedules 1, 5 and 7 of the CPA.
[2559] See comments on corruption above under more serious offence.
[2560] Schedules 1, 2 (Parts I and II), 5, 7 and 8 of the CPA.
[2561] Schedules 5 and 7 of the CPA.
[2562] Schedules 1, 2 (Part II) and 7 of the CPA.
[2563] Schedules 1, 2 (Part III) and 8 of the CPA.
[2564] Schedules 1, 2(Parts II and III), 7 and 8 of the CPA.
[2565] Schedule 1 of the CPA.
[2566] Schedules 1, 2 (Parts 1, II and III), 7 and 8 of the CPAs. Note that part III of Schedule 2 refers to house breaking which is different from other forms of breaking.
[2567] Schedules 1, 2(Part III), 7 and 8 of the CPA.
[2568] Though intimidation offences under sections 1 and 1A of Intimidation Act 72 of 1982 are listed under Schedule 2 (Part III) of CPA, it is argued that the offence of intentional killing under section 1A(1)(a) and (b) should have been classified under Schedule 6 of the CPA because the definition of violence in section 1A(4) which describes the offence in section 1A(1)(a)and (b) is close to premeditated murder in Schedule 6 of the CPA. Section 1A(1)(a) and (b) of Intimidation Act attracts an imprisonment not exceeding 25 years.
[2569] Paragraph 10 of s 1 of the Schedule to RICA, Diamond Act 56 of 1986 and Schedule 2 (Parts II and III) of the CPA.
[2570] Chapter 4 of POCA 121 of 1998. Intimidation Act 72 of 1982 is classified under Schedule 2(Part III) of the CPA.
[2571] Para 6.3.3.2(b) of this chapter.

is arguably and proportionately applicable to conduct an OCI of a 'more and fifth class and stage of serious offence',[2572] which is higher than general serious offences classified in this study.[2573] The offences in the CPA Schedule in which the 'interest of justice' bail condition is considered for the conduct of an OCI application arguably include, for purposes of this study, offences such as high treason;[2574] terrorism;[2575] loss or serious risk of loss of life[2576] caused by murder;[2577] and attempted murder involving the infliction of grievous bodily harm.[2578] Other offences in this Schedule also include rape or compelled rape in other circumstances other than Schedule 6 condition;[2579] sexual assault, compelled sexual assault or compelled self-sexual assault, respectively on a child under the age of 16 years[2580] and terrorism under Schedule 5 of the CPA.[2581]

Other 'more serious offences' in the CPA Schedules in which the 'interest of justice' bail condition is considered for the conduct of an OCI application arguably include fraud,[2582] corruption,[2583] theft,[2584] extortion,[2585] offences relating to dealing in, smuggling or being in unlawful possession of ammunition, firearms, explosives or armament,[2586] income tax

[2572] See para 6.3.3.2(a) of this chapter.
[2573] Para 6.3.3.2(b) of this chapter.
[2574] Section 60(11)(b) of the CPA.
[2575] Sections 4(2) or 3, 13 and 14 of the Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004.
[2576] Schedules 1, 2 (Parts II and III), 5, 6, 7 and 8 of the CPA.
[2577] Schedules 1, 2 (Parts II and II) 5, 8 of the CPA.
[2578] Schedule 5 of the CPA.
[2579] Sections 3 and 4 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act 2007, see Schedules 1, 2 (Parts II), 5 and 8 of the CPA.
[2580] Sections 1, 5, 6, 7 and 8 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act 2007 and Schedules 1, 5 and 8 of the CPA.
[2581] See the submission with respect to the bailability of terrorism offences above.
[2582] Note that fraud in this class must involve an amount more than R500, 000.00, R100, 000. 00 or 'R10,000.00' respectively, see Schedules 5 of the CPA as opposed to fraud in Schedule 7 of the CPA involving an amount which does not exceed R20,000.00 or Schedule 1 of the CPA which does not require any amount of monetary value.
[2583] See the only Schedule to PRECCA 12 of 2004. It is further noted that though PRECCA does not mention an amount of money as stipulated in Schedule 5 of the CPA, an amount of money concerned in the corrupt activities in PRECCA may be an important criterion for the court to consider in order to determine whether it is a more or general serious offence, as provided under the offence of fraud in Schedules 5 and 7 of the CPA.
[2584] See the above footnote on the explanation on fraud, which applies herein in theft.
[2585] See the above footnotes on the explanation on fraud and theft, which apply herein in extortion.
[2586] Schedules 5 and 8 of the CPA. It is noted that these offences are not distinguishable in Schedules 5 and 8 on whether to classify some firearm offences under Schedule 5 or 8 of the CPA unlike the distinction in fraud which falls under both Schedules 5 and 7 of the CPA with distinguishing conditions in monetary terms. Further it is noted that section 14 of the Armament Corporation of South Africa Limited 51 of 2003 is the only offence created under this Act, it does not fall under para 9 of section 1 of the only Schedule to RICA because section 14 prohibits conflict of interest issues in the company and does not prohibit the dealing in, smuggling or being in unlawful possession of firearms, explosives or armament. It is noted that one of the key statutes regulating the dealing in, smuggling or being in unlawful possession of firearms is the Firearms Control Act 60 of 2000 which has a regulation title the Firearms Controls Regulations 2004.

offences,[2587] customs and excise offences,[2588] and section13(f) of the Drugs and Drug Trafficking Act.[2589] Other 'more serious offences' in the CPA Schedules include offences relating to the Proceeds of Crime Act;[2590] offences of racketeering and unlawful activities;[2591] any offence referred to in section 13(f) of the Drugs and Drug Trafficking Act;[2592] any offence contemplated in Parts I to 4 and sections 17, 20 or 21 (in so far as it relates to the aforementioned offences) of Chapter 2 of the PRECCA;[2593] and offences in Cybercrime and Cybersecurity Bill (committed locally or internationally) which are similar to those in Schedule 5 of the CPA.

d. 'Exceptional circumstances' bail condition for a *fourth* class and stage of serious crime commission and most serious offence

Given that the broad application of the 'exceptional circumstances' bail condition in the CPA Schedules is a condition that is more stringent than the 'interest of justice', or better still, it is the most stringent bail condition in the CPA Schedule, the latter condition is arguably and proportionately applicable to a 'most and fourth class of serious offence',[2594] which is higher than 'more serious offences' classified in this study.[2595]

The offences in the CPA Schedule in which the 'exceptional circumstances' bail condition is considered for the conduct of an OCI application arguably include, for purposes of this study,

[2587] In the Income Tax Act 58 of 1962 schedules, no reference is made to the CPA for bail conditions. However, tax offences may be classified under fraud, corruption and theft offences accordingly, amongst other related offences under the CPA.

[2588] In Customs and Excise Act 91 of 1964 schedules, no reference is made to the CPA for bail conditions. However, customs and excise offences are likely to be classified under fraud, corruption and theft offences accordingly, amongst other related offences under the CPA.

[2589] Schedule 5 of the CPA.

[2590] In the Proceeds of Crime Act 76 of 1996, no reference is made to the CPA for bail conditions. However, the offences under the Proceeds of Crime Act are likely to be classified with fraud, corruption and theft accordingly, amongst other related offences under the CPA.

[2591] It is however noted that as much as fraud and corruption are likely to be classified under Schedules 1, 2 (part II), 5 and 7 of the CPA, racketeering and unlawful activities may be classified under Schedule 5 only because these two offences seem more serious despite the fact that no specific mention of monetary value is made in the commission of the offences. However, in view of the heavy penalties involved in these serious offences which may not be applicable in general serious offences, racketeering and unlawful activities should not be classified under Schedules 1, 2 and 7 of the CPA which fall under general serious offences.

[2592] See ss 13(f) and 5(b) of Drugs and Drug Trafficking Act No. 140 of 1992.

[2593] Prevention and Combating of Corrupt Activities Act ('PRECCA') 12 of 2004. See also the provisions of the Proceeds of Crime Act 76 of 1996; See the Schedule of PRECCA 12 of 2004.

[2594] See para 6.3.3.2(a) of this chapter.

[2595] Para 6.3.3.2(c) of this chapter.

offences and instances such as a repeat offender of the offence of high treason[2596] and terrorism.[2597]

Other 'most serious offences' in the CPA Schedule in which the 'exceptional circumstances' bail condition is considered for the conduct of an OCI application arguably include loss or serious risk of loss of life[2598] caused by premeditated murder;[2599] rape or compelled rape;[2600] and the trafficking in persons for sexual purposes.[2601] Also included in the 'most serious offences' are robbery involving firearms, infliction of grievous bodily harm or taking of a motor vehicle[2602] and terrorism under Schedule 6 of the CPA; killing, murder, extermination and slavery;[2603] offline and offline computer-related offences committed in and outside the

[2596] Reading through Schedule 6 of the CPA, Schedule 5 is included in Schedule 6 as one of the offences that is ordinarily not bailable, but may grant bail in exceptional circumstances, see section 60(11)(a)(b) of the CPA.

[2597] Such offences include sections 2, 3(2)(a), 4, (1), 5, 6, 7, 8, 9, 10 and 14 of Protection of Constitutional Democracy against Terrorist and Related Activities 33 of 2004. It is noted that ss 2 and 3 broadly cover the offence of terrorism and related offence. The effect of the commission of the first category of terrorism on victims is broad, grievous and more serious in its contents, going through sections 2, 3(2)(a), 4, (1), 5, 6,7, 8, 9, 10 and 14 of the Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004. Essentially, this category classifies terrorism as one of the most serious offences as prescribed in Schedule 6 of the CPA. The effects of the commission of these offences on victims are more grievous than the second circumstance which is narrow and less serious in its contents. The second circumstance classifies terrorism as more serious offence in Schedule 5 of the CPA which relates to sections 4(2) or 3, 13 and 14 of the Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004. However, there is one similarity between these two circumstances which is section 14 of Act 33 of 2004. Under this section, both circumstances acknowledge the offence of threat, attempt, conspiracy and inducing another person to commit offence, thus the bailing authority should relate section 14 to other relevant offences which then determine whether bail should be granted under Schedule 5 or 6 of the CPA. Section 60(11)(a) of the CPA. Sections 2, 3(2)(a), 4, (1), 5, 6,7, 8, 9, 10 and 14 of the Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004.

[2598] Schedules 1, 2 (Parts II and III), 5, 6, 7 and 8 of the CPA.

[2599] Schedule 6 of the CPA.

[2600] Sections 3 and 4 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act 2007, see Schedules 1, 2 (Parts II), 5, 6, and 8 of the CPA.

[2601] Section 71(1) or (2) the Criminal Law (Sexual Offences and Related Matters) Amendment Act 2007 and Schedules 1 and 2 (Part II) of the CPA.

[2602] Schedule 6 of CPA. It is noted that robbery other than robbery with aggravating circumstances under Schedule 7 of CPA is not classified as an offence in para 4 of s 1 of the only Schedule to RICA because it may not result in the loss of life or serious risk of loss of a person's life as opposed to robbery under Schedule 6.

[2603] Schedule 1 of the Rome Statute.

Republic which result in crime against humanity of torture,[2604] genocide,[2605]war crime[2606] or apartheid.[2607]

e. **'Exceptional circumstances' bail condition for offences that are potentially and actually threatening to the State and public and state of emergency offences at *third, second* and *first* classes and stages of serious crime commission**

The broad application of the 'exceptional circumstances' bail condition in the CPA Schedules is the most stringent bail condition.[2608] Any offence which falls under the broad 'ascending serious offence' theory can arguably be escalated to an offence that is potentially (under the third class of offences) and actually (under the second class of offences) threatening to the State or public safety and security and an offence that constitutes a state of emergency offence (under the first class of offences).[2609]

It follows therefore that the bail condition to be considered by the court to proportionately conduct an OCI in the foregoing offences is arguably the 'exceptional circumstances' bail condition.[2610] It is submitted that to formulate a higher bail condition for offences in these regards than the 'exceptional circumstances' bail condition would be tantamount to making a herculean condition to grant bail which may not be met when bail is considered. In effect, a higher condition will deny a suspect the right to bail in the CPA offences that are potentially and actually threatening to the State and public and state of emergency offences.

[2604] *SAPS v SAHRLC & Ors* supra 37 and 39; *Al- Bashir* case para 1; Section 232 of the Constitution.
[2605] See the Convention on the Prevention and Punishment of the Crime of Genocide, 9 December 1948 at articles 1-2, 4 and 6 and the Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (*Bosnia-Herzegovina v Serbia and Montenegro*), 26 February 2007 (ICJ), *SAPS v SAHRLC & Ors* supra 36; *Al- Bashir* case para 1.
[2606] Geneva Convention I at article 49; Geneva Convention II at article 50; Geneva Convention III at article 129; and Geneva Convention IV at article 146, *SAPS v SAHRLC & Ors* supra 38.
[2607] Dugard *International law: SA* at 157-8 and 169; *SAPS v SAHRLC & Ors* supra 30 -37 and 40; *Filártiga v Peña-Irala* 630 F 2d 876 (2d Cir 1980) (*Filártiga*) at 880 and 890; *Kiobel v Royal Dutch Petroleum Co* 133 S Ct 1659 (2013) at 1664 and 1669.
[2608] Para 6.3.3.3(d) of this chapter.
[2609] Paras 5.3.3.1, 5.3.6.1 and 6.3.2 of this study for the examination of minor offences becoming serious offences by virtue of the number of victims of the commission of such a minor offence.
[2610] See para 6.3.3.2(a) of this chapter.

6.3.3.3 The penology of serious offence criterion

a. Introduction

The penology of an offence is a criterion to be considered by a court in an OCI application in determining the seriousness of an offence and ultimately the proportionality of the conduct of an OCI in terms of the level of intrusion into online communication and the stage of crime commission at which an OCI may be conducted, amongst other requirements provided in RICA.

Despite the shift from custodial punishment in some offences[2611] to rehabilitation and reintegration of offenders,[2612] the former is still prominent and retained in the statutes[2613] (including RICA), as a good and effective form of deterrence to crime commission amongst other forms of punishments.[2614] However, it is noted that the scope of this study does not cover the examination of the effectiveness of the penalty for crime commission in the RSA.[2615]

Section 1 of the only Schedule to RICA provides various penalties for the commission of a crime. These penalties are determined by a combination of many factors.[2616] However, amongst

[2611] One of the objects of POCA is to remove the incentive to commit crime and not necessarily punish them, thus, the statutes (such as POCA) and authorities (such as the Assets Forfeiture Unit) resort to stripping the offenders off the proceeds of crime, see *NDPP & Another v Mohamed & Others* 2002 (2) SACR 196 (CC) 203-204 paras 15 and 16; Department of Justice and Constitutional Development 'Asset Forfeiture Unit' 15; Criminal Assets Recovery Account established in pursuance of section 63 and Chapter 6 of POCA; Kruger *Organised crime and proceeds of crime* 6.

[2612] AnKathuria A and Porporino F J 'Implementing information technology for corrections in Africa: A case example of the Namibian Correctional Service Automated Offender Management Information System' Special Edition No 2/2015 *Acta Criminologica: Southern African Journal of Criminology* at 1.

[2613] See Chapter 28 of CPA.

[2614] Muthaphuli P 'Different Route, Same Destination? Assessing the (R)Evolution of Offender Reform in South Africa Twenty Years into Democracy' Special Edition No 1/2015 *Acta Criminologica: Southern African Journal of Criminology* at 132, 136 and 137; Kruger *Organised crime and proceeds of crime* 1. Section 276 of CPA provides for life imprisonment, periodical imprisonment, declaration as a habitual criminal, committal to any institution established by law, fine, correctional supervision, imprisonment with correctional supervision under the discretion of the commissioner or parole board and forfeiture.

[2615] See para 1.8 of this study. The penalty of crime in the RSA has been examined as a PhD work by a colleague, see generally Badejogbin O A *Sentencing reform in a postcolonial society- Call for the rationalisation of sentencing discretion in Nigeria, drawing on South Africa and England* (PhD thesis UCT 2015) (Badejogbin *Sentencing Reforms*).

[2616] The other factors, in form of classification of sentencing are explained below. *State v Makwanyane* supra 44, 158-161, 163-166, 173-174, 177, 197, 199, 273 and 297; *State v Dodo* supra 1, 3, 8, 9, 29 and 34; *State v Malgas* supra 4, 8, 9, 12, 13, 19, 22, 23, 25 and 34; Section 51 of the Criminal Law Amendment Act 1997; Bekker P M *Criminal procedure handbook* 9 ed. (2009) 288-290; See *Veldman v DPP* supra 4, 17, 23, 32 -33, 36, 38 and 45; *N v The State* para 2 and 11; The exercise of discretion also considers the following: a) sentence must be proportionate to the offence; b) sentencing must not infringe on other rights, *State v Tshilo* supra 1078;

the forms of punishment in RICA, paragraph 14 of section 1 of the only Schedule to RICA[2617] identifies three categories of general, uniform and common criterion of terms of imprisonment as a yardstick for determining the threshold required to conduct an OCI. These three categories of punishments may be assigned to six categories of serious offences, which indicate that the harsher the term of imprisonment, the more serious an offence is.

In attempting to determine the possible statutory term of imprisonment as punishment, which in turn determines the threshold in RICA procedure, the following is classified.

b. Punishment exceeding five years imprisonment without an option of fine for a *sixth* class and stage of serious crime commission and general serious offence

Further to the examination of the definition of a serious offence,[2618] the general minimum or threshold punishment for the commission of any, general and sixth class of serious offence in RICA, which invokes the conduct of an OCI is that the punishment for the commission of such an offence[2619] must *exceed five years without an option of fine*.[2620] For example, amongst others, the offences for which the penalty falls under general serious offences arguably include offences relating to criminal gang activities resulting in the imposition of a term of imprisonment for a period greater than 5 years and not exceeding 6 and 8 years in this statutory provision.[2621]

In these two instances, the fact that the punishments are 6 and 8 years are far more than 5 years which equitably and arguably suffice to waive the requirement of no option of fine as described above because the additional 1 year and 3 years added to the 5 years in paragraph 14 of section

2000 (11) BCLR 1252 (CC); *N v The State* supra 11; *State v Muller* supra 1, 2 and 79 -82 and 112; *N v The State* supra 3. Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007 (SORMAA), see more at: NRSO 'FAQ: National Register for Sex Offenders (NRSO)' http://www.justice.gov.za/vg/nrso.html#sthash.l1ApZaBz.dpuf (Date of use: 12 June 2016); Section 51 (3)(a) and (6) of the Criminal Law Amendment Act 105 of 1997. *N v The State* supra 1, 2, 8, 9, 15 and 43; *State v Arthur Brown* supra 44, 100, 108 and 112; Section 51(2)(a)-(c) of the Criminal Law Amendment Act.

[2617] See the latter part of para 6.3.3.3 of this study for the examination of the three terms of imprisonment from the perspective of the definition of serious offence in RICA.

[2618] See para 6.3.2 of this study.

[2619] Para 2.7.1 of Chapter 2 of this study.

[2620] A period of a minimum of one-year imprisonment is provided in art 2(1) of the Extradition Agreement between the Republic and China, GNR 34 GG 27168 of January 2005.

[2621] Sections 9, 10(1)(a) and (c) and 11 of POCA.

1 of the only Schedule to RICA should be considered in lieu of the fine to make a penalty fall under this rubric.

Given the abovementioned facts, it follows therefore that where the penalty for the commission of an offence exceeds 5 years imprisonment without an option of fine or as equitably interpreted or as submitted above for 6 and 8 years and that the minimum offence allowed to be investigated through an OCI in RICA is a general serious offence, a court will accordingly and proportionately conduct an OCI of general serious offences in online communication.

c. Punishment at the reasonable mean or mid-point between the minimum and maximum penalties in paragraph 14 of section 1 of the only Schedule to RICA for a *fifth* class and stage of serious crime commission and more serious offence

It is given that the penalties for the commission of general serious and most serious offences are respectively a minimum of 5 years imprisonment without an option of fine —with equitable and alternative interpretation in this study—[2622] and a maximum of life imprisonment.[2623]

Therefore, it is submitted that the penalty for the commission of a fifth class and stage and the more serious offence is arguably a reasonable or equitable point close to or which is around the region of the mathematical —or non-mathematical— mean point or mid-point between the minimum and maximum penalties in paragraph 14 of section 1 of the only Schedule to RICA[2624] or arguably in a penalty provision that has its specific penalty range in a statute. Paragraph 14 creates the three categories of punishment namely minimum, medium and maximum.

It is submitted that the mathematical —or non-mathematical— mean point between the minimum[2625] and maximum[2626] penalties specifically stipulated —for example— in section 51 of the Criminal Law Amendment Act[2627] is found in section 51(2)(a)(ii) of the same Act, which

[2622] Para 6.3.3.3(b) of this chapter.
[2623] *State v Williams* supra 53F–G and 54 E-I, the court in the Republic suggest that life imprisonment is one of the sentences that may be 'wholly inappropriate or unconscionable'.
[2624] If one were to adopt mathematical expressions, the midpoint punishment for more serious offence is where punishment is reasonably > five years without an option of fine but < life imprisonment.
[2625] Para 6.3.3.3 of this chapter.
[2626] Para 6.3.3.3 of this chapter.
[2627] Criminal Law Amendment Act105 of 1997.

is 20 years imprisonment for more serious offences. This is because the minimum penalty in section 51(2)(a) is 15 years imprisonment while the maximum penalty is 25 years imprisonment. Section 51(2)(a) does not stipulate the imposition of a fine in addition to the term of imprisonment.

However, without delving into the adequacy of the penalty of offences,[2628] this provision, which relies on the principle created in paragraph 14 of section 1 of the only Schedule to RICA, is arguably, discretionary, equitably and proportionately adequate to place an offence in section 51(2)(a)(ii) at the mid-point of the three terms of sentences in section 51(2)(a) of the Criminal Law Amendment Act RICA.

The exclusion of a fine in the 20-year sentence by the court in an OCI application arguably justifies the relevance and application of the proportionality principle in this regard. This is because, as earlier canvassed for the role of equity in custodial punishment that is above five years,[2629] arguably, the heavier a penalty imposition —like the 20-year imprisonment— the lesser the probability of a fine imposition as an option in the custodial punishment. This is due to the fact that for any penological jurisprudence to have gone to the extent of imposing a heavy sentence of 20 years might arguably not have morally, logically and justifiably considered a fine imposition in lieu of the sentence imposition in such violent offences, save where the crime involves financial, liquidated or monetary benefit, gain or reparation.

Therefore, a 20-year sentence without imposition of a fine in section 51(2)(a)(ii) in the specific instance herein may arguably be equitably adequate to be considered by the court to be at a mean or mid-point of sentencing between the minimum and maximum sentencing when the court considers an OCI application for a more serious offence.

Other offences or instances in which sentencing falls between the minimum and maximum sentencing when the court considers an OCI application for more serious offences arguably, specifically, equitably and proportionately include sections 2, 5, 6, 7, 8, 9 or 10 on terrorism or loss of lives and where offences relating to corruption in the Prevention and Combating of

[2628] Badejogbin *Sentencing reforms.*
[2629] Para 6.3.3.3(b) of this chapter.

Corrupt Activities Act, leading to the imposition of imprisonment not exceeding 18 years by a regional court both cases, if convicted.[2630]

d. Life imprisonment for a *fourth* class and stage of serious crime commission and most serious offence

The Constitutional Court in *State v Makwanyane*, held that it is cruel and inhuman to impose death sentence on an offender for the most serious offence of murder.[2631] Given the decision of the court[2632] and legislation[2633] abolishing death sentence in the penal jurisprudence of the RSA, life imprisonment (which is stipulated in paragraph 14 of section 1 of the only Schedule to RICA) is the highest —and in some cases, the most appropriate and suitable form of— punishment for the commission of some relevant most and fourth class and stage of serious offences.

Thus, the life imprisonment imposition cures the defect of the imposition of death sentence in the old law.[2634] Other specific offences under this class include offences relating to terrorism or loss of lives under Terrorism Act or other law,[2635] racketeering activities[2636] and offences relating to corruption in Prevention and Combating of Corrupt Activities Act.[2637]

It is important to note that despite the penalty for killing a human being carries a heavy penalty, the courts have *discretionarily* handed down varying and lesser sentences than life imprisonment due to compelling reasons even where the intent is proven by the prosecuting

[2630] Section 18(1)(ii) of Terrorism Act No 33 of 2004 and s 26(1)(a)(ii) of Prevention and Combating of Corrupt Activities Act ('PRECCA') 12 of 2004.
[2631] *State v Makwanyane* supra 26, 134, 144 and 353.
[2632] *State v Makwanyane* supra 26, 134, 144 and 353.
[2633] See section 1 of the Criminal Law Amendment Act 105 of 1997.
[2634] See section 277(1)(a) of the CPA, which is now expunged from the Act, see *State v Makwanyane* supra 2, 26, 134, 144 and 353.
[2635] Sections 2, 5, 6, 7, 8, 9, 10 and 18 (1)(i) of the Terrorism Act 33 of 2004. However, it is noted that an imposition of term of imprisonment not exceeding 5 years by any magistrate court will classify the offence of terrorism into less serious offence in section 18(1)(iii) of Terrorism Act 33 of 2004. It is argued that since section 18(1)(iii) does not comply with para 14 of section 1 of the only Schedule to RICA, the investigation of any terrorism offences resulting in the conviction in section 18(1)(iii) may be unlawful, unreasonable and unjustifiable. Further, the punishment of the offence of sedition under section 12 of the Regulation of Gathering Act 205 of 1993 is a less serious offence. See also section 10(1)(b) of POCA 121 of 1998. In Canada, an OCI cannot be used for less serious offences, Hubbard, Brauti and Fenton *Wiretapping* 4-12.
[2636] Sections 2 and 3(1) of Chapter 2 of POCA Act 121 of 1998.
[2637] Parts I to 4 and sections 17, 20 or 21 (in so far as it relates to the aforementioned offences) of Chapter 2 and section 26(1)(a)(i) of PRECCA 12 of 2004.

authority.[2638] The variation of sentencing is influenced by some factors which include the motive behind the commission of the offence of killing a human being which may result in either murder or culpable homicide and the age of the killer, amongst other factors.

The variation in sentencing for an offence of murder poses a concern in strictly recommending that all cases relating to the killing of human beings be regarded as the most serious offences in terms of RICA provisions. Perhaps the variation in imposing life imprisonment could be the reason that the High Court in the RSA adduced in extradition cases that the term of imprisonment is an issue in extraditing an individual to a Requesting State, wherein *State v Williams*, the court held that life imprisonment is seen as 'wholly inappropriate or unconscionable' for extradition cases.[2639]

e. Life imprisonment for offences that are potentially and actually threatening to the State or public safety and security and state of emergency offences for *third, second* and *first* classes and stages of serious crime commission

Given the application of the 'ascending serious offence' theory,[2640] an offence that is potentially (under the third class of offences which are) and actually (under the second class of offences which are) threatening to the State or public safety and security and an offence that constitutes a state of emergency offence (under the first class of offences) can be investigated[2641] where the court will arguably, equitably, rationally and proportionately consider a life imprisonment criterion as the more likely, and the appropriate penalty for the commission of these offences in an OCI application for these classes and stages of serious offences.

[2638] See *State v Pistorius* the sentence of which is still on appeal from the High Court to the Supreme Court of Appeal. This study excludes the examination of the adequacy of penology in this study.
[2639] *State v Williams* supra 53F-G and 54 E-I.
[2640] Paras 5.3.6.1, 6.3.2 and 6.3.3.2 of this study.
[2641] Paras 6.3.3.1, 6.4.5, 6.4.6.1 and 6.4.6.2 of this chapter.

6.3.3.4 Irreversibility of the effect of the commission of a serious offence criterion

a. Introduction

The irreversibility, irretrievability or irredeemability or otherwise of the effect of crime commission on victims is a criterion to be considered by a court in an OCI application to determine the seriousness of an offence and ultimately the proportionality of the conduct of an OCI in terms of the level of intrusion into online communication and the stage of crime commission at which an OCI may be conducted, amongst other requirements provided in RICA.

Since the methodology of this study does not include an empirical study to examine the psychological or emotional aspects[2642] of this study, the irreversibility of the psychological or emotional effect of crime commission is not extended to the psychological or emotional aspects of the irreversibility of the commission of a crime.[2643]

It is submitted that the broad principle of irreversibility is a state where, if an offence is committed, it becomes *impossible* to bring back or undo the *act* of commission or omission of the crime, and also becomes *impossible,*[2644] *difficult or costly* to bring back the *consequence, effect or impact* of the act of commission or omission of a crime to its initial *status quo* before the commission of an offence. It is further submitted that irreversibility can be described as a foundational dysfunctional state where the effect of the commission of crime collapses the system from running or running effectively.[2645] According to the irreversibility criterion,

---

[2642] Loubser M *et. al*. *The law of delict in South Africa* 2nd ed. (2012) 303-312 (Loubser *Delict*). Non-Patrimonial loss is 'That part of an individual's universal rights and duties which are not of any economic nature, or which does not have an economic value, is non-patrimonial'. For example, they include 'personality or pain and suffering, inconvenience, and loss of amenities of life associated with one's own bodily injury', Van der Walt J C & Midgley J R *Delict- Principles and cases: Volume 1: Principles* 2nd ed. (1997) 32(Van der Walt & Midgley *Delict- Vol 1: Principles*).

[2643] See the definition of who a victim is at para 2.3.1 of this study.

[2644] *State v Makwanyane* supra 26, 134, 144 and 353.

[2645] Roque P C 'Angola: Parallel governments, oil and neopatrimonial' *Institute for Security Studies- Situation Report* http://dspace.africaportal.org/jspui/bitstream/123456789/32306/1/6June2011Angola.pdf?1 (Date of use: 2 October 2016); Gupta V 'What do you mean by parallel government and cooperative federalism in India?' https://www.quora.com/What-do-you-mean-by-parallel-government-and-cooperative-federalism-in-India (Date of use: 2 October 2016); Olschimke M 'Dual Sovereignty and Parallel Government' http://www.olschimke.eu/2012/01/14/dual-sovereignty-and-parallel-government/ (Date of use: 2 October 2016); Straitstimes 'South Sudan president blasts UN for wanting 'parallel' government' available at http://www.straitstimes.com/world/south-sudan-president-blasts-un-for-wanting-parallel-government (Date of use: 2 October, 2016; France24 'Failed presidential candidate names parallel government in Gabon'

serious offences can be specifically classified into three, namely: reversible effect; partially irreversible effect; and absolutely irreversible effect.

b. Reversible effect of the commission of a *sixth* class and stage of serious crime commission and general serious offence

In the reversibility of offences criterion, the physical, and non-physical effects of the act of omission or commission of some serious offences are reversible. These offences arguably include economic, financial, fiscal or monetary offences,[2646] the effects of which are relatively reversible.[2647]

Given that the least set of offences covered by RICA is a general and sixth class of serious offence and that the minimum level of the criterion considered in this segment is the reversibility of the effect of a crime commission, it therefore follows that the court will proportionately consider the reversibility of the effect of the commission of a general serious offence when considering an OCI application.

c. Partially irreversible effect of the commission of a *fifth* class and stage of a serious crime commission and a more serious offence

In the partially irreversible serious offences, the physical, and non-physical effects of the act of omission or commission of some serious offences do not result in the absolute or permanent loss of substance, property, life, human body, endangered, scarce and protected game, plants, animals or part thereof.[2648]

Given that the next set of offences examined in this study is a more and fifth class of serious offence and that the next, logical and reasonable level of the criterion considered in this segment is the partially irreversible effect of the commission of a serious offence, consequently, the court will arguably, equitably, rationally and proportionately consider the partial

http://www.france24.com/en/20110126-andre-mba-obame-names-parallel-government-gabon-ivory-coast (Date of use:2 October 2016).

[2646] Reversible offences can be found in paras 8 (Chapters 2 and 3 of Prevention of Organised Crime Act No 121 of 1998), 9, 10, 11 and 12 of section 1 of the only Schedule to RICA. See section 38(2) of POPIA for the definition of relevant function where economic interest of the public is defined.

[2647] Sections 297, 297A, 300 and 301 of the CPA.

[2648] Partially irreversible offences are found in paras 1, 2, 4, 6, 7, 8 (Chapter 4 of POCA 121 of 1998), 15 and 16 of section 1 of the only Schedule to RICA.

irreversibility of the effect of the commission of a more serious offence when considering an OCI application.

d. Absolute or permanent irreversible effect of the commission of a most serious, potentially and actually threatening and state of emergency offences in the *fourth, third, second* and *first* classes and stages of serious crime commission

In absolute or permanent irreversibility of serious offences, physical and non-physical effects of the act of omission or commission of some serious offences result in the absolute or permanent loss of the substance, property, life, human body, endangered, scarce and protected game, plants, animals or part thereof.[2649]

Given that the next set of offences examined in this study is a most and fourth class of serious offence[2650] and that the final, logical and reasonable level of the criterion considered in this segment is the absolute or permanent irreversible effect of the commission of a serious offence; accordingly, the court will arguably, equitably, rationally and proportionately consider the absolute or permanent irreversibility of the effect of the commission of a most serious offence when considering an OCI application.

In addition, given the application of the 'ascending serious offence' theory,[2651] the next set of offences examined in this study are offences that are potentially (under the third class of offences which are) and actually (under the second class of offences which are) threatening to the State or public safety and security and an offence that constitutes a state of emergency offence (under the first class of offences). The logical and reasonable level of the criterion considered in this segment is also arguably the absolute or permanent irreversible effect of the commission of the offences mentioned herein because of the respective *medium*, *high* and *severe* risks that the commission of the offences pose. Consequently, the court will arguably, equitably, rationally and proportionately consider the absolute or permanent irreversibility of the effect of the commission of these offences when considering an OCI application.

[2649] Absolute irreversible offences are found in paras 1, 2, 4, 5, 6, 7, 8 and 13 of section 1 of the only Schedule to RICA; Section 1 of the National Prosecuting Authority Act 32 of 1998; Chapter 4 of the POCA 121 of 1998.
[2650] Para 6.4.7.1 of this chapter.
[2651] Paras 5.3.6.1 and 6.3.2 of this study.

6.3.3.5 Degree of economic gain or harm criterion in the commission of a serious offence

a. Introduction

Economic, financial or fiscal harm is a patrimonial[2652] loss that is unconnected 'to any physical injury or damage' and *the effect of which is 'much more widespread than physical effects*'.[2653] For example, economic harm includes harm resulting from fraud and dishonesty.[2654]

The degree of economic harm criterion in crime commission on a victim is a criterion to be considered by a court in an OCI application to determine the seriousness of an offence and ultimately the proportionality of the conduct of an OCI in terms of the level of intrusion into online communication and the stage of crime commission at which an OCI may be conducted, amongst other requirements provided in RICA.

b. Minimum financial or monetary gain or loss at the *sixth* class and stage of a serious crime commission and a general serious offence

The least set of offences covered by RICA is the sixth class and stage and general serious offence and the minimum level of the criterion considered in this segment is the minimal financial or monetary gain to an offender or harm or loss to a victim. It therefore follows that the court will arguably, equitably, rationally and proportionately consider the minimal financial

[2652] Sections 297, 297A, 300 and 301 of the CPA. Patrimonial loss is 'the pecuniary loss which flowed from the physical deterioration of a corporeal thing…both actual and prospective'. It not only includes 'loss suffered' but 'deprivation of a benefit'. Patrimonial loss includes the following: 'ownership earning capacity, debts incurred, contractual duties, expectation of an inheritance' or 'future contractual benefit', rights to 'maintenance, loss of profit', and anticipated expenses, Van der Walt and Midgley *Delict- Vol 1: Principles* 31-33. In the assessment of patrimonial loss, the loss is calculated prior to the commission and post the commission of the offence. The 'sum-formula' is used which calculates the actual or hypothetical value or position of the victim if the commission of an offence had not occurred and after it has occurred. When there is a liability, damages (or compensation), retraction, apology and interdict are specific remedies in delict, Loubser *et. al*. *Delict* 400 and 416.

[2653] Loubser *et. al*. *Delict* 228-233. Patrimonial offences include 'offences that do not constitute any kind of physical threat, let alone violence', see *Ex Parte Minister of Safety and Security and Others: In Re S v Walters and Another* supra 41.

[2654] See *Minister of Finance v Gore NO* 2007(1) SA 111 (SCA) para 87. See section 38(2) of POPIA for the definition of relevant function where economic interest of the public is defined. It is noted that since economic harm in serious offences is one of the criteria for determining the seriousness of an offence, which is different from the definition of serious offence, one should therefore not misinterpret the criticism of broadness, vagueness, redundancy and ineffectiveness of the definition of serious offence in para (b)(i)-(iii) of section 1 of RICA with this criterion herein.

or monetary gain to an offender or harm or loss to a victim when considering an OCI of general serious offences.

In the case of *Famanda v State*,[2655] an NPA prosecutor was convicted for taking a bribe of R3500 to quash a case before him, wherein the court held that a charge regarding millions of rand is a more serious offence than an amount of R3500 or few thousands of rands, though not undermining the amount in this case.

c. Reasonable financial or monetary gain or loss at the *fifth* class and stage of a serious crime commission and a more serious offence

The next set of offences covered by RICA is a fifth class and stage and more serious offence and the minimum level of the criterion considered in this segment is the 'reasonable financial, fiscal or monetary gain' to an offender[2656] or harm or loss to a victim. It therefore follows that the court will arguably, equitably, rationally and proportionately consider the 'reasonable financial, fiscal or monetary gain' to an offender[2657] or harm or loss to a victim when considering an OCI of more serious offences.

d. Substantial financial gain or loss at the *fourth* class and stage of a serious crime commission and a most serious offence

The next set of offences covered by RICA is a *fourth* class and stage and most serious offence and the next level of the criterion considered in this segment is the 'substantial financial, fiscal or monetary gain'[2658] to an offender or harm or loss to a victim. It therefore follows that the court will arguably, equitably, rationally and proportionately consider the 'substantial financial, fiscal or monetary gain' to an offender[2659] or harm or loss to a victim when considering an OCI of most serious offences.

[2655] *Famanda v State* supra 12.

[2656] To comply with the principle of exactness in relation to the reasonable and predictable limits in patrimonial loss, it is submitted that the minimum financial jurisdiction of the High Court may be used as the threshold for the definition of 'reasonable financial, fiscal or monetary gain' Loubser *et. al. Delict* 228.

[2657] Loubser *et. al. Delict* 228.

[2658] Though this phrase is defined as a serious offence in RICA, see the definition of serious offence in section 1 of RICA.

[2659] Loubser *et. al. Delict* 228.

e. Medium, high and severe national economic losses in potentially and actually threatening and state of emergency offences at the *third*, *second* and *first* classes and stages of a serious crime commission

Given the application of the 'ascending serious offence' theory,[2660] the next sets of offences examined in this study are offences that are potentially (under the third-class offences which are) and actually (under second class offences which are) threatening to the State or public safety and security and offences that constitute a state of emergency (under the first-class offences).[2661]

Furthermore, given that the logical and reasonable levels of the criteria considered in this segment are the *medium*, *high* and *severe* national economic losses and risks criteria, it follows therefore that the court will arguably, equitably, rationally and proportionately consider the respective medium, high and severe national risks in the conduct of an OCI of these respective three classes of offences.

6.4 POPOOLA MATHEMATICAL AND NON-MATHEMATICAL FORMULAE APPLIED IN THE STANDARDS OF PROOF IN ONLINE CRIMINAL INVESTIGATION APPLICATION

6.4.1 Introduction

Before the conduct of an OCI; LEAs, LEO and other stakeholders are required to prove legitimate and articulate aim of embarking on an OCI[2662] in pursuance of the protection of the right to the presumption of innocence of an individual.[2663] The aim to be proven by LEAs ranges from protecting national security to preventing disorder, crime and breach of peace in the society.[2664] Thereafter LEAs must establish the relevant reasonable ground standard clause

[2660] Paras 5.3.6.1 and 6.3.2 of this chapter.
[2661] Section 16(5)(a)(ii) of RICA.
[2662] In some cases, the objective may be to: a) identify the parties involved in the crime; b) to identify the chain or pattern of crime commission; c) to identify the 'process and means in which they commit it', Alberti A A *Wiretaps: A complete guide for the law and criminal justice professional* (1999) 6 and 7 (Alberti *Wiretaps*); False information must not be supplied to obtain evidence, art 23(a) of TOCC.
[2663] Schwikkard P J *Presumption of innocence* (1999) 29 and 35 (Schwikkard *Presumption of innocence*); Stumer A *The presumption of innocence –Evidential and human rights perspectives* (2010) at xxxvii.
[2664] Georgieva I 'Privacy under Fire- Foreign Surveillance under NSA and the GCHQ' (2015) 121.

concerning the conduct of an OCI, which is different from the standard of proof required at the criminal prosecutorial decision and trial stages in the criminal justice system.
The standard of proof that will enable the prosecuting authority to proceed with criminal prosecution is based on a 'reasonable prospect of a successful prosecution' clause,[2665] while the standard of 'proof beyond reasonable doubt' clause is required by the court in the conviction of an accused person in a criminal court trial.[2666]

In establishing the relevant reasonable ground standard to conduct an OCI, the rules of legislative drafting rely on and insert tables, samples, computations, definitions, regulations, and schedules to further express and clarify the intention of legislation on the substantive and adjectival proof of the relevant reasonable ground standard for a cause of action.[2667]

However, the standard of proof to conduct an online criminal investigation in the three classes and stages of crime commission set out in RICA in South Africa[2668] are not expressed in specific, easily determinable, functional and mathematical standards or formulae in any primary, subsidiary or common law to accurately express or clarify the intention of the legislature on the standards of proof in the conduct of an OCI.

This inadequacy is corroborated by the Constitutional Court of the RSA, which pronounced on the need for some serious offences to be conducted *earlier* than some other offences because the effects of the commission of some offences are more serious than the others in the offline world.

However, emphatically, the courts have unequivocally not made a distinctive pronouncement on the specific, certain and easily determinable standards required to conduct an *earlier* offline

[2665] NPA Prosecution policy 2013 at 5 and 6 and NPA *Lawyers for the people- South African prosecuting service* (2011) at 33- 34.
[2666] Hubbard, Brauti and Fenton *Wiretapping* 3-8.
[2667] Dick R C *Legal drafting in plain English* (3rd ed.) 133-137.
[2668] The three stages of crime commission are whether a serious offence 'has been', 'is being' or 'is likely to be' committed, section 16(5)(a)(i) of RICA; Paras 6.3.3.1 of this chapter.

investigation[2669] of such categories of serious offences,[2670] let alone made a pronouncement on the standards required to conduct an *earlier* OCI of such serious offences under RICA or any law in the RSA.

In addition, given the abundant available resources in the knowledge commons of the contemporary society that we live in and the arguable novelty of the emerging, controversial, and unsettled issues in cyberlaw jurisprudence, this study *inevitably* becomes *inchoate* if no adequate mathematical formulae are espoused in the standard of proof to conduct an OCI. The proposal to include some mathematical formulae in this study forms part of the ancillary tools to, with foresight; *painstakingly, indispensably*, *objectively*, *functionally* and *comprehensibly* interpret the provisions of RICA in conducting an OCI in a contemporary artificially intelligent and quick-silver technological society such as the RSA.

The use of mathematics to solve legal problems is loosely opposed in some quarters. The reason for the opposition is not due to any form of illegality of the use of mathematical formulae but that of unnecessary and unsubstantiated phobia for mathematics in some quarters[2671] who seemingly ignore that lawyers are logicians in argument and evidence and consequently, unconscious mathematicians.[2672]

However, the general need for the application of mathematical standards or formulae to address legal problems has some unequivocal legal backing at the higher court in two cases in the RSA. In the Supreme Court of Appeal in *State v Mavinini*, Cameron JA highlights the significant function of the application of mathematics in the decision-making process of the court,

[2669] Legal precedent is required in arriving at a new decision, Ernst M L and Schwartz a U *Privacy-The right to be let alone* (1968) 44. Para 6.4.2.2 of this study. *LSD v Vachell* 1918 WLD 127 (*LSD v Vachell*); *Secombe v Attorney-General* 1919 TPD 270 (*Secombe v Attorney-General*); *Cine Films (Pty) Ltd v Commissioner of Police* 1971 (4) SA 574 (W)(*Cine Films v Commissioner of Police*); *R v Van Heerden* 1958 (3) SA 150 (T) (*R v Van Heerden*); *S v Nell* 1967 (4) SA 489 (SWA)(*S v Nell*); *Ndabeni v Minister of Law & Order* 1984 (3) SA 500 (D)(*Ndabeni v Minister of Law & Order*); *Alex Cartage (Pty) Ltd v Minister of Transport* 1986 (2) SA 838 (E) (*Alex Cartage v Minister of Transport*); *Mnyungala v Minister of Safety & Security* 2004 (1) SACR 219 (TK)(*Mnyungala v Minister of Safety & Security*); *Ralekwa v Minister of Safety & Security* 2004 (2) SA 342; *Minister of Safety & Security v Sekhoto* 2011 (5) SA 367 (SCA) and *Rautenbach v Minister of Safety & Security* 2017 (2) SACR 610 (WCC)(*Rautenbach v Minister of Safety & Security*).

[2670] *Investigating Directorate v Hyundai and Smit No* supra 46, 48, 53 and 54 and *Thint* supra 127, 153, 168, 247, 252 and 257.

[2671] *Intercape v Pro-Haul* supra15; *Foodcorp v Deputy Director-General* supra 35 and 68.

[2672] Para 6.4.4.3 of this study.

however, no mathematical standards were proposed by the court.[2673] In corroboration in *Bane v D'Ambrosi*, the Supreme Court of Appeal emphasises the importance of applying the 'mathematically-based route' before embarking on 'the less desirable alternative' in the decision-making process of the court; nevertheless, no mathematical formulae were also pronounced by the court.[2674]

Without doubt, the mathematical proposal in this study *does not* in any way intend to offend, stiffen or tamper with the constitutional and inherent judicial independence and dynamism of the courts in the RSA[2675] and the constitutional academic freedom of scholars[2676] to express a contrarian view in the espousal of mathematical formulae in this study.

Importantly, any doctoral thesis in contemporary general cyberlaw jurisprudence that does not adopt some scientific and innovative methods —as shown in this rubric—[2677] in addressing artificial intelligence cyber robotics-based legal problems is *arguably* and *conclusively* attempting to *gag, stiffen* or *close up a voyage of robust academic and practical discovery* or *scholarship* in this regard.

In effect, attempting to *gag, stiffen or close up scholarship* by this author in his doctoral study will amount to a *myopic* and *malicious de-service* to the contribution to the body of knowledge in the development of general cyberlaw jurisprudence in the RSA. In a doctoral thesis, a candidate is expected to express independent, objective and logical views. These views are equally subject to unrestricted, logical, substantiated and robust criticisms by proponents of other schools of thought who are at liberty to hold a belief that the mathematical standards postulated in this study are illogical, irrational, null, void, and unnecessary.

Accordingly, firstly, this segment examines the general standard of proof required to investigate offences. Secondly, as a corollary to the former, this rubric interprets the standard of proof required for investigation at the three classes and stages of crime commission in RICA

[2673] Para 6.4.4.3 of this study. *State v Mavinini* 2009 (1) SACR 523 (SCA) 26; Schwikkard P J and Van der Merwe S E 'The standard and burden of proof and evidential duties in criminal trials' in *Principles of evidenc*e (2017) 614 (Schwikkard and Van der Merwe *The standard and burden of proof*).
[2674] Italics mine. Para 6.4.4.3 of this study. *Bane and Others v D'Ambrosi* (279/08) 2009 (ZASCA) 98 (*Bane v D'Ambrosi*).
[2675] Section 165(2) of the Constitution.
[2676] Section 16(1)(b) - (d) of the Constitution.
[2677] Para 6.4 of this study.

—or better still, the six classes and stages of crime commission conceptualised and examined in this study—[2678] in terms of the application of mathematical and non-mathematical formulae in the conduct of an OCI of serious offences in the RSA.

6.4.2 Setting the scene for the general standard of proof in online criminal investigation

6.4.2.1 Introduction

Whatever standard of proof that is required to investigate the six classes and stages of crime commission, there are two main sources of information on the commission of a crime[2679] in both offline and online worlds. Specifically, aside from the direct knowledge by LEAs or LEOs of crime commission, informants also trigger an investigation of the commission of a crime.[2680] Informer's tips come in many shapes, sizes, great value and reliability from many different types of persons.[2681]

Whatever the source of information for the investigation of crime commission might be, it is the credibility or reliability of an informant that is more important.[2682] In weighing the credibility of an informant's information, no one factor is determinative.[2683] The fact that a tip is specific and detailed is a credibility factor.[2684] It is acceptable that the precision and accuracy of precise details surrounding the matter together with a *history* of *proven reliability* can prove the relevant standard of proof to investigate.[2685] In conducting an investigation, a LEO should determine whether the information is 'based on *more than mere rumour* or *gossip*, whether the informer discloses his or her source or means of knowledge and whether there is any indication of his or her reliability', such as furnishing historical and 'reliable information' or

[2678] Paras 6.3.3.2 - 6.3.3.5 of this chapter.
[2679] The sources of information include that will require further investigation 'interviews; interrogations; admissions, confessions, and written statements; recording interviews and interrogations; informants; tracing and sources of information; observation and description, identification by witnesses, fingerprints and the mechanics of recording, latent fingerprints, casting, various impressions, broken glass, firearms, tracing materials, and detective dyes', Charles E. O'Hara; Gregory L. O'Hara *Fundamentals of criminal investigation* 7th ed. (2003) http://www.ncjrs.gov/App/publications/abstract.aspx?ID=200051 (Date of use:3 March 2016), see para 2.9 of this study.
[2680] Hubbard, Brauti and Fenton *Wiretapping* 3-9 to 3-10.1.
[2681] Hubbard, Brauti and Fenton *Wiretapping* 3-10.2.
[2682] Hubbard, Brauti and Fenton *Wiretapping* 3-8.
[2683] Hubbard, Brauti and Fenton *Wiretapping* 3-8 and 3-9 to 3-10.
[2684] Hubbard, Brauti and Fenton *Wiretapping* 3-8.
[2685] Hubbard, Brauti and Fenton *Wiretapping* 3-10.1.

corroboration of part of his or her story by a LEO.[2686] The fact that the information can be corroborated in an undercover investigation is helpful.[2687]

6.4.2.2 Distinction in the standards of proof between suspicion and belief

a. Overview of the concepts of suspicion and belief

According to the Constitutional Court in *Investigating Directorate v Hyundai and Smit No* and *Thint*, different standards of factual matrixes apply to sensitive, complex, complicated and serious, organised and economic crimes which must be investigated earlier than the other offences.[2688] The ratio in the decision of the Constitutional Court has two main effects, both of which must be symmetric, otherwise, the effects create a legal incongruity which leaves the court and LEAs or LEOs in the battlefield of determining the interpretation or enforcement of the effects of the ratio of the Constitutional Court.

Firstly, there must be a classification of offences in statutes, highlighting all the serious offences that must be investigated earlier than the others. However, the CPA and other laws do not classify offences according to the criterion of early investigation; instead, offences are classified according to other criteria such as the conditions required for securing bail. However, this study conceptualises six categories of offences under four criteria which are relevant in determining whether an offence is investigated earlier than the offences.[2689]

Secondly, the effect of the ratio of the Constitutional Court clearly shows that the standard that will be used to conduct an earlier investigation of serious offences sharply differs with the standard that will be used for general offences that will be investigated later. Undoubtedly, the age-long and well-known standards which are 'suspicion' and 'belief' are the two and only standards of proof applied in a criminal investigation. It is submitted that the former standard —which is suspicion— is considered to conduct earlier investigation of serious offences while the latter standard —which is belief— is used for the investigation of general offences.

[2686] Hubbard, Brauti and Fenton *Wiretapping* 3-10.1.
[2687] Hubbard, Brauti and Fenton *Wiretapping* 3-10.1.
[2688] The serious offences mentioned in these cases include tax matters, fraud, theft, forgery, uttering, corruption or an economic offence involving patrimonial loss, see *Investigating Directorate v Hyundai and Smit No* supra 46, 48, 53 and 54 and *Thint* supra 127, 153, 168, 247, 252 and 257.
[2689] Paras 6.3.3.2 - 6.3.3.5 of this study.

Essentially, where a serious offence is investigated earlier than general offences, it practically implies that the LEAs or LEOs will be required to investigate such a serious offence before the completion of the commission of such a serious offence or at such time that a LEA or LEO is aware of the commission of the serious offence.[2690] It is noted that despite that such a serious offence is detected at a later stage does not subtract from the fact that the same standard of proof is required for the investigation of such a serious offence.

However, the concepts 'suspicion' and 'belief' are erroneously legislated, defined, described, and applied as concepts that mean the same thing by the legislature and courts respectively. Also, the Constitutional Court did not set out an accurate, specific and easily determinable standard for the investigation of offences that are investigated earlier than the other offences. Since these two standards of proof are different, arguably, *a LEO or court cannot 'suspect' and at the same time 'believe' in the standard of proof to investigate an offence in the same scenario and vice versa*,[2691] otherwise, the ratio in *Investigating Directorate v Hyundai and Smit No* and *Thint* will be invalid, null, void and of no effect.

Consequently, in putting the ratio of the court into effect in *Investigating Directorate v Hyundai and Smit No* and *Thint* on the two concepts, this study conceptualises and examines six standards of proof[2692] which are arguably *accurate*, *specific* and *easily determinable* to conduct an OCI of six classes of offences identified in this study.[2693]

According to the provisions of RICA which rigidly and contradictorily use the concept 'belief', though clarifies its meaning in the three stages of crime commission herein;[2694] LEAs become aware or have knowledge[2695] of the commission of a complete or incomplete[2696] offence at any of the following three stages of crime commission or standards of proof that a serious offence: i) 'will probably be committed', which is '*merely speculative* or *suspicious*' in nature in the

[2690] Paras 6.4.2.3 and 6.4.3 of this study.
[2691] For example, an accused person cannot be charged for attempted murder and murder of the same person, at the same time, venue and circumstances. One of either an attempt or a completed act must give way for the other.
[2692] Paras 6.4.5–6.4.8 of this study.
[2693] Paras 6.3.3.2 (c)-(e), 6.3.3.3 (c)-(e), 6.3.3.4 (c) and (d) and 6.3.3.5 (c)-(e) of this study.
[2694] Section 16(5)(a)(i) of RICA.
[2695] See para 2.2 of this study.
[2696] Incomplete crimes include attempt, conspiracy and incitement; see the definition of serious offence in s 1 of RICA.

conduct of an OCI; ii) 'is being committed', which is '*reasonably speculative* or *suspicious*' in nature in the conduct of an OCI;[2697] and iii) 'has been committed',[2698] which is a reasonable belief and is '*justifiable*' in nature in the conduct of an OCI.[2699]

These three standards are also required to be proved in the U.S. as the precedent for the occurrence of an OCI.[2700]

It is noted that these three stages of crime commission are incongruously drafted in RICA because they create uncertainty in the application of section 16(5)(a) of RICA, given that the provisions of section 16(5)(a)(i)-(v) are not cumulative in nature to give meaning and effect to the provisions. This is because none of the provisions of section 16(5) (a) (ii)-(v) are an alternative to section 16(5)(a)(i). Essentially, section 16(5) (a) (ii)-(v) cannot be applied without conditionally considering the three stages of 'reasonable ground' standards in section 16(5)(a)(i).[2701]

The factual matrixes at the three stages of crime commission identified in RICA are interpreted and classified in two broad standards of proof —which are suspicion and belief— upon which

[2697] Section 16(5)(a)(i) of RICA. These two standards may not constitute belief. Belief is the standard at the third stage of crime commission (which requires that a serious offence 'has been committed') in OCI standard. The use of OCI is not automatic because LEOs are still required to proof the procedural aspects of OCI, some of which may be Herculean, hence the opinion by Swart that the OCI must be 'absolutely necessary', Swart H 'Communication surveillance by the South African intelligence services' 2016 at 20 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use:13 August 2016) (Swart http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use:13 August 2016). A reasonable suspicion means something more than a mere suspicion and something less than a belief based upon reasonable and probable grounds', Hubbard, Brauti and Fenton *Wiretapping* 3-17 to 3-18.

[2698] Section 16(5)(a)(i) of RICA for the various sections in RICA where the three stages are provided. In *B C C Pharmaceuticals (Pty) Ltd v Minister of Health & Others* 2007 (3) SA 72 (C), RGS that an offence has been or is being committed according to section 28(1)(a)(ii) of Medicines and Related Substances Act 101 of 1965 means 'reasonable surmise without proof that an offence was committed'. In *Investigating Directorate v Hyundai and Smit No* supra 6, 31, 33 and 56, the Constitutional Court recognises two forms of reasonable ground to believe in both complete and attempted offences which are that a serious offence: 'is being committed' and 'has been committed'. Section 16(5)(a)(i) of RICA. In Canada, not all applications require RGB. The proof of RGS is required for tracking devices or 'digital number record' which requires minimal expectation of privacy, while RGB is required for the invasion of video or audio investigation, Hubbard, Brauti and Fenton *Wiretapping* 3-6.2 to 3-6.3 and 3-16; In Canada, three stages are applied namely: a) 'is about to be committed'; b) 'is being committed' and c) 'has been committed', *R v Debot* (1989) 52 C.C.C. (3d) 193, [1989] 2 S.C.R. 1140 at 1166, *R v Jir* (2010) 264, C.C.C (3d) 64, 80 C.R (6th) 53, Hubbard, Brauti and Fenton *Wiretapping* 3-13, 4-2c and 4-2.3.

[2699] In the definition section of 'serious offence', it is expressed as any offence that '*will probably be committed, is allegedly being* or *has allegedly been committed*.', see section 1 of RICA and Bawa *ROICA* 320.

[2700] Caproni *Lawful electronic surveillance* 209.

[2701] Para 6.3.2 of this chapter.

offline criminal investigation is initiated to comply with the investigative description set up by the Constitutional Court.[2702]

A distinction is made between these two standards. The South African and U.S. courts have posited that it is vague and difficult to define the concepts of 'suspicion' and 'belief' because they are abstract principles which do not constitute 'hard certainties',[2703] both of which are based on probabilities.[2704] However, the distinguishing factor in 'suspicion' and 'believe' is that 'suspicion' is a less demanding standard of proof than 'belief'.[2705] In other words, in *R v Van Heerden*, the court held that 'suspicion is apprehension without clear proof'.[2706]

However, in the RSA, the court in *AmaBhugane* was not prepared to dive into the ocean of debate on the distinction between 'reasonable ground to believe' standard and a high degree of probability' standard, wherein the latter is otherwise regarded as 'suspicion'.[2707] 'Suspicion' requires a mere degree of probability of level of involvement of an individual in criminal activity,[2708] which 'can arise from less reliable information' than 'reasonable ground to believe'.[2709]

On the one hand, the concept of suspicion, which arguably stems from the preventive point of view,[2710] 'requires a degree of satisfaction, not necessarily amounting to belief, but at least extending beyond speculation as to whether an event has occurred or not'.[2711] The preventive

[2702] *Investigating Directorate v Hyundai and Smit No* supra 1, 2, 6, 8, 27, 28, 30, 31, 34, 44, 45, 46, 47, 48, 51 - 54; See *SAPS v SAHRLC & Ors* case for offline RGB standard.
[2703] *R v Van Heerden* supra 128; *Ornelas v U.S* 517 1996 U.S. 695-696; *Illinois v Gates* 462 U.S. 213, 232 (1983); Hubbard, Brauti and Fenton *Wiretapping* 3.10.1 to 3.10.2 and 3-20; *U.S. v Cortez* Id 417.
[2704] *R v Van Heerden* supra 128; Hubbard, Brauti and Fenton *Wiretapping* 3-10.1 to 3-10.2.
[2705] Hubbard, Brauti and Fenton *Wiretapping* 3-6-2 to 3-6-3.
[2706] *R v Van Heerden* supra 128.'
[2707] *AmaBhungane v Minister of Justice* supra 141.
[2708] Hubbard, Brauti and Fenton *Wiretapping* 3-18.
[2709] Hubbard, Brauti and Fenton *Wiretapping* 3-18.
[2710] Arts 29(1)(a), 30(4), 31, 31 (5), (6) of TOCC.
[2711] Anon 'Drug Trafficking and organised Crimes (Amendment) Bill 2000- Note on "Reasonable Grounds to Suspect", "Reasonable Grounds Believe" and "Reasons for Introducing Two Money Laundering Offences Using Different Mental Elements"' Paper No CB (2) 820/00-01(01) at 2; *Commissioner of Corporate Affairs v. Guardian Investments Pty Ltd* [1984] VR 1019 at 1023-1025). In the Canadian jurisprudence on suspicion, RGS cannot be reduced to a 'checklist of factors' but a totality of circumstances, which if each factor is taken separately is capable of being given an innocent explanation. Essentially, in RGS, one may 'not rule out the possibility of innocent conduct'; *U.S v Cortez* 449 U.S. 411(1981) at 417 - 418; *United States v Arvizu* 534 U.S. 266 (2002); *U.S v Sokolow* 490 U.S 1 (1989) 7; *Illinois v Wardlow* 528 U.S 119, 125 (2000). LEAs must operate within minimum criteria in order to avoid any arbitrary assessment. The criteria must be in relation to a 'reasonable suspicion of crime' and not to a credibly based probability of crime. There must be an 'articulable cause' or legal justification for the invasion of privacy, Hubbard, Brauti and Fenton *Wiretapping* 3-16 to 3-18 and 3-19 to 3-20.

point of view explains the rationale behind the use of the phrase 'reasonable ground to suspect' in both preparatory investigations and 'enquiry' in *Investigating Directorate v Hyundai and Smit No*[2712] in which an OCI may be conducted at the earlier stage of the commission of a crime subject to the degree of seriousness of an offence to prevent the occurrence of the offence.[2713]

The court in the U.S. warns that as much as LEAs are not compelled to have complete information about a crime —which relatively defeats the purpose of an OCI if all the facts are gathered which would make the conduct of an OCI unnecessary, 'fishing expedition' should not be embarked upon by LEAs where there is no known general presence of criminal activity about a criminal organisation.[2714]

Arguably, the suspicious standard of proof to determine the commission of a crime necessitating the conduct of an OCI is at the early stage of crime commission or where there is insufficient fact or uncertainty about the formation of reasonable belief of the commission of an offence. Reasonable —as it is generally referred to— the suspicious standard has a very low standard of proof and constitutes a 'high degree of probability' and reasonable 'speculative grounds'[2715] which are used to conduct an early investigation of more serious offences.[2716]

The supply of a *simple conclusive fact by an informer* to a LEO would not amount to the reasonable ground for infringing the right of an individual.[2717] The evidence that is gathered must not be perceived and measured in terms of library examination by scholars, but with the

---

[2712] *Investigating Directorate v Hyundai and Smit No* supra 1, 2, 6, 8, 27, 28, 30, 31, 34, 44, 45, 46, 47, 51 and 52; See para 7.6.3.3 of this study.

[2713] *Investigating Directorate v Hyundai and Smit No* supra 46; Paras 6.3.3.2(c)–(e), 6.3.3.3(c)-(e), 6.3.3.4(c) & (d) and 6.3.3.5(c)-(e) of this study.

[2714] Hubbard, Brauti and Fenton *Wiretapping* 3-12 and 3-15.

[2715] *Investigating Directorate v Hyundai and Smit No* supra 31, 33 and 45. Mare A and Duncan J 'An Analysis of the communications surveillance legislative framework in South Africa: Media policy and democracy project' (2015) 22 and 31 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf (Date of use:1 December 2017) (Mare and Duncan http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf (Date of use:1 December 2017)**.** In Canada, the first stage of crime commission necessitating interception stipulates that *'an offence is about to be committed*'. Three stages of crime commission are identified by the court in Canada, namely, that an 'offence *has been, is being* or is *about to be* committed', *R v Madrid* [1994] B.C.J. No 1786 (C.A.) para 82 and *CanadianOxy Chemicals Ltd v Canada (Attorney-General*) (1999) 1 S.C.R 743,133, C.C.C. (3d) 426 para 14 (*CanadianOxy v Canada*); Hubbard, Brauti and Fenton *Wiretapping* 4-2c and 4-2.3. In the U.S., the first stage of crime commission is described as being proactive in nature, the commission of which is seen as 'on-going and not yet factually identified as one distinct incident', Alberti *Wiretaps* 2.

[2716] *Investigating Directorate v Hyundai and Smit No* supra 46; Paras 6.3.3.2(c) –(e), 6.3.3.3(c)-(e), 6.3.3.4(c) & (d), 6.3.3.5(c)-(e) and 6.4.5- 6.4.7 of this study.

[2717]Hubbard, Brauti and Fenton *Wiretapping* 3-10.1.

understanding of experts in the field of law enforcement.[2718] In *R v Van Heerden*, the court held '…that suspicion…must be interpreted objectively, and thegrounds of suspicion must be thos e which would induce a reasonable man to have the suspicion.'[2719]

On the other hand, 'reasonable ground to believe' must be reasonable, rational and objective and should not be based on 'arbitrary' and 'unsubstantiated speculative' ground.[2720] Belief standard requires some reasonable conviction, which has been summarised by the court as the standard that is not only less than a criminal conviction but is also less than the civil standard of proof which is based on the preponderance of evidence.[2721] Arguably, a unique standard of preponderance of evidence[2722] is required in the conduct of an OCI, in which the six standards of proof conceptualised in this study are accommodated.[2723]

Belief standard is the state where facts are not based on rumour,[2724] the equivalence of which in Canada, is referred to as 'fair or reasonable probability or belief'[2725] to investigate general serious offences.[2726] Belief is the point where credible-based probability, 'non-technical and common sense assessment or probability of the totality of the circumstances' or where facts replace suspicion.[2727]

[2718] Hubbard, Brauti and Fenton *Wiretapping* 3-10.2.

[2719] *R v Van Heerden* supra128.

[2720] *Investigating Directorate v Hyundai and Smit No* supra 36; *NDPP v Stander & Others* 2008 (1) SACR 116 (E) paras 13, 21 and 23; Kruger *Organised crime and proceeds of crime* 10, 101, 108 and 159; See ss 4(2)(b), 5(2)(b) and (c), 6(2)(d), 7(1)(a) and (b), 8(1)(b) and (2), 16(2)(e) and (5)(a)-(c), 22(4)(a) and (b) and 23 of RICA; Bawa *ROICA* 320. These terminologies are referred to as 'reasonable and probable grounds' in U.S. while the Canadian jurisprudence uses the phrase '*reasonable grounds to search*', which have the same meaning and standard. Hubbard, Brauti and Fenton *Wiretapping* 3-7.

[2721] Hubbard, Brauti and Fenton *Wiretapping* 3-8.

[2722] 'It is also accepted that it is for the police to prove on the balance of probabilities that the arresting officer suspected that the person arrested was guilty of the offence, and that there were reasonable grounds for that suspicion', see *Minister of Safety & Security v Sekhoto* supra 53.

[2723] Paras 6.3.3.2 – 6.3.3.5 and 6.4.5 – 6.4.8 of this study.

[2724] *Thint* paras 133; *Powell v Van der Merwe* supra 38; Basdeo V *A Constitutional Perspective of Police Powers of Search and Seizure in the Criminal Justice System* (LL.M dissertation Unisa 2009) 68 (Basdeo *A constitutional search and seizure*).

[2725] Hubbard, Brauti and Fenton *Wiretapping* 3-7.

[2726] *Investigating Directorate v Hyundai and Smit No* supra 46; Paras 6.3.3.2(b), 6.3.3.3(b), 6.3.3.4(b), 6.3.3.5(b) and 6.4.8 of this study.

[2727] *Lahaie v Canada* (Attorney-General) (2010), 320 D.L.R (4th) 385, 190 A.C.W.S. (3d) 421 (Ont. C.A.). Application for eave to appeal was turned down, see 327 D.L.R (4th) iv; *R v Debot* (1989) 52 C.C.C. (3d) 193, [1989] 2 S.C.R. 1140, 3-8. *R v Debot* (1989) 52 C.C.C. (3d) 193, [1989] 2 S.C.R. 1140 at 1166, *R v Jir* (2010) 264, C.C.C (3d) 64, 80 C.R (6th) 53. The provisions of RICA use phrase 'reasonable ground to believe' in different contexts (which include sections 4(2)(b), 5(2)(b), 7(1) (a), 8(1)(b), 16(5)(a),(b) and (c), (8)(b)(ii), 17(4), 19(4), 21(4)(a), 22(4)(b), 23(4)(a) and 51(7) of RICA and the phrase 'reasonable ground to suspect' (in sections 6(3), 9(2), 10(2), 21(1) and 52 of RICA); NIA 'Investigations on Mr. Macozoma' at 6; Jurgens and Savides 2015- 07-12 *Sunday Times* 1-2; Maphumulo 2016-08-30 *The Sunday Independent* at 1; Shaikh 2015-08-30 *The Sunday Independent* 3; Puren 2015-10- 29 *You* 136-137; Maphumulo 2015-11-03 *The Star* 2;

Although the belief standard is *fluid* in form,[2728] the standard of proof required to enable LEAs to embark on an OCI is generally not based on mere speculation or suspicion.[2729] Belief is not just any form of suspicion but could be regarded as 'particularised suspicion'.[2730] Belief is an 'inclination of the mind towards assenting to, rather than rejecting, a proposition',[2731] which arguably stems from the detective and control point of view.[2732]

While it is advocated in some quarters that LEAs require a common sense, facts finding-oriented approach and practical considerations of everyday life in which reasonable and prudent men and that not legal technician's act makes inferences from the existence of the fact,[2733] others say that LEAs must be equipped with knowledge or skill similar to that of a judge.[2734]

However, borrowing from the principles guiding opinion evidence, it is argued that the standard skill required by LEAs in the determination of the 'reasonable ground to believe' is a relative one, which can be located in between the knowledge or skill of a layperson and an expert with regards to opinion evidence.[2735] The JSCI of the National Assembly of the RSA posits that a LEO must comprehend the facts necessary for the commission of a serious offence to conduct of an OCI, otherwise, an OCI cannot be conducted.[2736] The Court will not allow a copy and

---

Swart 28 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use:13 August 2016); Hubbard, Brauti and Fenton *Wiretapping* 3-7 to 3-9, 3-10.1 to 3-10.2, 3-15 and 4-28.

[2728] Hubbard, Brauti and Fenton *Wiretapping* 3-3 to 3-20.

[2729] The provisions of RICA use phrase 'reasonable ground to believe' in different contexts (which include sections 4(2)(b), 5(2)(b), 7(1) (a), 8(1)(b), 16(5)(a),(b) and (c), (8)(b)(ii), 17(4), 19(4), 21(4)(a), 22(4)(b), 23(4)(a) and 51(7) of RICA and the phrase 'reasonable ground to suspect' (sections 6(3), 9(2), 10(2), 21(1) and 52 of RICA); See Hubbard, Brauti and Fenton *Wiretapping* 3-3 – 3-20; see NIA 'Investigations on Mr. Macozoma' 6; Jurgens and Savides 2015-07-12 *Sunday Times* 1-2; Maphumulo 2016-08-30 *The Sunday Independent* at 1; Shaikh 2015-08-30 *The Sunday Independent* 3; Puren 2015-10- 29 *You* 136-137; Maphumulo 2015-11-03 *The Star* 2.

[2730] Hubbard, Brauti and Fenton *Wiretapping* 3-10.1 and 3-16.

[2731] Anon 'Drug Trafficking and organised Crimes (Amendment) Bill 2000- Note on "Reasonable Grounds to Suspect", "Reasonable Grounds Believe" and "Reasons for Introducing Two Money Laundering Offences Using Different Mental Elements"' Paper No CB (2)820/00-01(01) at 2.

[2732] Art 29(1)(a) and 30(4) of TOCC.

[2733] *Lahaie v Canada* (Attorney-General) (2010), 320 D.L.R (4th) 385, 190 A.C.W.S. (3d) 421 (Ont. C.A.). Application for eave to appeal was turned down, see 327 D.L.R (4th) iv; Hubbard, Brauti and Fenton *Wiretapping* 3-9 and 3-10.1 to 3-10.2, 3-15.

[2734] Hubbard, Brauti and Fenton *Wiretapping* 3-3 to 3-20.

[2735] Van der Berg E and Van der Merwe S E 'Opinion evidence' in Schwikkard P J and Van der Merwe S E *Principles of evidence* 3rd ed. (2012) 90 and 93-100. In Chapter Five, certain criteria will be examined to classify the level of seriousness of offences in RICA and other laws in which some offences will accordingly be examined with regards to the reasonable ground to believe in serious, more and most serious offences

[2736] JSCI Report 2016 at 40.

paste approach where a LEO copies the facts of the previous investigations and pastes in a new application which has become the practice for LEOs when conducting an OCI in the RSA.[2737]

The belief must contain sufficient grounds or better still draw from the totality of the circumstances in deciding whether to investigate an offence[2738] or whether to enter, search, seize, forfeit or arrest a person. It is however in practice impossible for a LEO to be aware of all the information necessary to form a reasonable ground to believe, more particularly when lengthy and complex investigations of criminal activities are at issue.[2739] The totality of the circumstances approach requires flexibility.[2740]

Essentially, on the one hand, if an offence is investigated earlier than the others, it arguably means that though all the facts in the commission of such an offence are *inchoate*, but an investigation is still pursued. This is because the effect of the commission of an offence is more serious (such as *most* and *more* serious offences conceptualised and classified in this study)[2741] than some other offences which are general serious offences.[2742] Consequently, the standard of proof for an investigation can, once again, arguably be located in a reasonable ground to *suspect* where the serious offence: i) *'will probably be committed*', which is '*merely speculative*' in nature in the conduct of an OCI and ii) *'is being committed*', which is '*reasonably speculative*' in nature in the conduct of an OCI.[2743]

On the other hand, if an offence is *not* required to be investigated *early* or if an offence is categorised as a *general serious offence*, there is or there must have been enough time to gather all the facts in the commission of such an offence to trigger an investigation which is located

[2737] JSCI Report 2016 at 40.

[2738] *Simataa v Magistrate of Windhoek* supra 10,12-13, 16, 20-21, 31-32, 34, 36, 39, 38 and 40-42; *Minister of Safety and Security & Another v Swart* (194/11) [2012] ZASCA 16 4, 5, 11, 12, 13, 19, 20, 21, 22 and 23; *Sydney v Minister of Safety & Security* Case No.: CA115/2009 5, 15, 16 and 17; Sections 20(a)-(c), 21(1)(a)-(b), 22(b), 24, 25(1) and (3), 26, 27(2) and 40(1)(b) of CPA; *Web Call v Botha* supra 7 and 8; Paper No. CB(2)820/00-01(01) Drug Trafficking and Organized Crimes (Amendment) Bill 2000 Note on "Reasonable Grounds to Suspect", "Reasonable Grounds to Believe" and Reasons for Introducing Two Money Laundering Offences using Different Mental Elements 1-4; *Powell v Van der Merwe* supra 62 SCA. Basdeo *A constitutional search and seizure* 61-78 and 108-117; NIA 'Investigations on Mr. Macozoma' 5 and 13-14.

[2739] Hubbard, Brauti and Fenton *Wiretapping* 3-9 to 3.10.1.

[2740] Hubbard, Brauti and Fenton *Wiretapping* 3-9 to 3-10 and 3.10.1.

[2741] Paras 6.3.3.2 (c)-(e), 6.3.3.3 (c)-(e), 6.3.3.4 (c) and (d) and 6.3.3.5 (c) -(e) of this study.

[2742] Paras 6.3.3.2 (b), 6.3.3.3 (b), 6.3.3.4 (b) and 6.3.3.5 (b) of this study.

[2743] See the introduction of para 6.4.4.2, 6.4.5, 6.4.6, 6.4.6.1, 6.4.6.2, 6.4.7, 6.4.7.1 and 6.4.7.2 of this study. Section 16(5)(a)(i) of RICA.

at the reasonable ground to *believe* standard where the offence '*has been committed*'[2744] or *completed*.

Given the defined and described concepts of suspicion and belief which are expressed in *accurate*, *specific*, *easily determinable*, and *mathematical* standards or formulae to conduct an OCI in the latter part of this study,[2745] some of the statutes and cases in this regard are examined below as per the herein italicised criteria which are conceptualised and examined in this study.[2746] It is noted that the examination below does not consider the validity of the limitation of the right of an individual in terms of entry, search, seizure, and arrest by LEAs or LEOs; rather, it examines the alignment of the *principal* or *composite* and *subsidiary* standards of proof in of 'suspicion' and 'belief' in the investigation of an offence.

b. Contradiction of the concepts of suspicion and belief in statutory provisions

Statutorily, the provisions in sections 21(1)(a), 22(2)(b), 25(1), 25(b)(ii), 25(3), 26, 27(2), 36(1)(a) and (b), 36C, 36E, 37(2)(b) of the CPA are examined with emphasis on the contradiction or inconsistency in the application of the standards of 'suspicion' and 'belief' when conducting an investigation. A provision in the POPIA is also considered in this regard.

Firstly, the consideration on whether there is a contradiction between the principal and subsidiary standards of proof to investigate an offence is provided in section 21(1)(a) of the CPA as follows:

> '(1) Subject to the provisions of sections 22, 24 and 25, an article referred to in section 20 shall be seized only by virtue of a search warrant issued—
>
> (a) by a *magistrate* or *justice*, *if it appears* to *such magistrate* or *justice* from information on oath that there are *reasonable grounds for believing* that any such article is *in the possession* or *under the control of* or *upon any person* or *upon* or *at any premises* within his area of jurisdiction'[2747]

[2744] Paras 6.3.3.2 (b), 6.3.3.3 (b), 6.3.3.4 (b), 6.3.3.5 (b) and 6.4.8 of this study.
[2745] Paras 6.4.4.1, 6.4.4.2, 6.4.4.3, 6.4.5, 6.4.6, 6.4.6.1, 6.4.6.2, 6.4.7, 6.4.7.1, 6.4.4.2, 6.4.8 and 6.4.9 of this study.
[2746] Paras 6.4.5 -6.4.8 of this study.
[2747] Italics mine.

In section 21(1)(a) of the CPA, the intention of the Legislature is clear to the extent that the clause '*reasonable grounds to believe*' is symmetric with the action by the investigatee who must have been '…*in the possession of*…'. This clause completes the elements of the commission of an offence that warrants a *belief* in the mind of a LEO to conduct an investigation and not a suspicious mind. However, it is argued that section 21(1)(a) contradicts itself by the use of the clause '…*if it appears*…' in the context that it is used herein because the clause is a synonym for the word 'seems' and other related words which can be located in the suspicious standard which does not align with the clause '*reasonable grounds for believing*'.

In the field of Philosophy as a subject matter, more importantly in the subdiscipline of the 'Problems of Philosophy' and most importantly, 'Appearance and Reality'; 'appearance' is not 'reality'. The former is more or less like a mirage which is likened to '*suspicion*' while 'reality' which is likened to '*belief*' is more relatively concrete as or dependent on a substance of existence in the context that it is used.

Thus, the Legislature, on the one hand, intended to invoke the '*belief*' standard which is rightly symmetric with the action of the investigatee who acts upon the completed or commission of an offence based on the earlier distinction made under this rubric above. On the other hand, the Legislature mistakenly applied an erroneous word in the draft of the legislation by inserting the word '*appears*' in the same provision, which negatives the belief standard intended in this provision. If the provision of section 21(1)(a) of the CPA is interpreted by the court with this approach, it will be contradictory as illustrated in the case law below and generally in this study.[2748]

It is therefore arguably recommended that the following re-draft may settle the lacuna in section 21(1)(a) of the CPA by expunging the clause '…*if it appears*…' with the italicised clause:

> 'by a magistrate or justice *based on the*[2749] information on oath that there are reasonable grounds for believing that any such article is in the possession or under the control of or upon any person or upon or at any premises within his area of jurisdiction'.[2750]

[2748] Para 6.4.4.3 of this study.
[2749] The italicized clause is my contribution to the provision.
[2750] Italics mine.

Secondly, the consideration on whether there is an inconsistency between the principal and subsidiary standards of proof to investigate an offence is examined in, section 22 (b) of the CPA as follows:

> '22 A police official may without a search warrant search any person or container or premises for the purpose of seizing any article referred to in section 20—
> (b) if he on *reasonable grounds believes*—
> (i) that a search warrant will be issued to him under paragraph (a) of section 21(1) if he applies for such warrant;'

Section 22(b) of the CPA does not apply to the issue being discussed in this rubric, which is the contradiction or inconsistency in the application of the standards of 'suspicion' and 'belief' in the investigation of an offence. This is because this provision does not relate to the substantive standard of proof to investigate a crime. However, the provision relates to the administrative or procedural necessity to search a person, container or premises in lieu of a warrant which can thereafter be issued by the authority to prevent the frustration of not being able to arrest a person while he or she is in the presence of the arrestor.[2751]

Thirdly, the consideration on whether there is a contradiction between the principal and subsidiary standards of proof to investigate an offence is stipulated in section 25(1) of the CPA as follows:

> '(1) *If it appears* to a *magistrate* or *justice* from information on oath that *there are reasonable grounds for believing*—
> (a) that the internal security of the Republic or the maintenance of law and order *is likely to be endangered* by or in consequence of any meeting which *is being held* or *is to be held* in or upon any premises within his area of jurisdiction; or
> (b) that *an offence has been* or *is being* or *is likely to be committed* or that preparations or arrangements for the commission of any offence *are being* or *are likely* to be made in or upon any premises within his area of jurisdiction,
>
> he may issue a warrant authorising a police official to enter the premises in question at any reasonable time for the purpose—
> (i)of carrying out such investigations and of taking such steps as *such police official may consider necessary* for the preservation of

[2751] See also section 25(3) the CPA which has the same provision with section 22(b) of the CPA.

> the internal security of the Republic or for the maintenance of law and order or for the prevention of any offence;
> (ii) of searching the premises or any person in or upon the premises for any article referred to in section 20 which such police official on *reasonable grounds suspects* to be in or upon or at the premises or upon such person; and
> (iii) of seizing any such article.'[2752]

In interpreting this provision, the earlier submissions on the contradiction made in section 22(1)(a) of the CPA are adopted *mutatis mutandis* as they relate to the clauses herein. In particular, the contradictions in section 25(1) of the CPA are however expressed in the following 'suspicious' standard clauses: '…*is likely to be endangered*…', '… *is being held* or *is to be held*…' '…*is being* or *is likely to be committed*…', '…*are being* or *are likely to be made*...', '…*may consider necessary*…' and '…such police official *on reasonable grounds suspects*…'.

These clauses do not constitute completed actions that will warrant an investigation by a LEO according to the principal or coordinate standard intended by Legislature in section 25(1) which is a '*belief*' standard expressed as '*...there are reasonable grounds for* believing—...', therefore, the principal or coordinate standard should have been a suspicious standard that aligns with the clauses above.

Fourthly, the consideration on whether there is an inconsistency between the principal and subsidiary standards of proof to investigate an offence is prescribed in section 26 of the CPA as follows:

> 'Where a police official in the investigation of *an offence* or *alleged offence reasonably suspects* that a person who may furnish information with reference to any such offence *is on any premises*, such police official may without warrant enter such premises for the purpose of interrogating such person and obtaining a statement from him: Provided that such police official shall not enter any private dwelling without the consent of the occupier thereof.'[2753]

In this provision, there is a contradiction in the principal or coordinate and subsidiary standards of proof to investigate an offence. The clause '…*is on any premises*…' is an action that has been completed which is likened to 'belief', the principal standard of which investigation is

[2752] Italics mine.
[2753] Italics mine.

'suspicion' which is expressed in the use of the clause 'Where a police official in the investigation of *an offence* or *alleged offence reasonably suspects*'. In other words, the principal standard with which the action is being investigated does not align with the action for which the investigation was conducted.

The fifth consideration on whether there is a contradiction between the principal and subsidiary standards of proof to investigate an offence is provided in section 36C of the CPA as follows:

> '(1) Any police official *may* without warrant take fingerprints or body-prints of a person or a group of persons, *if there are reasonable grounds* to—
> (a)*suspect* that the person or that one or more of the persons in that group *has committed* an offence referred to in Schedule 1; and
> (b)*believe* that the prints or the results of an examination thereof, *will be of value* in the investigation by *excluding* or *including* one or more of those persons as *possible perpetrators of the offence*.[2754]

In section 36C(1)(a) of the CPA, there is a contradiction between the principal and subsidiary standards of proof to investigate in the use of the clause '…*may* without warrant *take fingerprints*…if *there are reasonable grounds to*…*suspect*', which is a standard of 'suspicion', on the one hand and the action that necessitates investigation 'that the person…*has committed offence*', is a standard of 'belief', on the other hand. The question is, why would a LEO still be suspicious to take a fingerprint of a person if the LEO can conclude that the person has committed an offence under Schedule 1 of the CPA, which becomes a 'belief' standard at this stage?

In section 36(1)(b) of the CPA, there is also a contradiction between the principal or coordinate and subsidiary standards of proof to investigate a crime. On the one hand, '(1) Any police official *may* without warrant *take fingerprints* or *body-prints* of a person…' is discretionary which creates a 'suspicious' standard. On the other hand, '*if there are reasonable grounds* to—' (b)*believe* that the prints or the results of an examination thereof, *will be of value* in the investigation by *excluding* or *including* one or more of those persons as *possible perpetrators* of the offence' constitutes both 'belief' and 'suspicious' standards.

[2754] Italics mine.

The contradiction is seen in the 'belief' standard which is expressed as follows '…if *there are reasonable grounds to-(b) believe…will be of value*…' while the 'suspicious' standard is expressed as follows '*excluding* or *including*…as a *possible perpetrator of the offence*'. In other words, if the authorities are not certain about whether to *exclude* or *include* a person as *a possible perpetrator* of the offence in an investigation, why would anyone want to take a finger or body print of a person against whom there is no conclusive fact to constitute a 'belief' standard to investigate? This construction creates a contradiction or inconsistency in this provision.

The sixth consideration on whether there is an inconsistency between the principal and subsidiary standards of proof to investigate an offence is stipulated in section 36E of the CPA as follows:

> '(1) Subject to subsection (2) and section 36A(5), an authorised person *may take a buccal sample* of a *person* or a *group* of persons, or *supervise the taking of a buccal sample* from a *person* who is required to submit such sample and who requests to do so himself or herself if *there are reasonable grounds to*—
> (a) *suspect* that the person or that one or more of the persons in that group *has committed an offence* referred to in Schedule 8; and
> (b) *believe* that the *buccal sample* or the *results of the forensic DNA analysis thereof, will be of value* in the investigation by excluding or including one or more of those *persons as possible perpetrators of the offence*.
> (2) If a person does not consent to the taking of a buccal sample under this section, a warrant *may* be *issued* by a *judge* or a *magistrate if it appears* from written information given by the authorised person on oath or affirmation that *there are reasonable grounds for believing* that—
> (a) any person from whom a buccal sample is required *has committed an offence* listed in Schedule 8; and
> (b) the sample or the results of an examination thereof, *will be of value* in the investigation by *excluding* or *including* that person as *a possible perpetrator of the offence*.'[2755]

In section 36E(1)(a) of the CPA, the principal standard of proof to investigate is 'suspicion' as set out in the use of the clauses 'an authorised person *may take a buccal sample*…or *supervise*…' and '*there are reasonable grounds to suspect*'. However, the action that triggers an investigation which is '…*a person…has committed an offence*', which is a complete action is based on 'belief' standard which does not align with the principal standard. This non-

[2755] Italics mine.

alignment creates a contradiction in the standard of investigation, which leads to the misinterpretation by the courts, as will be shown below under case law analysis of the concepts of 'suspicion' and 'belief'.

In section 36E(1)(b) of the CPA, there is an inconsistency between the standard of proof in the use of the clauses '*may take a buccal sample*…or *supervise*…', on the one hand, and the '*reasonable ground to suspect*' and the '*believe* that the *buccal sample* or the *results of the forensic DNA analysis thereof, will be of value*', on the other hand. Whereas the standard of proof to investigate in the former is 'suspicion', the standard of proof to investigate in the latter is 'belief'.

The question therefore is, if there is a 'belief' that the buccal sample or the results of the forensic DNA analysis will be of value, why then would the decision of the authorised person to take the buccal sample be discretionary with the use of the word '*may*'? In conclusion, the two standards are contradictory in conducting an investigation. This results in uncertainty in an investigation which is pronounced by the courts, in addition to the fact that the courts have not pronounced on accurate, specific and easily determinable criteria, standard or formulae that will aid or assist in conducting an investigation.

In section 36E(2)(a) of the CPA, there is a contradiction in the standard of proof to investigate. On the one hand, 'a warrant *may* be *issued* by a *judge* or a *magistrate* if it *appears*' is a 'suspicious' standard which is not a conclusive proof. On the other hand, '*there are reasonable grounds for believing* that—any person from whom a buccal sample is required *has committed an offence*' is a conclusive proof, which is a 'belief' standard. Essentially, the standard in the former contradicts that of the latter; thus, leads to the erroneous interpretation by the courts as it is generally demonstrated in the case law below.

In section 36E(2)(b) of the CPA, there is a contradiction in the standard of proof to investigate. On the one hand, 'a warrant *may* be *issued* by a *judge* or a *magistrate if it appears*' is a 'suspicious' standard which is not a conclusive proof. On the other hand, '*there are reasonable grounds for believing* that— the sample or the results of an examination thereof, *will be of value* in the investigation by *excluding* or *including* that person as *a possible perpetrator of the offence*' constitutes both belief and suspicious standards. The contradiction is seen in the 'belief' standard in the latter which is expressed as follows '…*there are reasonable grounds*

for believing…will be of value…' while the 'suspicious' standard is expressed as follows '*excluding* or *including* that a person as *a possible perpetrator of the offence*'.

In other words, if the authorities are not certain about whether to *exclude* or *include* a person as *a possible perpetrator* of the offence in an investigation due to the 'suspicious' standard applied in this provision, why would any authority want to take a buccal sample of a person against whom there is no conclusive fact to constitute a 'belief' standard to investigate an offence? This construction creates a contradiction in this provision.

The seventh consideration on whether there is a contradiction between the principal and subsidiary standards of proof to investigate an offence is prescribed in section 37(2)(b) of the CPA as follows:

> 'If any registered medical practitioner attached to any hospital is on *reasonable grounds of the opinion that the contents of the blood of any person admitted to such hospital for medical attention or treatment may be relevant at any later criminal proceedings*, such medical practitioner *may take a blood sample* of such person or cause such sample to be taken.'[2756]

The principal or coordinate standard of proof to take a blood sample of a patient in section 37(2)(b) is the standard of 'suspicion' because of the use of the clause '*reasonable grounds of the opinion*' of a medical practitioner, the standard of which does not express a 'belief' standard as examined above in this rubric, therefore, there is *no contradiction* herein. The 'suspicious' standard is corroborated by the action that is expected of a medical practitioner who '*may take a blood sample*' where the taking of blood sample '*may be relevant at any later criminal proceedings*. Thus, since the expression of an 'opinion' does not constitute a 'belief' in the strict context of the issue at stake in this study, the action that needs to be fulfilled to conduct an investigation aligns with the principal standard of proof to conduct an investigation, which in this instance, is 'suspicion'.

However, despite the alignment of the principal and subsidiary standards in section 37(2)(b) of the CPA, this provision still does not set an accurate, specific and easily determinable criteria, standard or formulae that will aid or assist the medical practitioner to precisely determine if a blood sample will be taken for a later criminal proceeding.

[2756] Italics mine.

The eighth consideration on whether there is an inconsistency between the principal and subsidiary standards of proof to investigate an offence is stipulated in section 27(2) of the CPA as follows:

> 'The proviso to subsection (1) shall not apply where the police official concerned is on *reasonable grounds of the opinion* that any article which is the subject of the search *may be destroyed* or *disposed of* if the provisions of the said proviso are first complied with.'

In this provision, there is *no contradiction* in the principal or coordinate and subsidiary standards of proof to investigate an offence. It is submitted that the principal standard of proof for investigation which is '…*reasonable grounds of the opinion*…' is likened to 'suspicion' and aligns with the action '…*may be destroyed or disposed of*…' which is also likened to 'suspicion', given the irreversible effect of the action on an article. Thus, absolute facts are not required to investigate the offence of destruction or disposal at 'belief' standard but 'suspicion' standard.

However, despite the alignment of the principal and subsidiary standards in section 27(2) of the CPA, this provision still does not set an accurate, specific and easily determinable criteria, standard or formulae in this regard.

The ninth consideration on whether there is a contradiction between the principal and subsidiary standards of proof to investigate an offence is prescribed in section 36(1)(a) and (b) of the CPA as follows:

> '(1) Where an *article* is seized in connection with which—
> (a) *an offence was committed or is on reasonable grounds suspected to have been committed* in a country outside the Republic;
> (b) there are *reasonable grounds for believing* that *it will afford evidence as to the commission in a country outside the Republic of any offence* or that it *was used* for the purpose of or in connection with such commission of any offence,
>
> the magistrate within whose area of jurisdiction the article was seized *may, on application* and *if satisfied* that *such offence is punishable in such country by death* or by *imprisonment for a period of 12 months* or *more* or *by a fine of five hundred rand* or more, *order such article to be delivered to a member of a police*

> *force established in such country who may thereupon remove it from the Republic*.'[2757]

There are some contradictions in this provision. These contradictions are similar to the contradictions in the other provisions under this rubric.[2758]

However, there is a reasonable, accurate, specific and easily determinable standard or formulae to investigate an offence by the insertion of the clause '…*if satisfied* that *such offence is punishable in such country by death* or by *imprisonment for a period of 12 months* or *more* or *by a fine of five hundred rands* or more…'. The accuracy of the standard to investigate is centred on whether a foreign country punishes such an offence with a death penalty, imprisonment of 12 months or more or by a fine of five hundred rands or more, all of which standards are reasonably specific and easily determinable to investigate an offence.

The tenth consideration on whether there is an inconsistency between the principal and subsidiary standards of proof to investigate an offence is provided in section 21(2) of the POPIA as follows:

> The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person.

Although section 21(2) of the POPIA is not a provision that requires a criminal investigation, given that the non-compliance with the provision is not criminally sanctioned in the POPIA,[2759] however, the provision clearly illustrates the validity of the alignment of the principal and subsidiary standards of proof to conduct an investigation. This alignment is generally not available in the CPA, as examined above.

In section 21(2) of the POPIA, the concept 'belief' is consistently applied. Immediately it is established that the personal information of a data subject has been accessed or acquired by an unauthorised person, the activity of unauthorisation constitutes a concluded activity and therefore, there is a belief and not a suspicion that there is an unauthorisation. Therefore, the operator is bound to notify the responsible party of the completion of the activity which is the

[2757] Italics mine.
[2758] See the first to the sixth provision examined above.
[2759] See sections 19 and Chapter 11 of the POPIA.

unauthorised access and acquisition of personal data of a data subject. The duty to notify is not discretionary, hence the use of the word 'must' and not the use of the word 'may' in section 21(2) of the POPIA.

In the overall conclusion, there is only one provision which is not relevant to the issues discussed in this rubric under the CPA.[2760] However, aside from sections 37(2)(b) and 27(2) of the CPA and section 21(2) of the POPIA examined in the seventh, eighth and tenth rubrics above in which there is an alignment between the principal and subsidiary standards of proof to investigate an offence, there is no alignment or symmetry in other provisions examined above in this regard.

In other words, there are six major clear contradictions on the concepts of 'suspicion' and 'belief' out of the ten provisions examined above. The contradiction is in the use of 'suspicion, which is a low standard, as the principal or coordinate standard in one breathe, but still, the authorities apply the 'belief' standard, which is a high standard, in the action expected to trigger an investigation of a criminal offence, on the other hand, and vice versa.

To prevent a disequilibrium between the protection of the right to the SOC and the conduct of an OCI, it is therefore recommended that the various legislations concerning investigation that do not have an alignment between the principal and subsidiary standards of proof to investigate an offence should be amended to reflect the lessons learnt under this rubric.

c. Contradiction of the courts in the concepts of 'suspicion' and 'belief'

Arguably, the decisions of the Constitutional Court in *Investigating Directorate v Hyundai* and *Smit No* and *Thint*[2761] which are generally examined in this study and other cases by other courts on the concepts of 'suspicion*'* and 'belief*'* in the legislations are erroneous.

[2760] See the second provision in this rubric which is section 22(b) of the CPA.

[2761] The serious offences mentioned in these cases include tax matters, fraud, theft, forgery, uttering, corruption or an economic offence involving patrimonial loss, see *Investigating Directorate v Hyundai and Smit No* supra 46, 48, 53 and 54 and *Thint* supra 127, 153, 168, 247, 252 and 257.

Firstly, in the cases summarised below, the courts did not distinguish between the concepts of 'suspicion' and 'belief' concerning the seriousness of an offence which must be investigated earlier than the others.

Secondly, there is no case law on the distinction between the concepts of 'suspicion*'* and 'belief*'* in terms of setting an accurate, specific, easily determinable, and mathematical standards of formulae in conducting an *early* offline investigation of some offences that are more serious than the others, let alone set a standard in the conduct of an OCI. Arguably, at best, the Constitutional Court only compared the two concepts in *Investigating Directorate v Hyundai* and *Smit No* and *Thint*[2762] but did not contrast the concepts, as this study clearly does in the overall analysis.

Firstly, whether there is a contradiction between the principal and subsidiary standards of proof to investigate an offence is considered in Bristowe J in *LSD v Vachell* where the court held that:

> 'Warrants *may* be issued under sec. 49(1)(b) and (c) of Act 31 of 1917 directing search for and seizure of anything as to which there are *reasonable grounds for believing that it will afford evidence as to the to the commission of any offence,* or that itis intended to be used for the purpose of committing any offence; the offences referred to being quite general and notconfined to such as are mentioned in sec. 49(1)(a) as being in respect to corpora delicti.' [2763]

In addition to the earlier general interpretation of the word 'may',[2764] the effect of which in this rubric is 'suspicion' or discretionary, on the one hand, or mandatory (which means 'shall' where the execution of a particular mandate is compulsory) on the other hand; the use of '*may*' as the principal or coordinate standard of proof contradicts the 'belief' standard which is the subsidiary standard upon which an investigation is conducted.[2765]

[2762] The serious offences mentioned in these cases include tax matters, fraud, theft, forgery, uttering, corruption or an economic offence involving patrimonial loss, see *Investigating Directorate v Hyundai and Smit No* supra 46, 48, 53 and 54 and *Thint* supra 127, 153, 168, 247, 252 and 257.

[2763] *LSD v Vachell* 1918 WLD 127. Italics mine.

[2764] See para 3.9 of this study which examines the word 'may' in the role of stakeholder in the techno-legal integrity and security of the SOC in major statutes relating to the protection of online communication.

[2765] See paras 6.4.2.2 and 6.4.2.2(a) of this study.

However, to correct the defect in this case, it is argued that the word 'may' should be interpreted as 'shall'[2766] which is the principal or coordinate standard to apply in an investigation in this case. This is because the two subsidiary standards are premised on 'belief' standard which is arguably compelling that an investigation be conducted in the statutory provision. The subsidiary standards upon which an investigation is conducted are that:

> '*…there are reasonable grounds for believing that it will afford evide nce as to the commission of any offence*…'.[2767]

Secondly, whether there is an inconsistency between the principal and subsidiary standards of proof to investigate an offence is considered in *Secombe v Attorney-General* where the court held that:

> '…the complaint must show that there are *reasonablegrounds for susp ecting* that *any of the things* coming within the sub-section I have mentioned *are on the premises to be searched*. I think that protects a search warrant from being described a s a fishing or a roving warrant. Of course, you may call it a fishing warrant because it is looking for evidence, but at all ev ents the section provides that *there must be reasonable grounds for believing* that *an offence has been* or *is intend ed to be committed*. Whether it is fishing or not, as I have said, all I have to do is to construe the section.'[2768]

In *Secombe v Attorney-General,* there is an inconsistency in the principal or coordinate and subsidiary standards of proof in investigating this case because these two standards do not align with each other. There is a disequilibrium in the first sentence above because a complaint cannot, on the one hand, 'suspect' '…that there are *reasonable grounds for suspecting*…' and, on the other hand, rely on a 'belief' standard in the clause '…that *any of the things* coming within the subsection I have mentioned *are on the premises to be searched*.'

[2766] See para 3.9 of this study which examines the word 'may' in the role of stakeholder in the techno-legal integrity and security of the SOC in major statutes relating to the protection of online communication.
[2767] *LSD v Vachell* 1918 WLD 127.
[2768] *Secombe v Attorney-General* supra 273 - 274. Italics mine.

There is an alignment in the second sentence in the ratio above which is to the effect '…that *there must be reasonable grounds for believing that an offence has been… committed*'[2769] because the principal and subsidiary standards of investigation align with each other. However, there is a contradiction between the clause '…that *there must be reasonable grounds for believing that an offence…is intended to be committed*.'[2770] This is because the principal standard which is 'belief' does not align with the subsidiary standard which is '…*an offence is intended to be committed*'.

Thus, the principal standard should have been a 'suspicious' standard that aligns with the subsidiary standard of 'suspicion' too, aimed at giving effective meaning to the distinction between 'suspicion' and 'belief' standards which are described by the Constitutional Court. However, no *specific*, *accurate*, and *easily determinable* standard or formulae to investigate an offence was set by the court in *Investigating Directorate v Hyundai* and *Smit No* and *Thint*[2771] as opposed to the proposed formulae in this study.[2772]

Thirdly, whether there is a contradiction between the principal and subsidiary standards of proof to investigate an offence is considered in *Cine Films v Commissioner of Police*[2773] as follows:

> '"Whereas *it appears to me* on complaint made on oath that *there are reasonable ground for suspecting* that there *is upon* or *at the premises situated at*" (here follows a description of the premi ses)-
> Something in respect of which *there are reasonable grounds for belie ving* that *it will afford evidence as to the commission of an offence*, to wit, a contravention of sec. 22 (1) of Act 63 of 1965- Copyright Act, to wit: all stock books, stock sheets, invoices, invoice books, consignment notes, all correspondenc e, film catalogues and all films appearing on the attached list in respect of which a licence to publish is not held and an y other correspondence or circulars referring to such films.'[2774]

[2769] *Secombe v Attorney-General* supra 273-274 and 279-280.
[2770] *Secombe v Attorney-General* supra 273-274 and 279-280.
[2771] The serious offences mentioned in these cases include tax matters, fraud, theft, forgery, uttering, corruption or an economic offence involving patrimonial loss, see *Investigating Directorate v Hyundai and Smit No* supra 46, 48, 53 and 54 and *Thint* supra 127, 153, 168, 247, 252 and 257.
[2772] Paras 6.3.3.2(a)-(e), 6.3.3.3(a)-(e), 6.3.3.4(a)-(d), 6.3.3.5(a)-(e) and 6.4.5- 6.4.8 of this study.
[2773] *Cine Films v Commissioner of Police* supra 574.
[2774] Italics mine.

In a similar vein, as previous cases have been examined above, there are contradictions in the principal or coordinate and subsidiary standards in the *Cine Films v Commissioner of Police*[2775] which are highlighted in the italicised words above.

Fourthly, whether there is an inconsistency between the principal and subsidiary standards of proof to investigate an offence is considered by the court where it held in *R v Van Heerden*[2776] that:

> '*An arrest is clearly an assault*, and the appellant can only justify that assault if he shows, as stated in sec. 24 (1) (c) that he had "*reasonable grounds to suspect." It is not sufficient for him to show that he did in f act have a suspicion*.'[2777]

Similarly, there is an inconsistency between the principal or coordinate and subsidiary standards in the above-italicised words as expressed in previous cases examined under this rubric.

Fifthly, whether there is a contradiction between the principal and subsidiary standards of proof to investigate an offence is considered in *Ndabeni v Minister of Law & Order* where the court held that:

> '*Believing that the magazine promoted the objects of SASO*, that *its dis tribution would therefore amount to an offence* and that *its publication had already done so*, the second respondent *believ ed* by the same token that the copies which he seized had been concerned *in the completed offence* and were intended to be used in the planned one. *They would also afford evidence of an offence or suspected offence*, he thought, either t hat which had been committed in his eyes when the magazine was published or some other lurking in AZAPO's activities.'[2778]

In *Ndabeni v Minister of Law & Order*, the principal and coordinate standards which bother on 'belief' align with each other, on the one hand; while the principal standard which is 'belief' does not align with the uncompleted action '*its distribution would therefore amount to an*

[2775] *Cine Films v Commissioner of Police* 574.
[2776] *R v Van Heerden* supra 150.
[2777] *R v Van Heerden* supra 128. Italics mine.
[2778] *Ndabeni v Minister of Law & Order* supra 500. Italics.

offence' because the latter action is premised on a 'suspicious' standard as opposed to the completed clause '*its publication had already done so*'.

In the sixth case, whether there is an inconsistency between the principal and subsidiary standards of proof to investigate an offence is considered in *Alex Cartage v Minister of Transport* where the court pronounced as follows:

> 'empowering any inspector or any member of the South African Polic
> e to seize any motor vehicle *suspected on reasonable*
> *grounds to have been used in unauthorized road transportation*, and a
> ny goods upon such motor vehicle, and providing for
> the manner in which a motor vehicle and goods so seized shall be deal
> t with pending the disposal of criminal proceedings
> in respect of such unauthorized road transportation…[2779]
> (3)…an inspector and any member of
> the South African Police *may impound any motor vehicle reasonably s*
> *uspected of having been used in connection with the*
> *conduct of unauthorised road transportation*, as well as the goods con
> veyed on such vehicle."[2780]

The erroneous draft of this provision is not different from previous cases examined above because there is an obvious inconsistency in the principal and subsidiary standards of proof to investigate the offence in the italicised clause. A LEO cannot rely on 'suspicion' over an offence that has already been committed ('belief') whereby a motor vehicle had been used in unauthorised road transportation.[2781] Therefore, it is recommended that the principal standard of proof should be 'belief' standard which will be symmetric with the action of using unauthorised road transportation.

In the seventh case, whether there is a contradiction between the principal and subsidiary standards of proof to investigate an offence is considered in *Mnyungala v Minister of Safety & Security* where the court held that:

> '…the vehicle was seized in terms of sections 20 and 22 of the Cri
> minal Procedure Act 51 of 1977. Section 20
> permits the seizure of any property concerned in or *reasonably beli*
> *eved to be concerned in the commission or suspected*
> *commission of an offence*. The person effecting the seizure in this c

[2779] *Alex Cartage v Minister of Transport* supra 72-73.
[2780] *Alex Cartage v Minister of Transport* supra 73. Italics mine.
[2781] *Alex Cartage v Minister of Transport* supra 72-73 and 74.

> ase was found not to have formed the necessaryreasonable belief at the relevant time.'[2782]'…the State *may* seize anything (termed an " article"), inter alia, "which is concerned inor on *reasonable ground s believed* to be concerned *in thecommission* or *suspected commissi on of an offence*" or "which may afford evidence of the commissio n or suspected commission of an offence".' [2783]

Although there is an alignment of the principal and subsidiary standards of 'belief' in *Mnyungala v Minister of Safety & Security*, however, there are contradictions in the 'belief' and 'suspicion', all of which is italicised.

In the eighth case, whether there is an inconsistency between the principal and subsidiary standards of proof to investigate an offence is considered in *Ralekwa v Minister of Safety & Security* where the court reinstated a legislative provision as follows:

> "8 Warrant of arrest upon issuing of protection order (1) …. (2) …. 11 (3) …. (4) (a) A complainant *may* hand the warrant of arrest together with an affidavit in the prescribed form, wherein it is stated that *the respondent has contravened any prohibition, condition, obligation or order contained in a protection order*, to any member of the South African Police Service. (b) *If it appears to the member* concerned that, subject to subsection (5), *there are reasonable grounds to suspect* that the complainant *may suffer imminent harm* as a result of the alleged breach of the protection order by the respondent, the member must forthwith arrest the respondent *for allegedly committing the offence* referred to in section 17(a).'[2784]

In both paragraphs (a) and (b) of the statute, there are contradictions in the principal and subsidiary standards of proof to investigate the offence which are highlighted in italics above.

The court in *Ralekwa v Minister of Safety & Security* also pronounced as follows:

> 'In order for me to pronounce that Forbes exercised his discretion irrationally, I must conclude that the Plaintiff's arrest was not in accordance with section 8(4) of the Act, and that Forbes failed to apply the standards specified as contemplated in section 8(5) in arriving at the decision to arrest him. These subsections as fully quoted above make it clear that for Forbes to have been permitted to arrest the Plaintiff in terms of the Act, *it had to appear to him* that there were '*reasonable*

[2782] *Mnyungala v Minister of Safety & Security* supra 1.
[2783] *Mnyungala v Minister of Safety & Security* supra 1. Italics mine.
[2784] *Ralekwa v Minister of Safety & Security* 2004 (2) SA 342 para 24. Italics mine.

> *grounds to suspect*' that the Complainant may suffer 'imminent harm 'as a result of the alleged *breach of the protection order*. (My underlining). The word may in this context does not mean that the arresting officer must be convinced that 'harm is about to happen, if not certain to happen'. It only suggests there may be a possibility that it (imminent harm) may well happen.'[2785]

The foregoing pronouncement also highlights a contradiction in the principal and subsidiary standards of proof to investigate an offence in the italicised words because the use of the clause '*it had to appear to him*' falls under suspicion while the action is premised '*breach of the protection order*'.

In the ninth case, whether there is a contradiction between the principal and subsidiary standards of proof to investigate an offence is considered in *Minister of Safety & Security v Sekhoto*[2786] where the Supreme Court of Appeal expressed some inconsistency by simultaneously applying the suspicious and belief standards in the following ratios:

> 'The first plaintiff, Mr Sekhoto, was arrested on 15 July 2002 on *suspicion* of a contravention of section 2 of the Stock Theft Act 57 of 1959, which provides that a person *who is found in possession of stock or produce*, in regard to which there is *reasonable suspicion* that it *has been stolen* and *is unable to give a satisfactory account of such possession*, is guilty of an offence.'[2787] 'The plea was based on a defence contained in section 40(1)(b) and (g) of the Act, which provide that a peace officer *may* without warrant arrest any person –(b)whom he *reasonably suspects* of *having committed an offence* referred to in Schedule 1; or (g)who is *reasonably suspected* of *being* or *having been in unlawful possession of stock or produce* as defined in any law relating to the theft of stock or produce.'[2788] '...the jurisdictional facts for a section 40(1)(b) defence are that (i) the arrestor must be a peace officer; (ii) the arrestor must entertain *a suspicion*; (iii) the *suspicion* must be that the suspect (the arrestee) *committed an offence* referred to in Schedule 1; and (iv) the *suspicion must rest on reasonable grounds*. For purposes of para (g) the *suspicion must be that the arrestee was or is in unlawful possession of stock or produce as defined in any law relating to the theft of stock or produce*'.[2789] 'It is also accepted that it is for the police to prove on *the balance of probabilities* that the arresting officer *suspected* that *the person arrested was guilty of the offence* and that there were *reasonable grounds for that suspicion*.'[2790]

[2785] *Ralekwa v Minister of Safety & Security* paras 33 and 39. Italics.
[2786] *Minister of Safety & Security v Sekhoto* 2011 (5) SA 367 (SCA).
[2787] *Minister of Safety & Security v Sekhoto* supra 2, 21, 23 and 26. Italics mine.
[2788] *Minister of Safety & Security v Sekhoto* supra 5. Italics mine.
[2789] *Minister of Safety & Security v Sekhoto* supra 6, 21, 23 and 26. Italics mine.
[2790] *Minister of Safety & Security v Sekhoto* supra 53. Italics mine.

In summary, since the arrestee was found in possession of stock, the standard to be used to investigate could not have been a suspicion but belief, both of which are contradicted in this case.

In conclusion, the above cases in the RSA only express some broad, descriptive, interchangeable or simultaneous, and erroneous applications of the concepts of 'suspicion' and 'belief' to the facts of a matter. These cases do not pin down some *accurate*, *practical*, *specific*, *certain* and *easily determinable* standards or formulae to conduct a general criminal investigation, let alone apply such description to the conduct of an OCI to give meaning and effect to their descriptions.

d. Conclusion

In the overall conclusion on the distinction between 'suspicion' and 'belief' standards, the two main effects of the ratio of the Constitutional Court in *Investigating Directorate v Hyundai and Smit No* and *Thint*[2791] are the classifications of offences and the *accurate*, *specific* and *easily determinable* standards of proof to accordingly investigate such classified offences. These two effects must be symmetrical, otherwise, the effects of the ratio of the Constitutional Court create a legal incongruity which leaves the court and LEAs or LEOs in the battlefield of determining the validity of every investigation.

This is because the principal or coordinate and subsidiary standards for investigation in most of the statutory provisions and case law examined under this rubric are not symmetrical to comply with the effect of the ratio of the Constitutional Court in *Investigating Directorate v Hyundai and Smit No* and *Thint.*[2792] Thus, this ratio actually identifies the conflict on how the courts and LEAs or LEOs misconstrue the standard of proof used in an investigation.

[2791] The serious offences mentioned in these cases include tax matters, fraud, theft, forgery, uttering, corruption or an economic offence involving patrimonial loss, see *Investigating Directorate v Hyundai and Smit No* supra 46, 48, 53 and 54 and *Thint* supra 127, 153, 168, 247, 252 and 257.

[2792] The serious offences mentioned in these cases include tax matters, fraud, theft, forgery, uttering, corruption or an economic offence involving patrimonial loss, see *Investigating Directorate v Hyundai and Smit No* supra 46, 48, 53 and 54 and *Thint* supra 127, 153, 168, 247, 252 and 257.

In concluding this rubric on the standards of 'suspicion' and 'belief', it is submitted that the factors that are cumulatively considered in the totality of the circumstances for 'suspicion' and 'belief' are summarised in the *three 'Cs' test*:[2793] a) 'was the information predicting the commission of an offence compelling'?[2794] b) 'where the information was based on a tip-off originating from a source outside the LEAS, was the source credible'?[2795] and c) 'was the information corroborated by' LEAs before deciding whether to breach any of the rights?[2796] However, should there be any deficiency in one aspect of this hypothesis, the fulfilment of the aspect of the hypothesis, may, 'to some extent', be done by ensuring compliance with the other two aspects.[2797]

6.4.2.3 Preference for the conduct of online criminal investigation of serious offences at national security risk levels

Having made a distinction in the reasonable ground standards between suspicion and belief,[2798] both of which are fluid in nature,[2799] the emphasis is placed on the hierarchical conduct of an OCI at the lowest levels of standard of proof to conduct an OCI at the '*severe*', '*high*' and '*medium*' national risk levels in crime commission. Although the effects of the commission of a crime at these national risk levels may not necessarily have to be irreversible, however, the 'irreversibility' of the commission of an offence is the most reasonable, rational, preferred and justifiable criterion to be considered in justifying the conduct of an OCI at the above three risk levels amongst the six classes and stages of serious offence commission.[2800]

Essentially, the greater emphasis of investigation is placed at the national risks levels which occur at the first, second and third classes and stages of crime commission[2801] where an offence *'will probably be committed'*[2802] without undermining the significance of the commission of serious offences at the other classes and stages against private persons in the RSA. This is

[2793] *R v Debot* supra 215. Hubbard, Brauti and Fenton *Wiretapping* 3-8 and 3-12.
[2794] Hubbard, Brauti and Fenton *Wiretapping* 3-8.
[2795] Hubbard, Brauti and Fenton *Wiretapping* 3-8.
[2796] *R v Caissey* [2008] 3 S.C.R 451, 299, D.L.R (4th) 432, affg. 227 C.C.C (3d) 322, 299 D.L.R (4th) 432 at 433 (Alta C.A.), *R v Hillgardener* (2010)252 C.C.C. (3d) 486, 483 W.A.C 200 (Alta.C.A.); Hubbard, Brauti and Fenton *Wiretapping* 3-8 and 3-10 to 3-11; *R v Debot* 215.
[2797] *R v Debot* supra 215; *R v Burke* (2011) 275 C.C.C (3d) 90, 965 A. P R 255 (N.B.C.A) at paras 18-19, Hubbard, Brauti and Fenton *Wiretapping* 3-8.
[2798] Para 6.4.2.2 of this chapter.
[2799] Hubbard, Brauti and Fenton *Wiretapping* 3-10.2.
[2800] Para 6.3.3.1 of this chapter.
[2801] Paras 6.3.3.1 (a)-(f), 6.4.4, 6.4.5 and 6.4.6 of this chapter.
[2802] Section 16(5)(a)(1) of RICA.

because where there is national security protection; private security is impliedly and simultaneously protected.

It is important to note that it is difficult to simply define with precision the notion of 'state security, public order and national interests'.[2803] The discretionary consideration of how serious an offence is; is in the hands of LEAs whose mandate is to protect 'national security' and who '…must be the sole judges of what national security requires.'[2804] However, Bawa warns that the phrase 'national security' should not be interpreted in a broad way to include 'any state of action' to justify the conduct of an OCI.[2805] The court in *AmaBhugane* held that the State must not, under the guise of protecting national security, undermine or destroy the benefits of democracy by unnecessarily using secret surveillance, rather, a balance be struck between the two divides.[2806]

The Supreme Court Appeal held in *Jwara v State* that the discretion of a LEO to conduct an OCI must be adequate and objective,[2807] while the Constitutional Court posits that LEAs must not exercise this power in bad faith.[2808] Although security strategy or risk assessment may be politicised[2809] and LEAs have wide discretion[2810] as the representatives of the executive authority to justifiably classify an offence at the '*severe* national security risk' class, level and standard; if classifying such an offence at other standards, such as '*high*' or '*medium*' security risk standards would be too risky to avert the commission or the effect of the commission of an offence in such category.

However, after the 9-11 terrorist attacks, the courts in the U.S. have now become 'extremely submissive to executive authority 'in the name of security'[2811] which takes away the objectivity

[2803] Van der Vyver *State secrecy* 53.
[2804] Mathews *State secrecy* 40.
[2805] Bawa *ROICA* 320.
[2806] *AmaBhungane v Minister of Justice* supra 102.
[2807] *Jwara v State* supra 11.
[2808] *Kaunda v President* supra 80.
[2809] Tang S 'A Systemic theory of the security environment' (2004) Vol. 27 *The Journal of Strategic Studies* 1-7 and 15. The politicisation of this discretion in the U.S.A made the Congress to enact the Foreign Intelligence Surveillance Act of 1978 to prevent the abuse of the enforcement of the concept of national security which was unjustifiably used, see Swire and Ahmad (eds.) *Introduction* 7-8.
[2810] American Bar Association 'Standards on Prosecutorial Investigations' paras 2.1 (a) and (c)(ii) and (iii) https://www.americanbar.org/publications/criminal_justice_section_archive/crimjust_standards_pinvestigate.html (Date of use:12 July 2017).
[2811] Greenwald G 'U.S. Filmmaker repeatedly detained at border' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 185 (Greenwald *U.S. Filmmaker repeatedly detained at border*)

of the court. It is noted that LEAs must not claim to be protecting the public criminal interests of the country by intercepting the online communication of investigative journalists; whereas, 'historically and institutionally', the interception is usually meant to protect the powers that be: the king or the 'semi-democratic substitute'.[2812]

In the RSA, for example, the structure of SABC management has been used to intimidate or tap personal online communication of journalists who work at the media house which is declared and disguised as a national key point or owned by the government to suppress the editorial views of the broadcaster.[2813] The High Court expresses its view in *AmaBhugane* where it held that bulk interception cannot be used to vet people as a substitute for security clearance.[2814]

LEAs may exercise their discretion and be compelled to conduct an OCI at the first class and stage or '*severe*' risk level,[2815] where, in accessing and determining the seriousness of an offence at the '*severe*' risk level,[2816] it may suffice to consider one outstanding element or aspect of risk in either '*high*' or '*medium*' security risk levels or in the other classes, levels and

[2812] Right2Know 'Spooked- Surveillance of Journalists in SA' at 7 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use:27 November, 2018 (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use:27 November 2018); Maphanga C 'Police documents were classified to hinder intelligence investigations, Zondo commission hears' https://www.news24.com/SouthAfrica/News/police-documents-were-classified-to-hinder-intelligence-investigations-zondo-commission-hears-20190917 (Date of use:18 September 2019).

[2813] Right2Know 36–37 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[2814] *AmaBhungane v Minister of Justice* supra 151, 154 and 155.

[2815] Para 6.3.3.1 of this chapter.

[2816] American Bar Association 'Standards on Prosecutorial Investigations' paras 2.1 (a) and (c)(ii) and (iii) https://www.americanbar.org/publications/criminal_justice_section_archive/crimjust_standards_pinvestigate.html (Date of use:12 July 2017).

stages where, for example, an offence is not statutorily, and adequately categorised —such as the most serious offence[2817] of terrorism[2818] caused by armed drones.[2819]

In this circumstance, it is arguably reasonable, rational and justifiable to conduct an OCI at the first class and stage or '*severe*' risk level even though the full elements of the risks at the first class and stage or '*severe*' level are not present to complete the commission of a serious offence by a person or group of persons at the first class and stage of crime commission or '*severe*' risk level to trigger off the conduct of an OCI at the first class and stage or '*severe*' risk level.

The occurrence of the most serious offence of terrorism caused by armed drones[2820] is a strong security signal or indication that *en masse* or *non-en masse* insurrection or disorder by an individual or the public may spontaneously or later erupt if not nipped in the bud,[2821] otherwise,

---

[2817] See sub-para (d) of para 6.3.2.2 of Chapter 6 of this study.

[2818] According to the various criteria in the statutes in the RSA, this study classifies terrorism as a most serious offence. Terrorism offences are found in sections 2, 3(2)(a), 4, (1), 5, 6, 7, 8, 9, 10 and 14 of the Protection of Constitutional Democracy against Terrorist and Related Activities No. 33 of 2004. It is noted that ss 2 and 3 broadly cover the offence of terrorism and related offence. The effect of the commission of the first category of terrorism on victims is broad, grievous and more serious in its contents, going through sections 2, 3(2)(a), 4, (1), 5, 6,7, 8, 9, 10 and 14 of the Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004. Essentially, this category classifies terrorism as one of the most serious offences as prescribed in Schedule 6 of the CPA. The effects of the commission of these offences on victims are more grievous than the second circumstance, which is narrow and less serious in its contents. The second circumstance classifies terrorism as more serious offence in Schedule 5 of the CPA, which relates to sections 4(2) or 3, 13 and 14 of the Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004. However, there is one similarity between these two circumstances in s 14 of Act 33 of 2004. Under this section, both circumstances acknowledge the offence of threat, attempt, conspiracy and inducing another person to commit offence, thus the bailing authority should relate section 14 to other relevant offences which then determine whether bail should be granted under Schedule 5 or 6 of the CPA. Section 60(11)(a) of the CPA. Sections 2, 3(2)(a), 4, (1), 5, 6,7, 8, 9, 10 and 14 of the Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004.

[2819] Agwu F A *Armed drones and globalisation in asymmetric war on terror- Challenges for the law of armed conflict and global political economy* (2018) i and xi-xv (Agwu *Armed drones and globalisation in asymmetric war on terror*); Di Nucci E and De Sio F S (eds.) *Drones and responsibility- Legal, philosophical and socio-technical perspectives on remotely controlled weapons* (2016) i and ix (Di Nucci and De Sio (eds.) *Drones and responsibility- Remotely controlled weapons* (2016).

[2820] Phakgadi P 'KZN premier Mchunu has 21 days to study the Moerane report on political killings' http://ewn.co.za/2018/06/13/kzn-premier-mchunu-has-21-days-to-study-moerane-report-on-political-killings (Date of use: 10 July 2018). In the U.S., the alleged cyberwar by Russia and China against the critical national infrastructure of the U.S for the former's political and economic gains prompted the U.S. to embark on a special cyberwar project to protect its cyberspace, Cornwell R 'US declares cyber war on China: Chinese military hackers charged with trying to steal secrets from companies including nuclear energy firm' https://www.independent.co.uk/life-style/gadgets-and-tech/us-charges-chinese-military-hackers-with-cyber-espionage-bid-to-gain-advantage-in-nuclear-power-9397661.html (Date of use:12 December 2018); Yi S 'Talk of US cyber war on China ridiculous' available at http://www.globaltimes.cn/content/1107699.shtml (Date of use: 12 December 2018); Goud N 'Did United States declare a Cyber War on Russia?' https://www.cybersecurity-insiders.com/did-united-states-declare-a-cyber-war-on-russia/ (Date of use: 12 December 2018).

[2821] For example, the 2016/2017 '#feesmustfall' national mass campaign by students which simultaneously occurred in almost all the universities and some high schools in the RSA may fit into this illustration.

the commission of terrorism caused by armed drones may result in intended, unintended, and uncontrollable actions, omissions, and consequences respectively in the State.

For example, on the one hand, the 2011 Arab spring leaves devastating and irreversible effects in that part of the world especially in Syria,[2822] more particularly where, for instance, there is an action or omission by perpetrators, constituting a '*severe* national security risk' or '*severe*' magnitude attack on the 'critical infrastructure database'[2823] or non-database infrastructure, facility or national key point.

On the other hand, one of the consequences of compelling the conduct of an OCI at the first class and stage of crime commission or '*severe*' risk level is the consideration of the likelihood of declaration of a state of emergency to avert the occurrence of '*severe* national security risk' in the RSA. However, this consideration is, in most cases, not usually resorted to in a normal democratic system such as the RSA.[2824] This is because meeting the requirements for the declaration of a state of emergency is Herculean despite that —drawing on foreign jurisprudence— the courts have become 'extremely submissive to the executive authority 'in the name of security' to grant unreasonable request.[2825] It is a Herculean effort to prove the

[2822] Cornell University Library 'Arab spring: A research & study guide' https://guides.library.cornell.edu/arab_spring/Syria accessed (Date of use: 20 December 2018) (Cornell University Library https://guides.library.cornell.edu/arab_spring/Syria (Date of use: 20 December 2018).

[2823] Para 3.4.5.3 of Chapter 3 of this study; See Chapter 11 of the CCB -B6-2017, more particularly sections 57(2), (3), (4), (5), (6) and (12)(a).

[2824] Section 203 of the Constitution; State of emergency 'is the last measure that government adopts to restore order in times of war, general insurrection and disorder', State of emergency 'is the last measure that government adopts to restore order in times of war, general insurrection and disorder', Mabuza https://www.timeslive.co.za/news/south-africa/2017-12-12-explainer--what-the-law-says-about-declaring-a-state-of-emergency/ (Date of use:12 March 2018); Staff Writer 'The 30 worst areas in South Africa for crime in 2017' https://businesstech.co.za/news/lifestyle/207191/the-30-worst-areas-in-south-africa-for-crime-in-2017/ (Date of use: 12 March 2018) (Staff Writer https://businesstech.co.za/news/lifestyle/207191/the-30-worst-areas-in-south-africa-for-crime-in-2017/ (Date of use:12 March 2018); Staff Writer 'The 30 worst areas in South Africa for crime in 2017' https://businesstech.co.za/news/lifestyle/207191/the-30-worst-areas-in-south-africa-for-crime-in-2017/ (Date of use:12 March 2018) (Staff Writer https://businesstech.co.za/news/lifestyle/207191/the-30-worst-areas-in-south-africa-for-crime-in-2017/ (Date of use:12 March 2018); Bawa *ROICA* 297 where Bawa states that interception is meant for crime investigation and intelligence gathering; Rose M and Baker L 'Can France's leader-less 'yellow vests' become a true political force?' https://globalnews.ca/news/4743632/yellow-vest-political-movement-france/(Date of use: 9 December 2018); Landau Lawful electronic surveillance in the face of new technologies 223; Snyder T 'America lost a cyberwar to Russia in 2016. When will we have truth?' https://www.theguardian.com/commentisfree/2018/feb/12/america-cyberwar-russia-2016-memo-truth (Date of use: 12 December 2018).

[2825] Greenwald *U.S. Filmmaker repeatedly detained at border* 185. It is submitted that it is controversial and remains to be seen whether the courts would submit to the threat by President Trump of the U.S. to declare a state of emergency on ground of the so called 'economic caravan invasion' of the border between the U.S. and Mexico, see Associated Press 'Trump threatens emergency declaration ahead of US-Mexico border visit'

elements of a state of emergency because the proof is almost comparable to the task of attempting to take a camel through the eye of a needle.

Instead of embarking on the path of state of emergency declaration, what is more reasonable, rational and justifiable to do is to conduct an OCI at the first class and stage or '*severe*' risk level without necessarily envisaging a declaration of a state of emergency in mind, given that other classes or instances exist in the first class and stage, which though are not as serious as a state of emergency instance, but yet, they cannot be classified under the second class of offences because the risk is still '*severe*'.

The state of emergency declaration may require the temporary and qualified suspension of the enforcement of some provisions of the Constitution, legislation and other law. For example, the suspension of section 14 of the Constitution may include partial compliance or proportionate non-compliance with the provisions of RICA when conducting a general or mass OCI.[2826]

At the first stage of crime commission or '*severe*' risk level, an OCI is sparingly conducted in the society because the evidence may generally not be reasonably sufficient to justify the extreme intrusion into the innermost sanctum of the right to the SOC at this stage,[2827] but a LEO may still proceed to conduct an OCI for the foregoing reasons. This is because the facts required to conduct an OCI are at the minimal or almost at the *zero* proximate points of the facts required to commit such an offence.

Essentially, it is argued that although the standard of proof to conduct an OCI at the first class and stage of crime commission or '*severe*' risk level is very low, or better still, is the lowest, yet it is the most difficult standard to proof because of the far-reaching legal requirements and non-legal intended and unintended actions, omissions and consequences by and in the State and to the individuals who are targets of the conduct of an OCI at the first stage or '*severe*' risk level.

---

https://www.news24.com/World/News/trump-threatens-emergency-declaration-ahead-of-us-mexico-border-visit-20190110 (Date of use:11 Januarry, 2019 (Associated Press https://www.news24.com/World/News/trump-threatens-emergency-declaration-ahead-of-us-mexico-border-visit-20190110 (Date of use:11 Januarry 2019).

[2826] Para 6.13 of this chapter.

[2827] Para 3.4.5 and 3.8 of Chapter 3 of this study.

It is important to note that, generally, where an offence, which falls under the first class and stage offence or '*severe*' risk level —for example— is not detected at that stage to trigger an OCI but it is only detected at a later stage —at the sixth class and stage, for example;[2828] the conduct of an OCI of such first-class and stage offence or '*severe*' risk level is not invalid if the offence is conducted at stage six or at any of the stages below stage six. This is because the principle of proportionality would have been applied in this regard.

Similarly, it is noted that given the 'ascending serious offence' theory propounded in this study,[2829] the other classes and stages of serious offences can be conducted at the first class and stage or at the other classes or stages of the six classes or stages of serious offences in pursuance of the application of the proportionality principle.

In summary, it is argued that it is high time the society regarded the role of LEOs as that of ministers in the temple of justice —as lawyers and judges are— by ensuring that the powers vested in them to conduct an OCI at the national security risk levels are not abused. This is because one day, that particular LEO who abuses his or her powers will disengage from active service of the security agencies and be a victim of the abuse by his or her former colleagues, thus, he or she that lives in a glass house should not throw stones.

6.4.3 Opportunistic online access and convertible intrusive standard of proof principle

In curing the defects in the loss of opportunity to conduct early detection of the commission of a first-class and stage crime[2830] and in curing the defects in the practically difficult and blurred proof or implementation of the forms of suspicious and belief standards of proof in the mathematical and non-mathematical standards of proof to conduct an OCI,[2831] this rubric attempts to strike a balance in the conflict between the various forms of suspicious standards and the only form of belief standard in the hierarchy of standards of proof required in the conduct of an OCI below.[2832]

[2828] Para 6.3.3.1 of this chapter.
[2829] Para 6.3.2 of this chapter.
[2830] See the closing paragraph of para 6.4.2.3 of this chapter.
[2831] Paras 6.3.3.1, 6.4.1, 6.4.2.1–6.4.2.3, 6.4.3, 6.4.4.1–6.4.4.3, 6.45, 6.4.6.1, 6.4.6.2, 6.4.7.1, 6.4.7.2 and 6.4.8 of this chapter.
[2832] Paras 6.4.2 and 6.4.4 - 6.6.8 of this chapter.

This attempt seeks to ultimately strike a balance in the conflict between the protection of the sanctum of the right to the SOC[2833] and the conduct of an OCI so that a LEO is not seen as attempting to embark on a 'fishing expedition' where there is no need to do so, thus, this conflict is managed by the conceptualisation of the principle of 'opportunistic online access and convertible intrusive standard of proof'.

The application of this principle is fundamentally anchored on the presumption that there is a practically difficult and blurred proof of the various forms of standards or proof in the conduct of an OCI where facts are discovered or gathered by LEAs in quick succession or jet pace and an unpredictable fashion in the commission of a serious offence. More importantly, these succession and unpredictability make it generally difficult for LEAs to, at a glance, place the facts in a particular standard of proof in contemplation of making an application before the court until such a time that LEAs trigger a reaction or an *offline* investigation or until such a time where the facts are equally sufficient enough for the court to grant an opportunity to LEAs to access court to conduct an OCI on any of the standards of proof.

This process is the first aspect of this principle which is referred to as the 'opportunistic online access' to court because a LEO is granted an opportunity to be heard by a court at any of the classes and stages of serious crime commission, while the court ultimately converts this access into a proportionate intrusion of the reasonable continuum of the right to the SOC relevant to the serious offence being initially investigated titled 'convertible intrusive standard of proof' which is the other aspects of the principle. In sum, the two steps of being granted access to court and the consequential access to online communication are termed the 'opportunistic online access and convertible intrusive standard of proof' principle.

The facts gathered enable the court to grant an opportunity to a LEO for example, at the '*reasonable suspicious higher ground*' standard or at the *fifth* class and stage of serious crime commission which eventually entitles the court to grant an OCI access direction at the proportionate complex sanctum in the right to the SOC equivalent to the relevant *fifth* class serious offence *initially being investigated*. However, such an OCI access direction is converted to an OCI *destination* direction at the proportionate complex sanctum in the right to

[2833] Para 3.8 of Chapter 3 of this study.

the SOC equivalent to, for example, *first* stage and class serious offence that was *initially being investigated* in pursuance of the facts gathered at the *first* class and stage of crime commission *but which was not detected early* or *may be difficult to comprehensively prove at the early stages of detection* before an OCI application is submitted to the court.

It is noted that this principle is applicable in the manner expressed herein and not the other way round because, by default, any *first*-class serious offence that is investigated will enable the court grant access to the sanctum of the right to the SOC at any level in the sanctum which includes offences in the second to *sixth* classes of serious offences.

This illustration simply means that a more serious offence can be investigated if the facts of such a serious offence exist *ab initio* in the *offline world* which is *bona fide* presented in the OCI application, given that a LEO is given the opportunity to access the court for the conduct of an OCI of a general serious offence. Where false information is supplied which is punishable as a serious offence on its anyway,[2834] the evidence obtained therefrom in an OCI in the principle of 'opportunistic online access and convertible intrusive standard of proof' becomes a piece of void evidence, consequently inadmissible.[2835]

The principle of 'opportunistic online access and convertible intrusive standard of proof' is one of the exceptions in an OCI application where a LEA cannot enjoy the benefits of the principle of *windfall* evidence obtained in an OCI regarding the offences which were not the highlights of the initial conduct of an OCI.

The principle of 'opportunistic online access and convertible intrusive standard of proof' seems to be the most appropriate way to practically interpret, simplify and actualise the six mathematical and non-mathematical standards of proof of investigation at the earlier and earliest classes and stages crime commission as demonstrated above and below.[2836]

[2834] Paras 3.10.19 and 7.8.5.4 of this study.
[2835] Para 7.8.5.4 of Chapter 7 of this study.
[2836] Para 6.4.5–6.4.8 of this chapter.

6.4.4 Applying Popoola mathematical and non-mathematical formulae to determine the general standard of proof in online criminal investigation

6.4.4.1 Introduction

Given the uncertain and fluid nature of human mind —including LEOs, courts and other stakeholders— in the determination of the relevant reasonable ground standards[2837] in the conduct of an OCI, this study applies some dynamic and progressive standards[2838] by attempting to indispensably propose some logical,[2839] mathematical and non-mathematical formulae or guidelines. This proposal is made in attempting to accurately and reasonably determine the various reasonable ground standards in the minds of stakeholders when conducting an OCI at the necessary classes and stages of complete and attempted crime commission.

This proposal also lays the foundation for the practical appreciation, understanding, configuration and preparation by LEOs, computer programmers and other stakeholders respectively in the emerging use, development and deployment of AI applications in determining the various standards of proof required to conduct an OCI.

6.4.4.2 Significance of applying mathematical formulae in resolving legal problems

Judicial and quasi-judicial rationality,[2840] legal reasoning and administrative decisions by courts, LEAs and other stakeholders respectively cannot be made in the conduct of an OCI without the application of logic, which is a subset of mathematics. Galileo says that mathematics defines life '…without which means that it is humanly impossible to comprehend a single word. Without these, one is wandering about in a labyrinth'.[2841] In other words, while

[2837] Hubbard, Brauti and Fenton *Wiretapping* 3-10.2 and 3-13.
[2838] Hubbard, Brauti and Fenton *Wiretapping* 3-10.2 and 3-12.
[2839] Rule of logic was displayed by the Constitutional Court in *Kaunda v President* supra 101 and 139.
[2840] *Kaunda v President* supra 79 and 80.
[2841] Adem D T *Legislative drafting: Mathematics & other devices* (2013) 57 and 59 (Adem *Legislative drafting: Mathematics & other devices*); Wikipedia 'Portal Mathematics' http://en.wikipedia.org/wiki/portal:mathematics (Date of use:18 December 2017).

mathematics is a tool with which the foundation of life is navigated,[2842] jurisprudence, which is the overall foundation of life, cannot function without the application of mathematics. Mathematics is a science, which expresses the relationship between quantities and magnitudes, which are represented by numbers or symbols.[2843] Arguably, the quantities constitute the facts expected to be gathered from the commission of an offence, which triggers the conduct of an OCI, while the magnitude constitutes the seriousness of the commission of an offence.

Historically, mathematics was mostly used for purposes of trading, land measurement, recording of time, et cetera.[2844] In contemporary society, mathematics has broadly been extended to other areas of knowledge to investigate problems which fall outside pure mathematics, thus establishes the concept of applied mathematics,[2845] from which this study conceptualises mathematical formulae to determine the standards of proof to conduct an OCI in the field of law, amongst other fields.

The fields in which mathematics has been expanded include '…cybernetics, cryptography, financial mathematics…mathematical biology, the mathematics of engineering, mathematics in medicine, mathematical chemistry, mathematical physics…, operations research, probability and statistics.[2846] To demonstrate the use of financial mathematics, section 223(1) of the Tax Administration Act of South Africa contains tables with percentages on the Understatement Penalty Percentage.[2847] More specifically, drawing on the Seventh Schedule of the Ugandan Constitution, some mathematical formulae are provided on revenue sharing between the local and national governments on decentralised services in Uganda.[2848]

Therefore, in a similar vein, if a provision is propounded in a 'clear, unambiguous, precise, concise and intelligible manner' or language, it will stand 'the test of time'.[2849] Mathematics,

---

[2842] Wikipedia http://en.wikipedia.org/wiki/portal:mathematics (Date of use: 18 December 2017; Adem *Legislative drafting: Mathematics & other devices* 57 and 59.

[2843] *The new international Webster's pocket dictionary of the English language* (new rev ed.) (United States of America: Trident Press International, 1998) at 616; Adem *Legislative drafting: Mathematics & other devices* 55.

[2844] Adem *Legislative drafting: Mathematics & other devices* 56.

[2845] Adem *Legislative drafting: Mathematics & other devices* 56.

[2846] Adem *Legislative drafting: Mathematics & other devices* 56.

[2847] Tax Administration Act 28 of 2011.

[2848] Adem *Legislative drafting: Mathematics & other devices* 66.

[2849] Adem *Legislative drafting: Mathematics & other devices* 59-60; Dauda M *Plain language in drafting legislation in Nigeria*: *The Possible Benefits* (LL.M dissertation 2016) 6-7 http: //ft.lk/2011/10/08/mathematical-language-can-language-legal-drafting-icta-chairman-prof-espasinghe (Date of use: 3 June 2018).

which is the mother of logic, upon which legal argument is based, can be used to define or represent law, 'leverage legislative drafting' provisions[2850] and resolve legal abstracts in 'a series of letters, numbers or symbols that represent a rule or law'.[2851]

6.4.4.3 Jurisprudence of the application of mathematical formulae in resolving legal problems in South Africa

The Constitutional Court in *Investigating Directorate v Hyundai and Smit No*[2852] and *Thint*[2853] held that there is a need to conduct an earlier investigation into the commission of certain offences that are more serious than the others.[2854] However, there are no specific, determinable and adequate guiding principles and functional legal frameworks or logical or mathematical formulae that examine or simplify the 'seriousness, class and stages of crime commission proportionality' principle in South Africa.[2855]

This principle relates to the reasonable ground standards required to conduct an OCI according to the seriousness or class of an offence and the appropriate timing of the investigation based on the effect or the degree of the seriousness of the crime committed. In addition, this inadequate legal framework is exacerbated by the fact that LEOs are not required by law to have special knowledge or skill to conduct an OCI.[2856] These inadequacies negative the protection of the right to the SOC because LEOs will inadvertently take steps contrary to the protection of this right due to lack of knowledge or ignorance.[2857]

This lacuna, *ab initio*, results in some confusion, uncertainty or ambiguity in the minds or mental imageries of LEOs and other stakeholders when considering the proportionate determination of the standards of proof required not only at the stages of crime commission but also at the various degrees of serious offences.

[2850] Adem *Legislative drafting: Mathematics & other devices* 56 - 57 and 59.
[2851] Adem *Legislative drafting: Mathematics & other devices* 57.
[2852] *Investigating Directorate v Hyundai and Smit No* supra 1, 2, 4, 6, 7, 8, 13, 14, 27, 28, 30, 31, 33, 34, 44, 45, 46, 47, 48, 51 and 52.
[2853] *Thint* supra 80, 127, 153, 168, 247, 252 and 257. See also *Estate Board v Auction Alliance* supra 63 where the Constitutional Court states that the legislature should be given the 'latitude to formulate the inner and outer reaches of the search power'.
[2854] *Investigating Directorate v Hyundai and Smit No* supra 1, 2, 4, 6, 7, 8, 13, 14, 27, 28, 30, 31, 33, 34, 44, 45, 46, 47, 48, 51 and 52.
[2855] See Chapter Five (para 5.4.4) of the attached Table of Content of this study.
[2856] Paras 4.3 and 4.6 of Chapter 4 of this study.
[2857] Hosea 4: 6 in the Holy Bible.

The reasons for the non-pronouncement or recognition of mathematical formulae by the Constitutional Court are neither due to any illegality, unlawfulness or invalidity of the application of mathematical formulae in the decision-making process of the court nor are they due to any scientific proof or evidence-based principle to reject the merit in the application of mathematical formulae in resolving legal issues.

However, according to the candid, magnanimous and progressive admission of the High Court in *Intercape v Pro-Haul*, it states that the non-pronouncement or non-recognition of the mathematical formulae by the courts is not due to any other reason but is due to the non-existing valid reasons of the courts to reject the application of the formulae.[2858] Essentially, the courts are merely reluctant or do not have any appetite to subscribe to the application of mathematical formulae.[2859] This reluctance defies logic, a segment of mathematics, the very foundation upon which legal problems are resolved.

To further corroborate the reluctance of the courts in the same case, the High Court innocently expresses its candid, unscientific and unequivocal view by stating that the courts believe that mathematical formulae are nothing but the usurpation of the inherent function of the court.[2860] This is because the consideration or application of mathematical formulae prevents the court from applying its mind in the adjudication of cases that require usual daily or ordinary mental effort to resolve.[2861]

Nevertheless, further to the acknowledgement by the court of the functional use of mathematical formulae in adjudicating legal problems in court, the judge humbly conceded that he lacked the proficiency to apply mathematical formulae in *Foodcorp v Deputy Director-General*.[2862] In his words, he states that utmost judicial respect be conferred on policy-burdened and multi-dimensional administrative acts that require expert knowledge in the field of mathematics which most judges do not possess if any possess at all.[2863] He unequivocally admits to the truism that he is bereaved of the treasure of having an aptitude in developing and

[2858] *Intercape v Pro-Haul* supra 15.
[2859] *Intercape v Pro-Haul supra* 15.
[2860] *Intercape v Pro-Haul supra* 15.
[2861] *Intercape v Pro-Haul supra* 15.
[2862] Emphasis mine. *Foodcorp (Pty) Ltd v The Deputy Director-General - Department of Environmental Affairs and Tourism: Branch Marine and Coastal Management and Others* Case No: 3519/02 para 68 (*Foodcorp v Deputy Director- General*); *NJJ Webb v Road Accident Fund* Case No: 2203/14 para 35 (*NJJ Webb v RAF*).
[2863] Emphasis mine. *Foodcorp v Deputy Director- General* supra 68; *NJJ Webb v RAF* 14 supra 35.

applying such a complex world, processes or systems of mathematical knowledge in adjudicating legal decisions.[2864]

In the same *Foodcorp v Deputy Director-General*, the High Court expressed some optimism in adopting some combined mathematical formulae in resolving a legal problem.[2865] The court states that it is usual, reasonable and non-arbitrary for a court to intensely comprehend the recommendation of experts and apply their mind when adopting the same in their decision.[2866] The court goes further by saying that it is, at all times, in good faith and ultimately, bound to consider in its proceedings, amongst other options, 'complex mathematical formulae' placed before it in arriving at an informed decision.[2867]

The U.S. jurisprudence is not left out in contributing to the debate on the application of mathematical formulae to resolve legal problems by lawyers. However, although the U.S. jurisprudence in this regard focuses on lawyers, nevertheless, invaluable lessons can be learnt in building up the rationale for the understanding of mathematical formulae by LEOs (who though are the main case study in this study), the courts, executing authorities and other stakeholders who are respectively involved in the conduct and oversight of an OCI. In the words of Oliver Wendell Holmes Jnr., he states that lawyers cannot be trained in law without being trained in logic, thus logic is *sine qua non* for legal training[2868] and logic is impeccably a segment of mathematics. The training programme requires lawyers to be comfortably and competently analytical, discerning and inferential.[2869]

Primarily, logic is the language and tool with which judicial decisions are taken, even though with some reasonable and justifiable uncertainty or inexact logical conclusion, because every conclusion has a logic and 'relative worth' behind it, the reasoning of which may be based on a communal or class attitude, belief, interest, opinion, policy, practice, and qualitative assessment.[2870]

[2864] Emphasis mine. *Foodcorp v Deputy Director- General* supra 68; *NJJ Webb v RAF* supra 35.
[2865] *Foodcorp v Deputy Director- General* supra 67 and 68; *NJJ Webb v RAF* supra 35.
[2866] Italics mine. *Foodcorp v Deputy Director- General* supra 67; *NJJ Webb v RAF* supra 35.
[2867] Italics mine. *Foodcorp v Deputy Director- General* supra 67; *NJJ Webb v RAF* supra 35.
[2868] Holmes O W Jnr 'The Path of Law'1897 10 *Harvard Law Review* 457; Hutchinson T 'Doctrinal research' in Watkins D and Burton M (eds.) *Research Methods in Law* (2018) 8 (Hutchinson *Doctrinal research*).
[2869] Holmes *Harvard Law Review* 10, 1897, 457; Hutchinson *Doctrinal research* 8.
[2870] Holmes *Harvard Law Review* 10, 1897, 457; Hutchinson *Doctrinal research* 8.

Ultimately, a lawyer who is knowledgeable and intelligent in complex models will be more effective in resolving issues than a lawyer without knowledge and intelligence, who is absolutely and always at the mercy of consultants for instructions on the next question.[2871] Furthermore, it is observed that the necessity to get acquainted with mathematical ideas does not only lie in scholars, lawyers and judges, but with legislators[2872] in understanding the basics of mathematical formulae in this study.

In addition, the indispensable requirement of the knowledge of logic as a subset of mathematics by LEOs in the conduct of an OCI lays a foundation for or reiterates the understanding, appreciation, preparation and development of the minds of LEOs and other stakeholders including, more importantly, algorithm programmers, in the respective use, practice, configuration, application or deployment of AI —which is not only steering us in the face but piercing it— in the conduct of an OCI.[2873] The development and deployment of logical or mathematical formulae expressed in AI to conduct an OCI is the simplification or oversimplification of human operations[2874] which require less human effort or does not involve a human effort to decide the standard of proof required to conduct an OCI of various serious offences.

In highlighting the significance of mathematical formulae in resolving legal issues, a part of the pronouncement of the High Court in *Foodcorp v Deputy Director-General*[2875] was corroborated by the Supreme Court of Appeal in *State v Mavinini*. Cameron JA in *State v Mavinini* highlights the significant function of the application of mathematics in the decision-making process of the court —in a different subject-matter— by articulating the relationship between the 'proof beyond reasonable doubt' and 'legal guilt'; however, no mathematical formulae were proposed by the court.[2876]

Furthermore, although the Supreme Court of Appeal in *Bane v D'Ambrosi* emphasises the importance of applying the 'mathematically-based route' before embarking on 'the less

[2871] Finkelstein and Levin *Statistics for Lawyers* x.
[2872] Finkelstein and Levin *Statistics for Lawyers* x.
[2873] Para 6.4.9 of this chapter.
[2874] Finkelstein and Levin *Statistics for lawyers* xi.
[2875] Italics mine. *Foodcorp v Deputy Director- General* supra 67; *NJJ Webb v RAF* supra 35.
[2876] *State v Mavinini* 2009 (1) SACR 523 (SCA) 26; Schwikkard P J and Van der Merwe S E 'The standard and burden of proof and evidential duties in criminal trials' in *Principles of evidenc*e (2017) 614 (Schwikkard and Van der Merwe *The standard and burden of proof*).

desirable alternative' in the decision making process of the court; nevertheless, no mathematical formulae were also pronounced by the court.[2877] Also, despite the significance of the use of 'data mining' in the U.S. jurisprudence, whereby mathematical formulae are employed to predict the patterns and future behaviour based on stored data,[2878] nonetheless, no mathematical formulae were conceptualised, defined nor published in this regard. Thus, the ignorance of the importance of the use of mathematics in resolving problems, including legal issues, knows no bound.

The proposition of the standard of proof propounded in this study goes beyond the mere identification by the Constitutional Court —without more— of the need to conduct an early investigation of some serious offences.[2879]

The proposition in this study suggests some perceptions that stir the comfort of the common convention of 'venerable legal institutions'.[2880] The proposal attempts to influence the current legal pattern of legal reasoning with a promise to demonstrate the use of some quantitative or numerative reasoning methods, which are not meant to make LEAs become mathematicians.[2881] However, the proposal is meant to create an imaginary assumption in the minds of LEOs and others alike on the standard of proof required to conduct an OCI in the RSA.

In emphasising the need to create an awareness in the minds of stakeholders on the understanding and application of mathematical formulae in conducting an OCI, the Supreme Court of Appeal held that the application of a mathematical formula gives 'an informed guess' in resolving legal issues rather than the non-application of mathematical formulae.[2882] In the human mind, although the non-application of mathematical formulae is believed to be 'fair and reasonable', but in reality, it results in a 'blind guess'[2883] which is detrimental to the criminal justice system that should take advantage of the accurate or near accurate and more scientific procedure by applying mathematics in contemporary society.

[2877] Italics mine. *Bane and Others v D'Ambrosi* (279/08) 2009 (ZASCA) 98 (*Bane v D'Ambrosi*)
[2878] The Economist *Learning to live with big brother* 26.
[2879] *Investigating Directorate v Hyundai and Smit No* supra 1, 2, 4, 6, 7, 8, 13, 14, 27, 28, 30, 31, 33, 34, 44, 45, 46, 47, 48, 51 and 52.
[2880] Finkelstein and Levin *Statistics for lawyers* viii.
[2881] Finkelstein and Levin *Statistics for lawyers* viii, ix and x.
[2882] Italics mine. *Singh v Ebrahim* (413/09) [2010]ZASCA 145 at152 (*Singh v Ebrahim*).
[2883] Italics mine. *Singh v Ebrahim* supra 52.

The mathematical proposition —which is a specific, simple and an application-friendly alternate logical proposition— assists in influencing the accurate gathering of facts by LEOs, in discerning facts before the court and in influencing the perceptions of other stakeholders in this regard.[2884] Beyond that, a good knowledge or insight of the mathematical formulae contributes to the rationale, civilised and robust discourse[2885] on the standards of proof required to proportionately conduct an OCI of the commission or attempted commission of the six categories, classes or stages of serious offences identified in this study. It is believed that these formulae are adequate to influence the proportionality principle in the application of the s 36 constitutional limitation clause.

The examination or simplification of six mathematical formulae primarily and secondarily empowers LEOs[2886] and other stakeholders respectively. The examination is to justifiably and reasonably choose the application of the most appropriate standard to strike a balance in the conflict between the protection of the right to the SOC and implementation of the substantive and procedural requirements for the conduct of an OCI at the six classes and stages of complete and inchoate crime commissions.[2887] The implementation of the six mathematical formulae below is simplified by the earlier examination of the principle of 'Opportunistic online access and convertible intrusive standard of proof'.[2888]

Unlike the proposition in this study, there are no same or similar mathematical formulae existing in the UK, U.S. or Canada[2889] as the leading countries in the development of the standard of proof required to conduct an offline investigation, let alone such extant formulae to conduct an OCI in the UK, U.S. and Canada, hence the proposal herein.

It is however noted and argued that any form of variation created by proponents in the mathematical formulae between the broad principles of suspicion and belief which *increase* or *decrease* the various standards below has some effect. In effect, there is an inevitable tendency, in practical terms, to *increase* or *decrease* the standards of proof of conducting an OCI to

[2884] Finkelstein and Levin *Statistics for lawyers* x- xi.
[2885] Finkelstein and Levin *Statistics for lawyers* xi.
[2886] *Thint* supra 82; *Bernstein v Bester NO* supra 792; Section 33 of the 1996 Constitution.
[2887] Paras 6.4.5, 6.4.6.1, 6.4.6.2, 6.4.7.1, 6.4.7.2 and 6.4.8 of this chapter.
[2888] Para 6.4.3 of this chapter.
[2889] Hubbard, Brauti and Fenton *Wiretapping* 3 - 4 to 3 - 90.

respectively fallacious, idealistic and unnecessarily onerous or too easy or simple standards that may only satisfy academic gymnastic requirements.

One the one hand, if another proponent mathematically argues that the proof in the suspicious standard be *increased* to the proof in the belief standard while belief standard is further *increased* beyond what is proposed below, it is very likely that the new standard argued by the proponent will be fallacious, idealistic and unnecessarily onerous to fulfil in conducting an OCI. This is because no offence —including the more serious offences that should be investigated earlier as pronounced by the Constitutional Court—[2890] may be investigated through the conduct of an OCI, given that a *higher* standard must be met in each of the standards formulated below.

On the other hand, if another proponent mathematically argues that the proof in the belief standard be *decreased* to the proof in suspicious standard while the suspicious standard is further *decreased* beyond what is proposed below, the new standard will likely be fallacious, idealistic and unnecessarily too easy or simple to fulfil when conducting an OCI. This is because some offences which may not ordinarily be qualified to be earlier investigated via an OCI may now be investigated through the conduct of an OCI, given that a *low* standard is now required to be met in each of the standards formulated below.[2891]

6.4.5 Popoola '*lowest* standard of *merely* reasonable suspicious ground' to investigate an offence posing 'severe national security risk' at the first class and stage of serious crime commission

In the non-mathematical principle, the factual matrix standard required to conduct an OCI of an offence is where the existence of a fact poses a '*severe* national security' risk in the RSA or elsewhere under a relevant international public law obligation which compels a declaration of a 'state of emergence' in the RSA.[2892] The existence of such a fact is investigated at the *first* class and stage where an offence[2893] *'will probably be committed'*[2894] or at the '*merely lowest*

[2890] *Investigating Directorate v Hyundai and Smit No* supra 1, 2, 4, 6, 7, 8, 13, 14, 27, 28, 30, 31, 33, 34, 44, 45, 46, 47, 48, 51 and 52 and *Thint* supra 80, 127, 153, 168, 247, 252 and 257.
[2891] *Investigating Directorate v Hyundai and Smit No* supra 1, 2, 4, 6, 7, 8, 13, 14, 27, 28, 30, 31, 33, 34, 44, 45, 46, 47, 48, 51 and 52 and *Thint* supra 80, 127, 153, 168, 247, 252 and 257.
[2892] Section 16(5)(a)(i) of RICA and paras 6.3.3.1(a), 6.3.3.2(e), 6.3.3.3(e), 6.3.3.4(d) and 6.3.3.5(e) of this chapter.
[2893] Para 6.3.3.1 of this chapter for the six classes of serious offences.
[2894] Section 16(5)(a)(i) of RICA.

reasonable suspicious' standard of crime commission, subject to the principle of the fluidity of determination of a serious offence.[2895]

In the mind of a LEO or any other stakeholder, the mathematical factual matrix standard is determined at the 'minimal or proximate point' standard or at *the estimated value of facts reasonably equal to* (=) *or greater than* (>) *0.1 % but less than* (<) *or equal to* (=) *10 % of facts* required for the commission of an offence at the *first* stage and class, subject to the principle of the fluidity of determination of a serious offence.[2896]

6.4.6 Popoola '*lower* and *low* standards of *merely* reasonable suspicious ground' to investigate offences posing *high* and *medium* risks at the *second* and *third* classes and stages of serious crime commission

Having located the first aspect of where an offence *'will probably be committed'* in the '*severe* national security' risk which requires the '*merely lowest reasonable suspicious'* standard[2897] of proof to conduct an OCI, the *second* and *third* classes and stages occur where the existence of a fact[2898] poses '*high* and *medium* national security risks' in the RSA or elsewhere under a relevant international public law obligation. The existence of such a fact is investigated where an offence '*will probably be committed'*[2899] or is investigated at the '*merely lower* and *low reasonable suspicious*' standards of crime commission, subject to the principle of the fluidity of determination of a serious offence.[2900]

Put differently, the Constitution enables an early investigation to prevent the occurrence[2901] of serious offences that constitute *actual* and *potential threats* to public interests, health or safety

[2895] Para 6.3.2 of this chapter.
[2896] Para 6.3.2 of this chapter.
[2897] Suspicion may arise from acts of commission or omission from conspiracy, incitement or attempt to commit the primary offence, *Investigating Directorate v Hyundai and Smit No* supra 46 and the definition of 'serious offence' in section 1 of RICA.
[2898] Para 6.3.3.1 of this chapter for the six classes of serious offences.
[2899] Section 16(5)(a)(i) of RICA.
[2900] Para 6.3.2 of this chapter.
[2901] Section 205(3) of the Constitution; *Glenister v President of the Republic of South Africa and Others* [2011] ZACC 6; 2011 (3) SA 347 (CC); 2011 (7) BCLR 651 or 176 (CC) (*Glenister II*); *Carmichele v Minister of Safety and Security and Another* [2001] ZACC 22; 2001 (4) SA 938 (CC); 2001 (10) BCLR 995 (CC) at paras 45 and 61; *SAPS v SAHRLC & Ors* supra 50 and 51 and 53. Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 83; Section 16 (5)(a)(ii) of RICA; The UNODC *Comprehensive study on cybercrime* (2013) 223.

and national security[2902] and *actual threat*[2903] to *compelling national economic interests*[2904] because such investigations are urgent and time-critical in these regards.[2905]

In effect, an investigation at the *second* class and stage serves as a preparatory or preliminary investigation which prepares LEOs for the next stage, which is the 'enquiry' and *third* stage in a criminal investigation, which requires a higher standard ground to suspect an individual.[2906]

The reasonable suspicious standard is suitable for the investigation of sensitive, complex, complicated and serious offences, organised crimes and economic crimes in which difficulty is encountered, requiring more efforts in identifying the criminal conduct in the commission of the offence.[2907] It is submitted that although the Constitutional Court used different non-appropriate offences to illustrate the need for an early investigation, however, the principle of fluidity of determination of a serious offence intervenes to resolve this non-appropriation by ensuring that the offences cited by the Constitutional Court are reasonably and differently re-classified for earlier investigation according to the fluidity principle examined in this study.[2908]

[2902] The phrase 'national security' in s 16(5)(a)(ii) and (iii) should not be given an overbroad interpretation to the extent of it being arbitrarily used by LEAs, Bawa *ROICA* 320; *SAPS v SAHRLC & Ors* supra 53 and 57; *Okah v State* (19/2014) [2016] ZASCA 155 (3 October 2016) para 12 (*Okah v State*); Section 16(5)(a)(iii) of RICA; Section 25 of the CPA; *Investigating Directorate v Hyundai and Smit No* supra 46, 48, 53 and 54. See para 7.6.3.3 of this study; Section 37(2) of the POPIA. Section 38(2) of the POPIA defines what is 'relevant function' in section 38(1) of the POPIA.

[2903] The UN states that where there is an 'imminent threat of harm', the urgency requires that extraterritorial data access can be conducted, UNODC *Comprehensive study on cybercrime* (2013) 223. Also, arguably, crimes listed under the jurisdiction of ICC may be grouped under actual and potential threat to the public, see Du Plessis 'International Criminal Courts' 175-189. Where there is actual or potential breach of peace or aggression, it may be regarded as serious offences, Du Plessis 'International Criminal Courts' 191. In *SAPS v SAHRLC & Ors* supra 57, the Constitutional Court held that high priority should be given to international crimes or most serious offences.

[2904] Since the Security Council regards economic sanction or coercion from other states as a serious violation of state sovereignty under the principle of non-intervention, it may threaten the political independence of the RSA, arguably, thus requires OCI, Resolution 2525 (XXV), Paust and Blaustein (1974) 68 *AJIL* 410; United States Comprehensive Anti-Apartheid Act of 1986 (1987) 26 *ILM* 111; 1986 Annual Survey 70, G N Barrie, 'International law and economic coercion- A legal assessment' (1985-1986) 11 *SAYIL* 40, Fergusson-Brown K 'The legality of economic sanctions against South Africa in contemporary international law' (1988-9) 14 *SAYIL* 59; Nicaragua case supra 244-5, Dugard *International law: SA* 497- 498; 6.4.2.1 of this study where government is also a victim of serious offence.

[2905] Arts 25 and 31 of CoCC provide for expedite access to data while art 35 of CoCC creates the use of 24/7 availability network service. Art 29 of CoCC preserves information before an OCI application is made; Osula A *Remote search and seizure of extraterritorial data* (PhD thesis 2017) 19-20 and 22 (Osula *Remote search and seizure of extraterritorial data*); Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 83.

[2906] *Investigating Directorate v Hyundai and Smit No* supra 1, 2, 6, 8, 27, 28, 30, 31, 33, 34, 44, 45, 46, 47, 48, 51 and 52. See 7.6.2.2 of this study.

[2907] These offences include fraud, theft, forgery, uttering, corruption or an economic offence involving patrimonial loss, see *Investigating Directorate v Hyundai and Smit No* supra 31, 44 and 48. Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 83.

[2908] Para 6.3.2 of this chapter.

The reasonable suspicious ground standard of proof or factual matrix required for the conduct of an OCI of crime commission is divided into two layers, namely: lower and low standards.

6.4.6.1 Popoola 'lower standard of merely reasonable suspicious ground' to investigate at the **second** *class and stage of serious crime commission*

In the non-mathematical principle, based on reasonable suspicious facts gathered to conduct an OCI of an offence, the standard of proof herein is where the commission of an offence '*actually*' threatens[2909] or poses a '*high*' security risk to the State security or public safety of the RSA or elsewhere under a relevant international public law obligation where such an offence '*will probably be committed'.*[2910] Thus a '*merely reasonable suspicious lower*' standard of proof[2911] is arguably required of LEAs at the '*second*' stage of crime commission to conduct an OCI[2912] subject to the principle of the fluidity of determination of a serious offence.[2913]

In the mind of a LEO or any other stakeholder, the mathematical factual matrix standard required to conduct an OCI of an '*actual* threatening offence' is gathered at the *second* stage of crime commission which is determined at a point of the *estimated value of facts reasonably or equitably equal to (=) or greater than (>) 10.1 % but less than (<) or equal to (=) 20 % of facts* required for the commission of such an offence, subject to the principle of the fluidity of determination of a serious offence.[2914]

6.4.6.2 Popoola 'low standard of merely reasonable suspicious ground' to investigate at the **third** *class and stage of serious crime commission*

In the non-arithmetical principle, based on *reasonable* suspicious facts gathered to conduct an OCI of an offence, the standard of proof herein is where the commission of an offence

[2909] Section 16 (3) (b) and (5)(a)(ii) of RICA and paras 6.3.3.1(b), 6.3.3.2(e), 6.3.3.3(e), 6.3.3.4(d) and 6.3.3.5(e) of this chapter.
[2910] Section 16(5)(a)(i) of RICA.
[2911] *Investigating Directorate v Hyundai and Smit No* supra 1, 4, 5, 6, 7, 13, 14, 28, 44 and 46; *Powell v Van der Merwe* supra 4; Section 16(5)(a)(ii) & (iii) of RICA.
[2912] Para 6.3.3.1 of this chapter for the six classes of serious offences.
[2913] Para 6.3.2 of this chapter.
[2914] Para 6.3.2 of this chapter.

'*potentially*' threatens[2915] or poses a '*medium*' national security risk or public safety in the RSA or elsewhere under a relevant international public law obligation where such an offence '*will probably be committed'*.[2916] Thus, a '*reasonable* suspicious *low*' standard of proof[2917] is required of LEAs to conduct an OCI at the '*third*' stage of crime commission,[2918] subject to the principle of the fluidity of determination of a serious offence.[2919]

In the mind of a LEO or any other stakeholder, the mathematical factual matrix standard required to conduct an OCI of a '*potentially* threatening offence' is gathered at the *third* stage of a crime commission which is determined at *a point of estimated facts reasonably or equitably equal to (=) or greater than (>) 20.1 % but less than (<) or equal to (=) 30 % of facts* required for the commission of such an offence, subject to the principle of the fluidity of determination of a serious offence.[2920]

6.4.7 Popoola 'high and higher standards of reasonable suspicious ground' to investigate at the *fourth* and *fifth* classes and stages of serious crime commission

This is the stage in crime commission that a LEO may conduct an OCI where there is a reasonable suspicion[2921] that *most* and *more* serious offences are *'being committed'*[2922] which require an early conduct of an OCI before the offence is executed at the *fourth* and *fifth* stages of crime commission[2923] —including where the commission of a crime is done via an e-mail,[2924] subject to the principle of the fluidity of determination of a serious offence.[2925]

The reasonable suspicious ground standard of proof required for the conduct of an OCI of serious crime commission is divided into two layers, namely: high and higher standards.

[2915] Section 16 (3)(b) and (5)(a)(iii) of RICA; Paras 6.3.3.1(c), 6.3.3.2(e), 6.3.3.3(e), 6.3.3.4(d), and 6.3.3.5 (e) of this chapter; Section 25 of the CPA; *Investigating Directorate v Hyundai and Smit No* supra 46, 48, 53 and 54.
[2916] Section 16(5)(a)(i) of RICA.
[2917] *Investigating Directorate v Hyundai and Smit No* supra 1, 4, 5, 6, 7, 28 & 44.
[2918] Para 6.3.3.1 of this chapter for the six classes of serious offences.
[2919] Para 6.3.2 of this chapter.
[2920] Para 6.3.2 of this chapter.
[2921] *Investigating Directorate v Hyundai and Smit No* supra 1, 2, 3, 6, 8, 10, 11, 13, 27, 28, 30, 31, 33, 34, 44, 45, 47, 49, 51 and 52; *Thint* supra 127, 252, 257, 265 and 291.
[2922] In paras 6, 31, 33 and 56 of *Investigating Directorate v Hyundai and Smit No*, the court recognises the third stage of crime commission in an attempted crime.
[2923] Para 6.3.3.1 of this chapter for the six classes of serious offences.
[2924] *Okah v State* supra 12.
[2925] Para 6.3.2 of this chapter.

6.4.7.1 Popoola 'high standard of reasonable suspicious ground' to investigate at the **fourth** *class and stage of serious crime commission*

In the non-arithmetical principle, based on reasonable suspicious facts gathered to conduct an OCI of a '*most*' serious offence, the standard of proof is where the commission of an offence may not constitute an offence in the *first* to *third* classes and stages of crime commission,[2926] but the commission of such an offence poses other forms of risks in the RSA or elsewhere under a relevant international public law obligation where such an offence 'is *being committed'*.[2927] Therefore, a 'reasonable suspicious *high*' standard of proof[2928] is required of LEAs at the '*fourth*' stage of crime commission to conduct an OCI,[2929] subject to the principle of the fluidity of determination of a serious offence.[2930]

In the mind of a LEO or any other stakeholder, the mathematical factual matrix standard required to conduct an OCI of a '*most*' serious offence is gathered at the *fourth* stage of crime commission which lies where *the estimated value of fact is reasonably or equitably equal to (=) or greater than (>) 30.1 % but less than (<) or equal to (=) 40 % of facts* required for the commission of such an offence, subject to the principle of the fluidity of determination of a serious offence.[2931]

6.4.7.2 Popoola 'higher standard of reasonable suspicious ground' to investigate at the **fifth** *class and stage of serious crime commission*

In the non-arithmetical principle, based on reasonable suspicious facts gathered to conduct an OCI of a '*more*' serious offence, the standard of proof is where the commission of an offence may not constitute an offence in the *first* to *fourth* classes and stages of crime commission,[2932] but the commission of such an offence poses other forms of risks in the RSA or elsewhere under a relevant international public law obligation where such an offence '*is being*

[2926] Aforementioned risks are mentioned in paras 6.4.5, 6.4.6.1 and 6.4.6.2 of this chapter.
[2927] Section 16(5)(a)(i) of RICA.
[2928] *Powell v Van der Merwe* supra 4.
[2929] Section 16(5)(a)(ii) and (iii) of RICA; Para 6.3.3.1 of this chapter for the six classes of serious offences.
[2930] Para 6.3.2 of this chapter.
[2931] Para 6.3.2 of this chapter.
[2932] Aforementioned risks are mentioned in paras 6.4.5, 6.4.6.1, 6.4.6.2 and 6.4.7.1 of this chapter.

committed'.[2933] Therefore, a 'reasonable suspicious *higher*' standard of proof[2934] is required of LEAs at the '*fifth*' stage of crime commission to conduct an OCI,[2935] subject to the principle of the fluidity of determination of a serious offence.[2936]

In the mind of a LEO or any other stakeholder, the mathematical factual matrix standard needed to conduct an OCI of a 'more' serious offence is gathered at the *fifth* stage of crime commission which lies where *the estimated value of facts is reasonably or equitably equal to (=) or greater than (>) 40.1 % but less than (<) or equal to (=) 50 % of facts* required for the commission of such an offence, subject to the principle of the fluidity of determination of a serious offence.[2937]

6.4.8 Popoola 'reasonable ground to belief' standard of investigation at the *sixth* class and stage of serious crime commission

In the non-arithmetical principle, based on the reasonable belief of facts gathered to conduct an OCI of a '*general*' serious offence, the standard of proof herein is where the commission of an offence may not constitute an offence in the *first* to *fifth* classes and stages of crime commission,[2938] but the commission of such an offence poses other forms of risks in the RSA or elsewhere under a relevant international public law obligation where such an offence '*has been committed'*.[2939] Thus, a '*belief*' standard of proof[2940] is required of LEAs at the *sixth* stage of crime commission to conduct an OCI,[2941] subject to the principle of the fluidity of determination of a serious offence.[2942]

In the mind of a LEO or any other stakeholder, the mathematical factual matrix standard required to conduct an OCI of a '*general*' serious offence occurs at the *sixth* stage of serious crime commission which is *the estimated value of fact reasonably or equitably equal to (=) or*

[2933] Section 16(5)(a)(i) of RICA.
[2934] Section 16(5)(a)(ii) and (iii) of RICA; *Investigating Directorate v Hyundai and Smit No* supra 1, 4, 5, 6 7, 13, 14, 28 & 44.
[2935] Para 6.3.3.1 of this chapter for the six classes of serious offences.
[2936] Para 6.3.2 of this chapter.
[2937] Para 6.3.2 of this chapter.
[2938] Aforementioned risks are mentioned in paras 6.4.5, 6.4.6.1, 6.4.6.2 and 6.4.7.1 of this chapter.
[2939] Aforementioned risks are mentioned in paras 6.4.5, 6.4.6.1, 6.4.6.2, 6.4.7.1 and 6.4.7.2 of this chapter.
[2940] *Investigating Directorate v Hyundai and Smit No* supra 14, 28 & 30.
[2941] Para 6.3.3.1 of this chapter for the six classes of serious offences.
[2942] Para 6.3.2 of this chapter.

greater than (>) 50.1 % of facts required for the commission of such an offence, subject to the principle of the fluidity of determination of a serious offence.[2943]

6.4.9 The role of artificial intelligence in determining reasonable ground standards in online criminal investigation

The use of AI is in pursuance of the use or role of a ROCI propounded in this study.[2944] An electronically configured program —which includes AI such as ML—[2945] is capable of executing almost everything that it is instructed to perform[2946] in devices, technologies, networks, applications and services to conduct an OCI.[2947]

In the conduct of an OCI, AI performs a task that goes beyond a CCTV camera function of merely recording visuals. In effect, an AI —in this study— assists in performing some configured administrative or quasi-judicial function by observing, watching, and sensing the unusual, uncommon, strange, confusing, chaotic or catastrophic activity, event or transaction that goes on within the system or environment. Thereafter, an AI takes steps to conduct an OCI of specific serious offences that the configured AI picks up based on the relevant reasonable ground standard required to intercept the serious crime commission in two environments, namely automated mobile and immobile environments.

First, an AI is used in conducting an OCI of serious crime commission in an automated mobile transport system or environment, which entails automated mobile, unstable, transitory, and non-permanent article or object such as robotic aircraft —which includes drones for warfare, robotic ships and submarines, robotic vehicles and trains.

The reasonable ground standards required to conduct an OCI using an AI in an automated mobile transport system remain the same general standards prescribed in this study,[2948] the standards of which are configured in the AI systems.

[2943] Para 6.3.2 of this chapter.
[2944] Para 2.11.4 of Chapter 2 of this study.
[2945] Kok J N et al. 'Artificial intelligence: definition, trends, techniques, and cases' http://www.eolss.net/sample-chapters/c15/e6-44.pdf (Date of use:22 November, 2019).
[2946] Adem *Legislative drafting: Mathematics & other devices* 151.
[2947] Para 6.4.4.3 of this chapter.
[2948] Para 6.4 of this chapter.

Second, given that robots are increasingly taking over human activities which reduce human involvement or interaction in daily or routine activities at home, office or business environment, an AI is used to conduct an OCI of the commission of a serious offence in an automated immobile or permanent place. For example, a child can be taken care of by a robot in a house, home or enclosed place, at which an OCI can be conducted where a serious offence is committed.

Where there is a serious crime commission in an automated immobile public place —e.g. in a restaurant— the reasonable ground standards required to conduct an OCI using an AI remain the same general standards prescribed in this study,[2949] otherwise, an OCI is prohibited in an automated immobile private place —including a personal home— save where there is a waiver of the right to the SOC by the occupant of the private home.

Generally, the admissibility of evidence obtained through an AI strictly requires that in both automated mobile transport system and automated immobile or permanent place system, the evidence obtained is basically and *ab initio* not admissible. This is because the conduct of an OCI is automated in the network of an Online Communication Service Provider or Interception Centre without going through the usual judicial process, given the urgency required to conduct an OCI in the system.[2950] However, admissibility may be considered in exceptional circumstances based on the proportionality and progressive principle of admissibility according to section 35(5) Constitutional limitation clause.[2951]

6.4.10 Conclusion

Any provision in RICA that places the standard of proof for the conduct of an OCI of a serious offence in one rigid standard of proof —such as the belief standard only—[2952] creates a jurisprudential fallacy in many ways such as a fallacy in the determination of the proportionality principle in terms of the classification of the seriousness of an offence, fallacy in the determination of the early investigation of such a serious offence and fallacy in the determination of other criteria required for the conduct of an OCI.

[2949] Para 6.4 of this chapter.
[2950] Paras 6.2.2 – 6.2.6 of this study.
[2951] Para 7.8 of Chapter 7 of this study.
[2952] For example, s 4(2)(b) of RICA.

Although it is widely perceived to be absurd to apply mathematical formulae in determining a legal problem such as the standard for the conduct of an OCI, however, this segment has presented the pros and cons of applying mathematical formulae in resolving legal problems such as the conduct of an OCI.

Drawing on a precedent,[2953] this study has attempted to establish that it is better, easier, more reasonable, rational and justifiable to apply mathematical formulae in the conduct of an OCI which is an informed guess in the determination of the standard of proof than applying non-mathematical and logical formulae, which still results in a blind guess.[2954] This is because the existing non-mathematical formulae do not have a consistent and reliable yardstick from which a more reasonable and justifiable OCI can be conducted than the mathematical formulae will do. It is concluded that if the Popoola mathematical formulae are properly applied, an accurate or near accurate outcome of the formulae —and not a guesswork— would occur. It is also concluded that the proposed Popoola non-mathematical formulae apply concerning the conduct of an OCI in each offence.

Although LEOs are not required to become professional mathematicians[2955] in this regard, however, it is important to reinstate that LEOs —like lawyers— practise and are trained in the field of logic[2956] when conducting a general investigation. Logic is a subset of mathematics, which lays the basis for the practical appreciation, understanding and preparation by LEOs, programmers and other stakeholders respectively in the emerging development, and deployment of AI applications[2957] in determining the various standards of proof required of LEOs to conduct an OCI.

It is not surprising therefore to learn that the application of an AI has already taken over the general or basic human operations in contemporary society, therefore, the field of cyber-criminal law and procedure should not be an exception with regards to the use of mathematical

[2953] Italics mine. *Singh* supra 152.
[2954] *Singh* supra 152.
[2955] Finkelstein and Levin *Statistics for lawyers* x.
[2956] Hutchinson *Doctrinal research* 8.
[2957] See generally the 'high level of technological readiness' of robust performance of autonomous artificial intelligence in the use of drones, which are tested outside the laboratory, Muller V C 'Autonomous killer robots are probably good news' in Di Nucci E and De Sio F S (eds) *Drones and responsibility- Legal, philosophical and socio-technical perspectives on remotely controlled weapons* (2016) 70 (Muller *Autonomous killer robots are probably good news*).

formulae standards in the conduct of an OCI. According to cyber law jurists, there is a marital symbiotic relationship between human and artificial intelligent entities, which ultimately create a powerful and more effective interdependent synergy that goes beyond the independent limit of each entity, otherwise, each entity is unable to solve complex problems individually.[2958]

In addition to the foregoing, this study heavily relies on human logic, as a supplement, to form the relevant reasonable ground standard to the extent that human effort constitutes the source of information gathered, upon which LEOs rely and input it into a system as if one is ticking some boxes at the end of which a result is released which indicates whether a reasonable ground standard is established in the *Popoola QOCI* protocol.[2959]

6.5 'NECESSITY' PRINCIPLE AS A STANDARD OF PROOF IN THE PROCEDURAL ASPECTS OF ONLINE CRIMINAL INVESTIGATION APPLICATION

6.5.1 Introduction

Basically, the requirements for conducting an OCI[2960] which generally provide that the court must be 'satisfied' with the facts in an OCI application before an interception direction is issued are strict.[2961] The satisfaction of the court is based on a balance of probability and not on an assurance of the necessity of the use of an OCI from the LEO to the court, which was erroneously the standard of proof under the previous OCI law in the RSA.[2962]

Aside from complying with the relevant substantive mathematical and non-mathematical standards of proof examined in this study;[2963] from another perspective, the standards of proof in the procedural aspects of 'reasonable ground' standard to conduct an OCI are based on a

[2958] De Greef T 'Delegation and responsibility: A Human –Machine perspective' in Di Nucci E and De Sio F S (eds.) *Drones and responsibility- Legal, philosophical and socio-technical perspectives on remotely controlled weapons* (2016) 139 (De Greef Delegation *and responsibility: A human –Machine perspective*).
[2959] Para 6.11 of this chapter.
[2960] Bawa *ROICA* 320.
[2961] Section 16(5), (7)(b) and (8)(a)(iii) & (b)(iii) of RICA; JSCI Reports 2016 at 40; Bawa *ROICA* 320; *AmaBhungane v Minister of Justice* supra 35.
[2962] Bawa *ROICA* 321.
[2963] Para 6.4 of this study.

thirteen-point procedural principle, amongst others.[2964] Chief amongst these are the principles of proportionality (which will not be examined in this segment because it has been severally examined in this study),[2965] necessity[2966] and 'urgency'.[2967] Although the necessity principle is examined as a separate concept, however, it is a broader concept that encompasses the thirteen principles including the urgency principle.

The principle of 'necessity' requires that the conduct of an OCI is not automatic neither does it have to be a last resort before it is embarked upon.[2968] However, the JSCI of Parliament of the RSA believes that the use of an OCI is not a first resort but must be the last resort to prevent privacy violation[2969] while Swart believes that an OCI must be 'absolutely necessary' before it is embarked upon.[2970]

[2964] Necessary and Proportionate 'Necessary and Proportionate Principles' http://es.necessaryandproportionate.org (Date of use: 12 December 2016). In art 16(5) of UNODC 'Model Legislative Provisions Against Organised Crime 2012, it is provided competent/ judicial authority which suggest that it may not necessarily be judicial authority but an authority that is competent. This study opposes a general non-judicial authority save in some circumstances involving master or captain of a ship or aircraft, see paras 2.11.4 and 6.4.9 of this study. Mare and Duncan 8-10 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf (Date of use:1 December 2017; Section 8(1)(d) of Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean '*Interception of Communication: Model Policy Guideline & Legislative Text'* (2012) https://caricom.org/documents/16583-interception_of_communication_mpg.pdf 16 April, 2016 (HIPCAR *Interception of Communication: 'Model policy guideline & legislative text* 2012).

[2965] More particularly paras 5.3.4, 5.3.6, 5.4 and 6.8 of this study. *Investigating Directorate v Hyundai and Smit No Hyundai* supra 54, 55 and 56; Mare and Duncan 8-10 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf (Date of use:1 December, 2017; In Canada, proportionality is referred to as 'Minimisation', Hubbard, Brauti and Fenton *Wiretapping* 4-40.3 to 4-44. *Thint* supra 274, 275, 276, 277, 284, 291 and 292.

[2966] In art 16(5) of UNODC 'Model Legislative Provisions Against Organised Crime' 2012, it is provided competent/ judicial authority which suggest that it may not necessarily be judicial authority but an authority that is competent. This study opposes a general non-judicial authority save in some circumstances involving master or captain of a ship or aircraft, see para 6.2 of this study. Mare and Duncan 8-10 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf (Date of use:1 December 2017). *Investigating Directorate v Hyundai and Smit No* supra 6, 8, 10, 12, 36 and 37 and *Thint* supra 128 - 129, 134, 229, 233, 234, 273, 280 - 281, 287, 290 - 296, 300, 302 - 321, 323 - 329, 331, 332 - 341, 345 - 350, 352, 354 - 358, 363, 366 - 368, 370 and 377 - 379.

[2967] *Thint* supra 356 and 361; *AmaBhungane v Minister of Justice* supra 91.

[2968] Paragraphs 5.3.4 and 5.3.6 of Chapter 5 of this study.

[2969] JSCI Report 2016 at 28 and 58. Canada does not believe that OCI should be a last resort but warned that an OCI should not be discretionarily used by LEOs as a as 'a tool of convenience', Hubbard, Brauti and Fenton *Wiretapping* 4-2a and 4-4. In the U.S., the principle of 'last resort' in one breath is adopted to the extent of showing the requirement of exhaustion and ripeness 'up to the time of submittal to the court' before conducting an OCI, Alberti *Wiretaps* 7. In another breath, the U.S. adopts a 'best efforts attempt' which expects LEAs to genuinely attempt other means but not exhaust all 'conceivable' means before adopting an OCI, Hubbard, Brauti and Fenton *Wiretapping* 4-21 to 4.22.

[2970] Swart 20 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use:13 August 2016).

Nevertheless, LEOs need to establish the reasonableness and justification of an OCI in 'all circumstances' by putting 'persuasive evidence' before the court, including the risk or frustration faced by LEOs in the midst of available less intrusive means when considering necessity principle.[2971] LEOs must also prove that they have the 'necessary technical capability to' conduct an OCI.[2972]

The 'urgency' principle is often and impliedly present in any procedural requirement of 'reasonable ground' to conduct an OCI.[2973]According to the Constitutional Court, the principle of 'urgency' states that LEOs may resort to an intrusive means once it is 'immediately apparent' to do so.[2974] The court also held that LEOs should not entertain delay in embarking on an intrusive measure immediately it is aware of the need to do so, otherwise, LEOs must explain the delay or the fear for not doing so on time.[2975] Foreign scholars also support this view by stating that serious offences require urgency in their investigation.[2976]

However, the proof of urgency principle may not be required in some interceptions such as sections 4(1), 5(1) and 6(1) of RICA because they are voluntary and consensual communications and intercepts.[2977]

Amongst the following six principles in the procedural aspects of the reasonable ground standards prescribed by RICA,[2978] LEAs are required —except otherwise stated— to prove three principles to conduct an OCI in all circumstances namely: a) 'affordability of evidence' principle, which is mandatory; b) one principle out of 'application and failure', 'unlikelihood of success' and 'too dangerous to apply' principles[2979] and c) one principle out of 'inadequate investigation' and 'inadequate information' principles.[2980]

[2971] *Thint* supra 276, 277, 279, 280, 281, 282, 285, 286, 291, 294, 295 and 361.
[2972] Caproni *Lawful electronic surveillance* 206.
[2973] See s 16(5)(b) & (c) of RICA and s 8(1)(a) & (c)(iii) of HIPCAR *Interception of communication: 'Model policy guideline & legislative text* 2012.
[2974] *Thint* supra 356 and 361. Justice delayed is justice denied, *Kaunda v President* supra 66 and 167.
[2975] *Thint* supra 356 and 361. Justice delayed is justice denied, *Kaunda v President* supra 166 and 167.
[2976] Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 41.
[2977] Para 6.2 of this chapter.
[2978] See s 16(5)(b) & (c) of RICA.
[2979] These conditions are also required in the U.S., Caproni *Lawful electronic surveillance* 209.
[2980] See paras 6.5.2 - 6.5.7 of this chapter which examine these six principles. These principles determine the effectiveness of the conduct of an OCI, same way that the effectiveness of a domestic court is determined before the UN Security Council refers a case to ICC for criminal prosecution, Du Plessis 'International Criminal Courts' 191.

According to the *ratios* established in *Thint* case,[2981] the factual matrixes in some of the six procedural principles of the reasonable ground standards may interchangeably apply to other principles herein.

It is also noted that the general standards of proof of the proportionality principle established earlier[2982] also apply in the procedural aspects of the conduct of an OCI. For example, the lowest standard of '*lowest standard of merely reasonable suspicious ground*' required to substantively conduct an OCI of a first-class serious offence[2983] is the same standard required to prove each of the six principles in the procedural aspects of the conduct of an OCI for a first-class serious offence.

6.5.2 Standard of proof in 'affordability of evidence' principle

In an OCI application,[2984] LEOs are required to prove that the conduct of an OCI will afford, establish or reveal evidence in online communication.[2985] In the case of *Jwara v State*, since the targets being investigated were LEOs themselves, the Supreme Court of Appeal held that no other tool of investigation other than an OCI would have been appropriate without jeopardising the investigation because of the endemic corruption in SAPS which the LEA wanted to be tackled effectively.[2986]

However, the U.S. erroneously held that if a target does not use a telephone to commit the criminal activity, the 'affordability of evidence' in an OCI is 'lacking and interception is 'ineffectual'.[2987] The decision of the U.S. court has the tendency of limiting the investigation

[2981] *Thint* supra 107, 110, 127, 130,280, 289, 294, 302 and 315.
[2982] Paras 6.4.5, 6.4.6.1, 6.4.6.2, 6.4.7.1, 6.4.7.2 and 6.4.8 of this chapter.
[2983] Para 6.4.5 of this chapter.
[2984] Affordability provisions are expressly or impliedly stipulated in RICA. The express provisions include sections 4(2)(b); 5(2)(c); 16(2)(d)(ii) & (5)(a)(ii)-(v),(b)(i); 17(2)(d)(ii) & (4); 19(4); 20(4); 21(4); 22(4)(a) & (b); 23(1),(2), (4)(a)(i),(ii) & (iii), (8)(a)(i) & (ii) and (11) of RICA; while the implied provisions include sections 6(2)(b)(i)(aa) & (bb); 7(1)(b) & (c); 8(1)(b) & (c)(i)(aa) & (bb),(2), (3)(a) & (b); 9(1); 10(c);11 and 16(5)(b)(ii) of RICA.
[2985] In an OCI application, LEOs are required to prove the 'reasonable ground to believe' that the use of an OCI will afford or reveal evidence, will be necessary to be conducted, will 'establish the existence of facts', will 'investigate or detect the unauthorised use' of a system, Hubbard, Brauti and Fenton *Wiretapping* 3 - 6 to 3 - 6.1, 4-2 and 4-2.10 to 4-2.11; JSCI Reports 2016 at 35.
[2986] *Jwara v State* supra 17.
[2987] Alberti *Wiretaps* 6.

of an OCI to cybercrime only, which is incongruous, whereas the concept of OCI broadly investigates the commission of offline and online offences.[2988]

LEOs are expected to use their discretion on how to handle the revelation of 'unforeseen information' in the course of an investigation.[2989] This is because LEOs are not entitled to embark on a fishing expedition, with the hope of finding some relevant items[2990] neither are they expected to know everything in advance that will likely be revealed[2991] when conducting an OCI. The affordability of evidence must be related to the purpose for which it is sought[2992] or the specific serious offence that is being investigated.[2993] However, LEOs are expected to determine what fact is 'entirely irrelevant to the investigation' and limit their investigation to what is relevant based on 'fair idea' or 'prior knowledge of the scope of the investigation.[2994] In the U.S., the court in *R v Willis* held that:

> **'**Once the monitoring agent has had a reasonable opportunity to assess the nature of an intercepted communication, he or she must stop monitoring that communication if it does not appear relevant to the government's investigation'.[2995]

By so doing, it gives a direction or clue to further or other investigative procedures, even though the interception may not reveal all the information required for the evidence.[2996]

[2988] Paras 2.5.2 and 2.5.3 of Chapter 2 of this study.
[2989] *Thint* paras 138, 139 and 145.
[2990] *Thint* paras 138, 139 and 144.
[2991] *Thint* para 145.
[2992] *R v Chow* [2005] 1 S.C.R. 384 para 34; Thus, an unknown person is someone who does not meet these two requirements, *R v Chesson* (1988) 43 C.C.C (3d) 353, [1988] 2 S.C.R 148 paras 7; *R v Schreinert* (2002), 165 C.C.C. (3d) 295, 159 O.A.C. 174 (Ont. C.A.) para 45; From the experience of LEOs in Canada, an individual who is known to another 'is more likely to confide in friends than strangers' and is also 'likely to speak to one another in areas of mutual interest' or 'matters of ordinary, everyday human experience' which 'might give' LEAs a 'significant lead' and assistance in their investigation, thus the need to conduct an OCI in the private communication of a known person, see *R v Schreinert* (2002), 165 C.C.C. (3d) 295, 159 O.A.C. 174 (Ont. C.A.) para 45; *R v Wright* (1990) 56 C.C.C (3d) 503 at p 517, 40 O.A.C. 171 (CA); *R v Pangman* [2000] 8 W.W.W R. 536, 147 Man. R. (2d) 93 (QB) paras 36 – 37; *R v Brand* (2006), 216 C.C.C. (3d) 65, 71 W.C.B (2d) 609 (B.C.S.C.) paras 28-39; *R v Chow* [2005] 1 S.C.R. 384 para 34; Hubbard, Brauti and Fenton *Wiretapping* 4-2.6 to to 4-2.8a, 4-2.10 and 4-2.11 to 4-2.14a.
[2993] Hubbard, Brauti and Fenton *Wiretapping* 4-2.2 and 4-2.8b.
[2994] *Thint* paras 144, 145 and 146. Section 19(3) of FICA Act 1 of 2017.
[2995] *R v Willis* No 99-1492 (7th Cir. 08/29/2002), see Hubbard, Brauti and Fenton *Wiretapping* 4.4.1 at page 4-43 to 4-44.
[2996] Alberti *Wiretaps* 1.

The JSCI in the RSA reveals that LEAs obtain information within *thirty-six hours* of the conduct of an OCI without the authorisation or knowledge of the court.[2997] However, it is reasonable for the governments of U.S. and Canada to instruct LEAs to monitor all calls of an identified target for a reasonable time which does not usually exceed *two to three minutes* to make an initial judgment —otherwise, two minutes periodical spot-check reassessment is done at an interval of one minute, especially in trafficking cases which involve a variety of topics— to determine the affordability or pertinence of evidence of the commission of the offence in the issue.[2998] It is easier said than done that LEAs would terminate the conduct of an OCI if the conduct does not afford evidence. However, LEOs do not have the gift of prescience and as such, they are not expected to have foreknowledge of the direction of the conversation.[2999]

However, the 'affordability of evidence' principle involves an element of anticipation, speculation or uncertainty,[3000] which requires that LEOs must inquire and establish the following questions: a) what is the expected to be obtained from the conduct of an OCI?; b) will whatever that is obtained be credible in a court of law?; c) will the outcome or objective of the conduct of an OCI justify the rationale for the investigation of the criminal activity?[3001]

According to the Constitutional Court, the standard of proof in the affordability of evidence is reasonable ground to believe that there is 'sufficiently plausible' reason that the object or item

[2997] JSCI Reports 2016 39; Para 3.5.7.8 of Chapter 3 of this study.

[2998] *R v Willis* (1997), 204 A.R.161 [1997] A.J. No 632 (QL) (Prov. Ct.); *United States v Mansoori* No 99-1492 (7th Cir. 08/29/2002) para 27; *United States v Ozar* 50 F.3d 1440, 1448(8th Cir.), see Hubbard, Brauti and Fenton *Wiretapping* 4.4.1 at page 4-43 to 4-44. It is noted that despite the intermittent two-minute interception, the defendant still complained, which impliedly means that lesser time could have been spent on the interception. *R v Steel* (1995), 34 Alta. L.R. (3d) 440 and *United States v Mansoori* supra 29; Hubbard, Brauti and Fenton *Wiretapping* para 4.4.1 at page 4-44. This aspect of the quote basically means that LEAs should be granted the leeway to determine whether an online communication is relevant. Para 3.5.7.8 of Chapter 3 of this study.

[2999] *United States v Quintana*, 508 F. 2d 867, 874 (7th Cir. 1975), see Hubbard, Brauti and Fenton *Wiretapping* para 4.4.1 at page 4-44.

[3000] Affordability certainly makes it impossible to determine what an individual will say in future or what 'evidence will necessarily be forthcoming', *R v Pangman* [2000] 8 W.W.W R. 536, 147 Man. R. (2d) 93 (QB) paras 36 – 37; Hubbard, Brauti and Fenton *Wiretapping* 4-2.11. In Canada, the court held that an OCI is for future communication which is speculative in nature unlike the standard in offline search and seizure procedure that has, in existence and at a particular place, the information that is being sought. An OCI is conducted 'during the period specified in the authorisation', see *CanadianOxy v Canada* supra 24 and 27; *R v Wright* (1990) 56 C.C.C (3d) 503 at p 517, 40 O.A.C. 171 (CA) and Hubbard, Brauti and Fenton *Wiretapping* 4-2 and 4-2.10 to 4-2.11. *R v Wright* (1990) 56 C.C.C (3d) 503 at p 517, 40 O.A.C. 171 (CA). *R v Wright* (1990) 56 C.C.C (3d) 503 at p 517, 40 O.A.C. 171 (CA); Hubbard, Brauti and Fenton *Wiretapping* 4.2.10. This case pre-supposes that the Canadian authority emphasises on archived communication unlike South Africa which provides for real-time as well, see sections 12 -15 of RICA.

[3001] Alberti *Wiretaps* 6.

of investigation must be connected to or have a bearing to the investigation.[3002] However, in the same Court, it held that the standard of affordability of evidence is the reasonable ground to suspect, which contradicts the earlier judgement of the court.[3003] This contradictory position of the Court reiterates the dichotomy between the two principles of suspicion and belief, which are reconciled and expanded into six standards of investigations in accordance with the proportionality principle of the procedural aspects of the conduct of an OCI in catering for the six classes of serious offences and the timing of the investigation of such serious offences.[3004]

For example, the lowest standard of reasonable suspicion required to substantively conduct an OCI at the first class and stage of serious offences[3005] is also required to prove the 'affordability of evidence' principle, otherwise, the purpose of classifying an offence and of investigating such offences at this stage will be defeated if more facts are needed for the affordability of evidence in the conduct of an OCI of first-class and stage offences.

It is further submitted that dynamic and proportionate affordability of evidence standards apply in different instances of the conduct of an OCI such as in the use of video surveillance, tracking devices,[3006] the use of and duration of use of content and mega or traffic data;[3007] the use of

[3002] *Investigating Directorate v Hyundai and Smit No* supra 8, 10, 12, 13, 36, 42(see sections 20 and 21 of the CPA), 48 and 52 and *Thint* paras 132, 138, 139, 144, 145, 146, 147, 149, 159, 160, 164, 165, 166, 167, 170, 172, 173, 176, 253, 255, 265, 288 and 291. In Canada, the best of what can be relied upon is 'reasonable probability' which is drawn on 'reasonable inference', *R v Pangman* [2000] 8 W.W.W R. 536, 147 Man. R. (2d) 93 (QB) paras 36 - 37; Hubbard, Brauti and Fenton *Wiretapping* 4-2.11. In the U.S., the standard is belief , Alberti *Wiretaps* 6. In the U.S., the condition is based on 'will afford', though the 'reasonable ground to believe' is fluid in nature, Hubbard, Brauti and Fenton *Wiretapping* 4-2.2 and 4-2.8b. In Canada, affordability is about 'being found' and not about 'if found'. In Canada, the standard is measured on 'credibly-based probability' and not mere possibility, Hubbard, Brauti and Fenton *Wiretapping* 4-2.2, 4-2.4 and 4-2.13.

[3003] *Thint* para 265. The court in Canada expresses the impossibility of knowing with certainty or 'absolute certainty' that the evidence will be revealed or is likely to afford and that further evidence obtained through physical search is executed, *R v Brand* (2006), 216 C.C.C. (3d) 65, 71 W.C.B (2d) 609 (B.C.S.C.) paras 28-39; Hubbard, Brauti and Fenton *Wiretapping* 4-2.4 to 4-2.6a and 4-2.13, 4-2.8b to 4-2.8c.

[3004] Paras 6.4.5 - 6.4.9 of this chapter. The standard of proof required in telephone record and tracking devices is RGS (Hubbard, Brauti and Fenton *Wiretapping* 5-53 to 5-60.2.) while it is argued that the standard of proof required in content data (be it video or audio) is RGB, Hubbard, Brauti and Fenton *Wiretapping* 3-6.3. It is noted that this study does not subscribe to the aforementioned rigid principles of RGS or RGB but relies on the proportionate and proportionate principle.

[3005] Para 6.4.5 of this chapter.

[3006] Sections 16(2)(d)(ii) & (5)(b)(i) and 17(2)(d)(ii) of RICA, amongst others; Hubbard, Brauti and Fenton *Wiretapping* 3-6 (or para 3.1), 3-20.8 to 3-20.10 (or para 3.5.5.1), 3-22 (or para 3.6.6), 3-26.1 (or para 3.7.5.1), 3-69 (or para 3.12.4.1), 3-76.1(or para 3.13.4), 3-76.6 (or para 3.14.4) and 3-77 to 3-90 (or para 3.15).

[3007] See sectiom 16 (2)(d)(ii), (5)(b)(i) & (ii) and other provisions of RICA. Hubbard, Brauti and Fenton *Wiretapping* 6 -22.14 to 6-22.15.

real-time[3008] or archived communication;[3009] use of o-toll monitoring;[3010] the type of devices, technologies, networks, applications and services used for the conduct of an OCI[3011] and many more.

6.5.3 Standard of proof in 'application and failure' principle

In the *Thint* case, the majority of the Constitutional Court held that the NPA complied with the principle of 'application and failure'.[3012] However, the minority decision, which expressed great concern over the majority judgment,[3013] was thorough in locating and evaluating credible evidence presented in the same court documents.[3014] The minority judgment pointed out that the LEO was neither truthful nor sincere with the information supplied to the court to secure an invasive means to investigate[3015] because the LEO did not use their power to query the targets.[3016]

These diverse and sharp views by the majority and minority decisions of the Constitutional Court indicate the difficulty in proving the application of this principle. It is however submitted

[3008] Hubbard, Brauti and Fenton *Wiretapping* 4-2 and 4-2.1 to 4-2.22.

[3009] Sections 12- 15 of RICA. In Estonia, the Supreme Court held that archived communication does not require court order but that of a prosecutor while real time communication requires a court order, Osula *Remote search and seizure of extraterritorial data* 57 and 60.

[3010] Hubbard, Brauti and Fenton *Wiretapping* 3 -75.

[3011] For example, first in relation to the criterion of reasonable expectation of privacy in o-toll technology, network, application, service and devices, borrowing from foreign jurisprudence, the Canadian case of *R v Wong* holds that there is no reasonable expectation of privacy if the place of surveillance is a public place (using CCTV camera or o-toll on the street or road), however, where it is not a public place, there is reasonable expectation of privacy, *R v Bryntwick* (2002) O J, No 3618(QL), 55 W.C.B (2d) 207(S.C.J); Hubbard, Brauti and Fenton *Wiretapping* 6-51 to 6-52. Similar decision was held in the U.S., *United States of America v Brijido Aguilera* 2008 U.S. Dits. LEXIS 10103, ADGN/2008-093; United States District Court for the Eastern Wisconsin, February 11, 2008; *United States v Knotts* 460 U.S. 276, 282, 103 S. Ct. 1081, 75 L. Ed 2d 55 (1983) Hubbard, Brauti and Fenton *Wiretapping* 3-74 to 3.76 and 6-52 to 6-53. Second, in relation to the criterion of frequency of use of technology, network, application, service and device by a user, a fax machine seems obsolete in the 21st century while a scanned document on the Internet is in vogue, thus, the reasonable ground standard to afford evidence is dependent on the frequency of use of such technology, network, application, service and device by a user.

[3012] *Thint* para 107,109, 110, 116, 117, 119, 125, 126, 127, 130, 133, 156 and 302.

[3013] *Thint* para 117, 125, 126, 233, 328 and 329.

[3014] *Thint* paras 230, 233-234, 253, 261, 273, 276 - 277, 279-282, 285 -286, 294, 296 - 303, 305 -329, 331-364, 366 -367, 370 -372 and 374- 382.

[3015] *Thint* paras 230, 233-234, 253, 261, 273, 276 - 277, 279-282, 285 -286, 294, 296 - 303, 305 -329, 331-364, 366 -367, 370 -372 and 374- 382. LEAs often face the problem of committing mistakes at the early stages of an OCI, Pieterse at 69 http://www.nstf.org.za/wp-content/uploads/2015/10/BrigPieterse.pdf (Date of use: 27 August 2017. This perhaps might be that some offences are difficult to detect and also difficult to secure conviction, such offences include racketeering, gang related offences, money laundering, Kruger *Organised crime and proceeds of crime* 9; *AmaBhungane v Minister of Justice* supra 140 and 141.

[3016] *Thint* para 142.

that although the majority decision constitutes the precedent, however, it is advised that the minority judgement may not be ignored as the threshold for the conduct of an OCI given the high risk and protection levels for the right to the SOC.[3017] In any case, LEAs must prove that there were no other means of investigation available, or better still prove that the conduct of an OCI is the 'only means to investigate'.[3018]

The reasonable ground standard required in the 'applied and failed' principle[3019] is that a LEO proves that other methods of investigations have been applied and failed to yield the desired result[3020] but the conduct of an OCI becomes an 'investigative necessity'.[3021]

Persuasively drawing on the decision of the Canadian Court in *R v Kokesch*, which though relates to the admissibility of evidence under section 24 (2) of the Canadian Charter which is equivalent to section 35(5) of the Constitution of the RSA; the relevance, interpretation and progressive development of the dictum below cannot be overemphasised. This dictum serves a second, dynamic and compelling purpose of espousing it *mutatis mutandis* under the onus of proof in this principle which is a strict proof in the dictum:

> '[o]f course, the reason why other investigative techniques were unavailable is that the police did not have the requisite grounds to obtain either a search warrant or an authorization to intercept private communications pursuant to the Criminal Code… the *unavailability of other, constitutionally permissible, investigative techniques is neither an excuse nor a justification for constitutionally impermissible investigative techniques…Where the police have nothing* but suspicion *and no legal way to obtain other evidence*, it follows that they must *leave the suspect alone, not charge ahead* and *obtain evidence illegally* and *unconstitutionally*. Where they take this latter course, the *Charter* violation is plainly more serious than it would be otherwise, not less'.[3022]

[3017] See paras 3.5.7 of Chapter 3 of this study.
[3018] *Jwara v State* supra 34.
[3019] In Canada, 'application and failure' principle is examined by Hubbard, Brauti and Fenton *Wiretapping* 4-2b, 4-3 to 4-31.
[3020] Section 16 (2)(e) and (5)(c) of RICA; Alberti *Wiretaps* 7. Section 6(2)(g) of HIPCAR *Interception of communication: 'Model policy guideline & legislative text* 2012.
[3021] See Hubbard, Brauti and Fenton *Wiretapping* 3-13, 3-20.4f, 4-3, 4-7, 4-12 to 4-20.
[3022] Italics mine. *R v Kokesch* [1990] 3 S.C.R 3, 61 C.C.C (3d) 207 5, 23 and 26-28, Sopinka J. See also para 5.3.6.1 of Chapter 5 of this study and paras 6.5.6 and 6.5.7 this chapter.

The 'applied and failed' principle must be proportionately proved at the various classes of serious offences and stages of crime commission to conduct an OCI of such serious crime.[3023]

6.5.4 Standard of proof in 'unlikelihood of success' principle

This principle indirectly emphasises the 'urgency' principle because LEAs may not bother to embark on an OCI at all based on the reliance on the conditional phrase 'if applied'.[3024]

In the 'unlikelihood of success' principle,[3025] the Constitutional Court held that it is unreasonable for LEAs to ignore less invasive means where it may succeed[3026] and that a LEO needs to establish the absence of the 'reasonable prospect' of using a less intrusive means[3027] before conducting an OCI. The Constitutional Court also held that a LEO must supply 'credible evidence' on why the other methods are unlikely to succeed given the non-disclosure of full facts by LEO before the court[3028] prior to the conduct of an OCI. The dissenting opinion of the Constitutional Court states that a 'first opportunity' be given to a third party who is not a suspect before deciding to embark on an intrusive investigative method.[3029]

The reasonable ground standard required in the 'unlikelihood of success' principle is[3030] what reasonably appears to a LEO that there is the immediate or specific likelihood of frustration from other investigative methods or immediate unlikelihood of success of other investigative methods[3031] which in its stead require the urgency of conducting an OCI.[3032] It is submitted that frustration does not arise from the fact that physical surveillance is expensive because someone will be hired to follow a target around.[3033] In any case, a comprehensive approach is adopted

[3023] Paras 6.4 and 6.5.2 of this chapter.
[3024] *Thint* supra 356; Section 16(5)(c) of RICA.
[3025] JSCI Reports 2016 at 34 and 35.
[3026] *Thint* supra 119, 127, 130, 276, 280, 294, 315, 356, 357, 359, 360, 363 and 371.
[3027] Thint supra 275.
[3028] *Thint* supra 356, 357, 359, 360.
[3029] *Thint* supra 363; Art 16(8)(b) of UNODC 'Model legislative provisions against organised crime 2012 at 82.
[3030] See also section 8(1)(c)(i) of HIPCAR *Interception of communication: 'Model policy guideline & legislative text* 2012. In Canada, 'Unlikelihood of success' principle is examined by Hubbard, Brauti and Fenton *Wiretapping* 4-31 to 4-34.4.
[3031] Such methods include 28 subpoena application in NPA Act which may induce suspects to hide or destroy documents being sought for by a LEO, see *Thint* para 119, 130, 280, 361 and 371.
[3032] Section 16(2)(e) and (5)(c) of RICA.
[3033] Blumberg and Eckersley *Locational privacy* 315.

in the fruitful prosecution of a particular case, which does not rely on the conduct of an OCI alone.[3034]

The 'unlikelihood of success' principle must be proportionately proved at the various classes of serious offences and stages of crime commission to conduct an OCI of such serious crime.[3035]

6.5.5 Standard of proof in 'too dangerous application' principle

The reasonable ground standard required in the 'too dangerous application' principle[3036] is that a LEO proves that other methods of investigations display some 'appreciable risks' or that that the application of other methods is likely to be too dangerous[3037] except the conduct of an OCI.

The 'too dangerous application' principle must be proportionately proved at the various classes of serious offences and stages of crime commission to conduct an OCI of such serious crime.[3038]

6.5.6 Standard of proof in 'inadequate investigation' principle

The reasonable ground standard required in the 'inadequate investigation' principle is that a LEO proves that information is neither forthcoming nor comprehensive from a suspect during an investigation or where a suspect covers his track of the commission of an offence.[3039] The standard also covers a situation wherein an overt investigation, a suspect does not respond

---

[3034] JSCI Reports 2016 at 52.

[3035] Paras 6.4 and 6.5.2 of this study chapter.

[3036] JSCI Reports 2016 at 34; See also section 8(1)(c)(ii) of HIPCAR *Interception of communication: 'Model policy guideline & legislative text* 2012. In Canada, 'too dangerous application' principle is examined by Hubbard, see Hubbard, Brauti and Fenton *Wiretapping* 4-34.4 to 4-36.

[3037] *Thint* paras 126, 130, 132 and 277; Section 16(2)(e) and (5)(c) of RICA; Arguably, danger includes potential and actual threats recognised by law from the physical, social, economic and environmental perspectives, s 16(5)(a)(ii) and (iii) of RICA. Mare and Duncan 18-30 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf (Date of use: 1 December 2017); In Canada, proportionality is referred to as 'Minimisation', Hubbard, Brauti and Fenton *Wiretapping* 4 - 40.3 to 4 - 44.

[3038] Paras 6.4 and 6.5.2 of this study chapter.

[3039] *Thint* paras 127, 130, 156, 280, 289, 294 and 302. In Canadian, the principle of 'inadequate investigation' states that serious offence is impracticable to investigate with the use of other methods, Hubbard, Brauti and Fenton *Wiretapping* 4-2b.

honestly and truthfully, which creates doubts in the confidence of continuing with the investigation.[3040] Heavy reliance is placed on the ratio in the Canadian jurisprudence in *R v Kokesch* which is earlier cited in this study, which highlights the heavy onus of proof of this principle on a LEO.[3041]

The 'inadequate investigation' principle must be proportionately proved at the various classes of serious offences and stages of crime commission to conduct an OCI of such serious crime.[3042]

6.5.7 Standard of proof in the 'inadequate information' principle

Where other investigating methods do not freely yield the envisaged information,[3043] a LEO may be justified to apply for the conduct of an OCI. The reasonable ground standard required in the 'inadequate information' principle is for a LEO to prove that information 'cannot adequately be obtained' through other 'appropriate manners' before conducting an intrusive method[3044] such as an OCI. Heavy reliance is placed on the ratio in the Canadian jurisprudence in *R v Kokesch* which is earlier cited in this study, which highlights the heavy onus of proof of this principle on a LEO.[3045]

The 'inadequate information' principle must be proportionately proved at the various classes of serious offences and stages of crime commission to conduct an OCI of such serious crime.[3046]

[3040] *Thint* supra 130 ; *AmaBhungane v Minister of Justice* supra 140 and 141.
[3041] *R v Kokesch* supra 5, 23 and 26-28. See para 5.3.6.1 of Chapter 5 of this study and paras 6.5.3 and 6.5.7 of this chapter.
[3042] Paras 6.4 and 6.5.2 of this study chapter.
[3043] *Thint* supra 118, 130.
[3044] *Thint* supra 106, 107, 108, 110, 127, 130, 133, 154, 155, 163, 280, 289, 294, 302 and 315; Section 16(5)(c) of RICA.
[3045] *R v Kokesch* supra 5, 23 and 26-28. See para 5.3.6.1 of Chapter 5 of this study and paras 6.5.3 and 6.5.6 of this chapter.
[3046] Paras 6.4 and 6.5.2 of this study chapter.

6.5.8 Conclusion

In conclusion, the various procedural principles required in the conduct of an OCI —including the proportionality, necessity and urgency principles— must be proved at the various stages of interception of serious crime commission in the conduct of an OCI in the RSA.

6.6 STANDARD OF PROOF REQUIRED TO INTERCEPT AND CONDUCT ONLINE CRIMINAL INVESTIGATION IN SPECIFIC INSTANCES

The standard of proof required to conduct an OCI of serious offences or relatively intercept in specific instances is stipulated in the various provisions of RICA: i) to intercept in the consensual, expedient and statutory and technical interception;[3047] ii) to investigate the commission of complete and incomplete offences;[3048] iii) to conduct an OCI of the commission of organised crime and terrorism at the international level;[3049] iv) to investigate the use of property as an instrumentality of the commission of serious offences;[3050] v) to investigate offline electronic and cyber-related crime;[3051] vi) to investigate the preservation of data in mutual legal assistance; vii) to investigate offences committed aboard a ship and an aircraft and viii) to investigate serious offences committed in artificially intelligent driven vehicles, sail ships and piloted aircraft.

6.7 APPLICATION BEFORE A MAGISTRATE AND JUDGE

RICA grants jurisdiction to a regional magistrate court or magistrate[3052] and a designated judge or judge[3053] to administer the provisions and adjudicate over issues relating to the conduct of an OCI, with wider powers vested in a designated judge than in an ordinary judge or magistrate. There are limited instances where an ordinary High Court judge —other than a designated

[3047] Paras 6.2.2, 6.2.4 and 6.2.6 of this chapter.
[3048] Section 2 of RICA.
[3049] Section 16(2)(e)(i) and (5)(a)(iv) & (c)(i) of RICA; JSCI Report 2016 at 11.
[3050] Section 16 (2)(e)(ii) and (5)(a)(v) & (c)(ii) of RICA.
[3051] Cameron S D Brown 'Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice' *International Journal of Cyber Criminology* Vol. 9 Issue 1 January – June 2015; U.S. Department of Justice *Electronic Crime Scene Investigation – A Guide for First Responders* 2001 (Washington, U.S Department of Justice).
[3052] Sections 19 (1), (3), (4) & (7), 48 and 59 of RICA.
[3053] Sections 1, 7(4),(5) &(6), 8(4)(b), (5) & (6), 16 (1), (5), (7)(b), (8)(a)(iii), (b)(iii) & (10)(b), 17(1),(3) & (4), 18(1),(2)(a), (3), (4)(a)&(b), 19(1), (3), (4), (7) & (8), 20(1), (3) & (4), 21(3),(4)(a)&(b), 23(3), (4)(a)&(b), (7), (8)(a) &(b), (10),(11) & (12)(a), 24, 25(1), (2), (3), 48, 58 (1) and 59 of RICA.

judge—[3054] is permitted to apply the provisions of RICA.[3055] These instances include where a judge allows a certificate of proof of facts signed by another judge and where a judge applies section 205 of the CPA under RICA provisions to obtain information from a witness on request by the National Prosecuting Authority.[3056] Given that RICA exempts an ordinary High Court judge from the general conduct of an OCI, though reasonably and justifiably, it highlights the following inadequacies in the general constitution of the adjudicating authorities in the conduct of an OCI.

Firstly, relying on *Popoola QOCI* protocol conceptualised in this study where an OCI application can be made to and granted by the court regarding real-time or archived online communication,[3057] it is unnecessary to appoint too many judicial officers in adjudicating an OCI application. This is because such applications can be considered by a judge or very few judges who can hear an OCI application in the virtual contemporary society.[3058] Moreover, in the last dispensation of the appointment of a designated judge, only a judge was appointed to administer an OCI manually and physically, though administratively, judicially and financially chaotic and ineffective, as reported by the JSCI.[3059]

Secondly, without prejudice to the training, knowledge, skill and experience of magistrates, they should be exempt from administering the provisions of RICA because of the general lack of knowledge and skill of the dynamic complexities in the protection of online communication and the conduct of an OCI by legal minds including magistrates and judges who are involved in the conduct of an OCI.[3060] Furthermore, the fact that not all judges of the High Court —but designated judges— are permitted to adjudicate on the general OCI application further buttresses the need to restrict the adjudication of an OCI application to some specific and specialised judges only.

Lastly, although there is one published or record of an allegation of misconduct levelled against a judge under RICA thus far in the report by Right2know where interception direction was

[3054] See the definition of 'designated judge' in section 1 of RICA.
[3055] Sections 48 and 59(1) of RICA.
[3056] Sections 48 and 59(1) of RICA. See para 6.12 of this chapter where the role of Magistrate Court in granting section 205 of the CPA is condemned.
[3057] Para 6.11 of this chapter.
[3058] Para 6.11 of this chapter.
[3059] JSCI Report 2016 at 21, 24, 28 and 53,
[3060] Para 3.5.5 and 3.5.7.2 of Chapter 3 of this study.

renewed by a judge without reasons for an interception against an investigative journalist,[3061] the fact that only a discharged or retired judge is appointed a designated judge creates a susceptible atmosphere of compromise, disloyalty to public criminal interests, non-committal or nonchalance by a designated judge.

As a corollary, despite the relative costs saving measure for hiring retired judges, concern has also been raised on the independence of designated judges presiding over OCI application proceedings since the designated judges are retired judges who may not owe allegiance to the public but to the appointing authority, which is the Minister of Justice.[3062] This is because, save for the loss of integrity, a designated judge who compromises in the adjudication of an OCI application loses nothing in terms of the enjoyment of pension benefit and career or employment elevation or opportunities because the appointment as a designated judge is a post-retirement position which has no bearing on the career of the designated judge.

Therefore, it is recommended that only a few serving judges or persons recommended by the National Judicial Service Commission who are certified knowledgeable and skilful in the conduct of an OCI[3063] be appointed as adjudicating officers in the administration of the provisions of RICA because of the foregoing reasons.

[3061] In this report, it was alleged that one of the editors of the newspaper petitioned the SSA for breach of unlawful interception. At the end, no reason was found in the file for the interception direction issued by a judge in Durban. Thereafter, the investigative journalist petitioned the Inspector-General of Intelligence who revealed that the true and correct identity of the investigative journalist, including the name of the media house, was supplied to Judge Khumalo before the direction was granted, Right2Know at 5-6 and 11 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[3062] Para 6.7 of this chapter; *AmaBhungane v Minister of Justice* supra 14, 27, 32, 40, 61- 66, 69 and 168(2); Bawa *ROICA* 308. JSCI Report 2016 at 55.

[3063] See para 4.3.8 of Chapter 4 of this study.

6.8 SPECIALISED AND PROPORTIONATE FUNCTION OF LAW ENFORCEMENT AGENCIES AND OFFICERS IN ONLINE CRIMINAL INVESTIGATION APPLICATION

RICA only provides for the specialisation of the LEAs,[3064] but RICA does not provide for the performance of the function of LEOs according to the seriousness of an offence.[3065] In an OCI application, LEAs perform some specialised functions, which in a way require the application of the proportionality principle, in that, aside from the general online law enforcement functions, some LEAs are better assigned some functions that are more proportionately, constitutionally, statutorily and practically related to their functions.[3066]

6.9 FORMS OF ONLINE CRIMINAL INVESTIGATION APPLICATION

6.9.1 Introduction

In RICA, an OCI application is physically presented before a court in two ways, which are in written and oral forms.[3067]

6.9.2 Written and oral physical application

Generally, under RICA, a LEO physically submits a written OCI application to the court to conduct an OCI where there is no urgency in the investigation of a serious offence. A LEO must, in the relevant application, provide all the substantive and procedural facts need to secure a direction of court according to the various proportionality requirements. The various requirements are provided in RICA, mainly an affidavit indicating the relevant information in the application.[3068]

[3064] Section 16(3)(b) of RICA assigns to DI-SANDF and SSA the conduct of an OCI of serious offences that are actually and potentially threatening to the national security and economic interests of the State and public health or safety in section 16(5)(a)(ii) and (iii) of RICA. In section 16(3)(c)(i) and (ii) of RICA, the conduct of an OCI of organised crime and terrorism —in pursuance of international law, relations, obligations and interests beneficial to the RSA and international mutual assistance agreement— is assigned to the CI-SAPS, HAWKS and SSA in section 16(5)(a)(iv) of RICA. it is the function of the ID-NPA in section 16(3)(d) of RICA to conduct an OCI of instances where property was used an instrumentality of the commission of a serious offence or where property is involved as a proceed of crime in section 16(5)(a)(v) of RICA.

[3065] Para 4.2 of Chapter 4 of this study.

[3066] Para 4.2 of Chapter 4 of this study.

[3067] Sections 8(2), 16(2), (6)(a), 17(2), (5)(a), 18(2)(b)(i), 19(2) &(5)(a), 20(2), 21(2) and 23 of RICA.

[3068] Sections 8(2), 16(2), (6)(a), 17(2), (5)(a), 18(2)(b)(i), 19(2) &(5)(a), 20(2), 21(2) and 23 of RICA.

However, where there is an urgent need to conduct an OCI in pursuance of the various proportionality requirements, an oral OCI application is physically made to court, under an oath justifying the need for the conduct of an OCI. The pursuance of an oral OCI application is premised on the fact that due to the certainty of issuance of an oral direction and urgency, exceptional circumstances or immediate necessity of a matter, it is reasonably impracticable to make a written application.[3069] In an oral OCI application, a LEO is required to satisfy the court that a written application must be submitted within 48 hours of the issuance of oral direction,[3070] upon which a written or oral direction may be issued.[3071]

However, it is ironic that RICA, being a law that regulates online communication and investigation, does not make provision that the request for an OCI be made in an online communication application instead of the written and oral physical applications[3072] with their inherent challenges, in which judicial notice is taken. In attempting to resolve this lacuna, this study proposes *Popoola QOCI* protocol to address the human errors involved in both written and oral physical OCI application.[3073]

6.10 TYPES OF ONLINE CRIMINAL INVESTIGATION APPLICATION

6.10.1 Ex-parte application

6.10.1.1 Introduction

Save in the conduct of a powered AI or ROCI and other exceptional circumstances which do not require a prior-consent of court,[3074] LEAs in the RSA generally rely on judicial authorisation to conduct an OCI through an ex-parte warrant[3075] for expedient and effective

[3069] Section 23, more particularly (1)-(4) and (7)-(9) of RICA. Section 14 of HIPCAR *Interception of communication: 'Model policy guideline & legislative text* 2012.
[3070] Section 23(4)(b) & (8)(b) of RICA.
[3071] Section 23 (5) and (7) of RICA.
[3072] See para 6.11 of this chapter for the examination under another rubric of the inadequacies of the forms of an OCI application.
[3073] Para 6.11 of this chapter.
[3074] Para 6.2 of this chapter.
[3075] In international law, whether it is a warrant relating to law enforcement or for national or public security, a warrant is required, Paragraphs 51-52 of Section III (Explanatory Notes on) HIPCAR *Interception of communication: 'Model policy guideline & legislative text* 2012. However, LEAs in the UK do not require judicial authorisation to conduct OCI, Paragraphs 32 and 49 of Section III (Explanatory Notes on) HIPCAR *Interception of communication: 'Model policy guideline & legislative text* 2012.

execution of the investigation process since a target is not supposed to be aware of the pre-conduct and post conduct of the covert OCI.[3076]

Two schools of thought contribute to the debate on the validity of making an ex-parte application or execution of the same to conduct an OCI.

6.10.1.2 Covert online criminal investigation

The first school of thought in which this study titles 'covert online criminal investigation' believes that since crime is committed in the secret, the investigation of such crimes should be done covertly.[3077] This study submits that the issuance of the notice before or during the conduct of an OCI to a target defeats the essence of the conduct of an OCI because a target may know the inner workings of the LEAs[3078] and a target may reasonably and arguably refrain from using the targeted devices if notified of pending conduct of an OCI, which is the ratio raised by the Supreme Court of Appeal in *Mngomezulu v NDPP* but the notice should be given thereafter.[3079] Therefore, an ex-parte application and execution of the warrant in an OCI is reasonable and justifiable as the High Court similarly held in *AmaBhugane*.[3080]

Given the unequivocal position that this study holds that online communication is techno-legally conscriptive in nature,[3081] it seems difficult for an individual in modern society to live without the constant use of an online communication device even where a target is notified of pending interception by LEAs.

Moreover, there is no legal or scientific study in the RSA that is publicly available to irrebuttably prove that there is total abstinence by a target of an OCI from making use of both content and non-content online communication after being aware of the conduct of an OCI against him or her. Thus, an OCI can be conducted covertly because online communication is

[3076] *Mngomezulu v NDPP* [2007] SCA 129 (RSA) para 6.
[3077] Section 16(7) of RICA; *R v Abelson* supra 231; Kruger *Organised crime and proceeds of crime* 1; Van der Vyver *State secrecy* 48.
[3078] *AmaBhungane v Minister of Justice* supra 50.
[3079] *Mngomezulu v NDPP* [2007] SCA 129 (RSA) paras 6 and 7.
[3080] *AmaBhungane v Minister of Justice* supra 41 – 45 and 52.
[3081] Para 2.3.3 of Chapter 2 of this study.

inherently and technically conscriptive; an OCI does not need further approval —such as a notice to a target— to carry out a covert OCI on such target.

6.10.1.3 Open online criminal investigation

The second school of thought in which this study titles 'open online criminal investigation' posits that a target should be timeously notified of the decision and the earlier evidence gathered in support of the decision to conduct an OCI.[3082] The notification avails a target the opportunity of challenging the decision or proposing a remedy[3083] concerning online communication infringement. This position is strengthened by the usual legal process that enables a respondent answer to allegations through a notice on motion arising from an initial an ex-parte motion. The rationale behind this school of thought is partially borne out of the fact that since the notice is immediately given or an audible announcement or a request for admission into the offline premises of a target is made by LEAs, a similar principle is applicable in an online interception.

In Europe, the law requires service providers to request for consent from an individual before accessing his or her data,[3084] the position of which is supported by some pressure groups (such as EFF) in the US.[3085]

Although RICA does not make provision for the notification of a subject data before and after LEAs have conducted an OCI on a user of online communication, however, the POPIA provisions generally require the issuance of a post-use notice, which may be delayed to prevent the impediment to the effective and efficient conduct of an OCI.[3086] A LEO is required to swear to a certified statement to the designated judge to the effect that a notice is issued.[3087]

[3082] EFF 'International principles on the application of human rights to communications surveillance'.
[3083] EFF 'International principles on the application of human rights to communications surveillance'.
[3084] Osula *Remote search and seizure of extraterritorial data* 41, 54, 55, 56, 57 and 58; Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 59.
[3085] Fischer C 'EFF amicus brief: The Privacy Act requires the FBI to delete files of Its Internet speech surveillance' https://www.eff.org/deeplinks/2018/08/eff-amicus-brief-privacy-act-requires-fbi-delete-files-its-internet-speech (Date of use: 10 August 2018) (Fischer https://www.eff.org/deeplinks/2018/08/eff-amicus-brief-privacy-act-requires-fbi-delete-files-its-internet-speech (Date of use:10 August 2018).
[3086] Section 22(3) and (4)(b) of the POPIA.
[3087] *AmaBhungane v Minister of Justice* supra 168(1).

The defect in RICA is also pronounced by the Supreme Court of Appeal in *Mngomezulu v NDPP* which held that there is no need for further secrecy where an OCI direction has been executed.[3088] This judgement is corroborated and further enforced by the High Court in *AmaBhugane* where the court held that post-OCI notice is mandatory (similar to Germany, Japan and the U.S.A but not Russia) and accordingly ordered an amendment of the provision of RICA.[3089]

The amendment includes a provision on the issuance of a post-OCI notice to a target of the conduct of an OCI within 90 days of the expiry of the conduct of an OCI (similar to the U.S.A and Canada, while notice is given within 30 days in Japan) and within 180 days at a time of expiry of the conduct of an OCI in exceptional circumstances,[3090] otherwise, the non-issuance of a notice makes the conduct of an OCI become absolute secrecy.[3091]

However, there may be a deferment of notice for renewable three months in exceptional circumstances which may last for three years after the conclusion of an OCI upon an application before a panel of three designated judges who may extend the three-year notice period.[3092] However, the proportionality principle highlighted in *AmaBhugane*[3093] is not strictly complied with when compared with the recommended duration of the conduct of an OCI.

6.10.2 Motion on notice to a ghost or public advocate

Although RICA regime does not provide for general issuance of a pre or post-notice to a target of the conduct of an OCI, nonetheless, a special regime in RICA allows only a post-OCI notice in a correctional facility.[3094] Save where there is an ongoing conduct of an OCI in a correctional facility, the head of the correctional centre or the designate is, in writing, as reasonable as practicable, required to furnish in a post-OCI notice the reasons for the conduct of an OCI to

[3088] *Mngomezulu v NDPP* paras 6 and 7.
[3089] *AmaBhungane v Minister of Justice* supra 43, 47, 49, 51 and 168(1).
[3090] *AmaBhungane v Minister of Justice* case supra 43, 47 and 168(1); Right2Know at 8 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).
[3091] *AmaBhungane v Minister of Justice* supra 41- 45 and 54.
[3092] *AmaBhungane v Minister of Justice* supra 41- 45 and 54.
[3093] *AmaBhungane v Minister of Justice* supra 50.
[3094] Reg. 8(5) of Correctional Services Regulation.

an inmate who is by right required to submit a representation with respect thereto the head of the centre or the designate.[3095]

Pursuant to the operation and execution of an ex-parte application, which applies in the conduct of an OCI application based on the covert nature of an OCI, a target of the conduct of an OCI was never informed before or after the conduct of an OCI before the 2019 decision of the High Court in *AmaBhugane*, thus LEAs perpetually kept the information gathered as secret in the old regime.[3096] This case now allows the dispatch of a post-OCI notice to a target of an OCI conduct in which RICA did not hitherto enable the usual or substantial practice of the adversarial administration of justice, thus RICA compromised the efficacy of the role of the judiciary before this precedent[3097] which is the last hope of a common man to seek for redress.[3098]

The non-issuance of a post-OCI notice is unlike an offline scenario where there is a likelihood of a prominent, and visible or express and spontaneous pre-entry or search notice or knowledge and express or implied post-entry and search notice issued, acknowledged or observed in the offline world if none of the targets of entry and search is present during the search.[3099]

There are two sides to the coin on the provision of a public advocate. On the one hand, it is argued in the case of *AmaBhugane* that it is presumed that the authorities select a judge that is diligent to play the adversarial and interrogatory role in an OCI application and that the applicant or LEA is equally under an ethical obligation to truthfully and fully disclose the facts. Therefore, it is unnecessary to have a public advocate who is not seized of the facts of the case of the target because the public advocate is not legally allowed to have access to the target of an OCI to verify the allegation in the OCI application due to the covert nature of an OCI.[3100] Moreover, it is a security risk to involve a third party in the conduct of an OCI (such as a public advocate), the risks of which include who or what authority should perform this third party

[3095] Reg. 8(5) of Correctional Services Regulation.
[3096] *AmaBhungane v Minister of Justice* supra 30, 31, 45, 61 and 72; Right2Know at 8 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November, 2018); Para 6.10.1.2 of this chapter.
[3097] *AmaBhungane v Minister of Justice* supra 61.
[3098] *AmaBhungane v Minister of Justice* supra 30, 31 and 45; Right2Know at 8 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018); Para 6.10.1.2 of this chapter.
[3099] Section 103(6)(b) and 105(4)(a) of the COPA.
[3100] *AmaBhungane v Minister of Justice* supra 76, 77, 140 and 141.

role, how would this person or authority be 'selected, vetted and briefed' and what are the implications for timing and accessing[3101] the public advocate in a method that requires urgency in conducting an investigation.

On the other hand, it is argued in the same case of *AmaBhugane* that there is no opportunity for the target of the conduct of an OCI to test the evidence produced by the LEA or LEO in an OCI application, which forces the target to rely on the integrity of the LEA or LEO[3102] and the impartiality of the court, thus a target is at the mercy of the LEA or LEO.

In attempting to strike a balance between the two divides, the practice of inviting an *amicus curie*, which is the practice in the U.S. does not really help matters because an *amicus curie* is not applied as a matter of default, but adopted as an *ad-hoc* and limited to the development of a novel law, in which the opinion of the *amicus* is neither here nor there, therefore this practice does not guarantee the protection of the right of a target in a particular application.[3103] The court in *AmaBhugane* also held that the alternative of having a panel of three designated judges to comply with the principle of *audi alteram partem* does not solve the problem of securing information in an OCI application, coupled with the diverse views to be expressed by the three judges in the court of first instance in an OCI application.[3104] Ultimately, the court declared the provision of section 16(7) of RICA invalid because it fails to provide for the establishment of the office of a public advocate.[3105]

It is therefore submitted that one of the remedies to the defect in the non-issuance of a post-OCI conduct notice is the establishment of an independent OGA or OPA[3106] who arguably, under a perpetual secrecy oath and other stringent conditions and without informing the target about the proposed —pending or concluded— conduct of an OCI, plays the role of a 'devil's advocate' —who may be called upon in line with the practice in the U.S.A—[3107] by defending

[3101] *AmaBhungane v Minister of Justice* supra 78.
[3102] *AmaBhungane v Minister of Justice* supra 77.
[3103] *AmaBhungane v Minister of Justice* supra 79.
[3104] *AmaBhungane v Minister of Justice* supra 80.
[3105] *AmaBhungane v Minister of Justice* supra 81-83.
[3106] This office should not be attached to the NPA and Ministry of Justice or its affiliates or be administered by any executive or judicial authority, but accountable to the National Assembly with appropriate legal framework to work as those of other independent authorities examined in this study.
[3107] *AmaBhungane v Minister of Justice* supra 72.

an OCI application brought by a LEA or LEO against a target of an OCI for inappropriate conduct of an OCI.[3108]

The establishment of this office is in furtherance of the practice of the natural law of *audi alteram partem*,[3109] which requires that a LEO serves a pre-hearing notice or motion on notice on an OGA, relying on *Popoola QOCI* protocol.[3110] Although it may be argued that the non-issuance of a pre-hearing notice in the conduct of an OCI through an OGA is an exception to the general rule of the *audi alteram partem* principle, which basically means that a target of the conduct of an OCI should not be heard in an OCI application through an OCI, nonetheless, one cannot overemphasise the complexity and delicacy of the risks involved in protecting the right to the SOC,[3111] the limitation of which right should not be executed unreasonably and unjustifiably.[3112]

In addition, it is submitted that an OGA should be given the power to have the same access to the techno-legal information that a LEA or LEO has in the conduct of an OCI. Such power includes the power of an OGA to, though without usurping the powers of a Cyber Inspector[3113] and the OIGI[3114] in conducting a technical investigation in response to complaints lodged by an aggrieved party, conduct a techno-legal investigation in defending a target. This complies with the principle of *audi alteram partem*, so that the OGA is not caught unawares in the outcome of a post-OCI application.

To some extent, the role and independence of the OGA in this regard may —in a way— be likened to an online communication OPP, which strikes a balance between the protection of the right to SOC and conduct of an OCI. Furthermore, whether or not an OGA is established, it is recommended that a post-OCI notice should be issued to a target of an OCI,[3115] though an

[3108] *AmaBhungane v Minister of Justice* supra 72 and 73.
[3109] *AmaBhungane v Minister of Justice* supra 74.
[3110] Para 6.11 of this chapter.
[3111] Chapters 2 and 3 of this study.
[3112] Chapter 5 of this study.
[3113] Para 7.3.3 of Chapter 7 of this study.
[3114] Para 7.6.3 of Chapter 7 of this study.
[3115] Sole S 'Surveillance: The silent spy on citizens and journalists faces court challenge' https://mg.co.za/article/2017-04-20-surveillance-silent-killer-of-journalism-and-democracy-1 (Date of use:5 April 2018). (Sole https://mg.co.za/article/2017-04-20-surveillance-silent-killer-of-journalism-and-democracy-1 (Date of use:5 April 2018); *AmaBhungane v Minister of Justice* supra 14 and 41.

international pressure group called EFF advocates that prior notice be dispatched to a target before an OCI is conducted,[3116] which defeats the purpose of the covert conduct of an OCI.

6.10.3 Intervening application by a vigilant target of online communication

Where an online communication user is vigilant or suspects 'through accident, coincidence or via a confidential source —without which it would be impossible to get any recourse'[3117] that an OCI will be, is being or has been conducted on him or her; such a user can rely on the provisions of the POPIA by requesting the LEAs or Online Communication Service Provider to supply such information.[3118] This submission is in pursuance of the common saying in the principle of equity, which states that equity aids the vigilant.[3119] It is further submitted that a vigilant target of an OCI must, in an intervening application and affidavit, show that the suspicion was not revealed to him or her by a LEA, LEO and OGA to guarantee the sanctity of the conduct of an OCI.

6.11 POPOOLA QUADRIPARTITE TECHNO-LEGAL ONLINE CRIMINAL INVESTIGATION APPLICATION PROTOCOL

The mode of presenting an OCI application to the court is obsolete[3120] and fraught with administrative bottlenecks. These bottlenecks range from inadequate appointment of a single designated judge to deficient logistics in daily transfer or transportation of paper or physical files to and from the court to the judge for adjudication.[3121] Some of these inadequacies take away the peculiar nature of judges working in secrecy in the conduct of an OCI, which is, to a

---

[3116] Fischer https://www.eff.org/deeplinks/2018/08/eff-amicus-brief-privacy-act-requires-fbi-delete-files-its-internet-speech (Date of use:10 August, 2018).

[3117] Right2Know at 5-6, 13-14 and 34 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[3118] Section 22 of the POPIA.

[3119] The Free Dictionary 'maxim' https://legal-dictionary.thefreedictionary.com/%22He+who+comes+into+equity+must+come+with+clean+hands.%22 (Date of use: 19 August, 2019).

[3120] The administrative officer attached to the interception judge physically transports the interception application to the judge, which could easily be done via a cell phone, the budget of which was approved but no funds to execute, JSCI Report at 20, 42 and 56. Given the fact that the method of crime commission changes, it is expected that the method of investigation should change, see art 27(3) and Forward page of TOCC at iii; O'Regan and McKaiser http://www.702.co.za/articles/379998/regulation-is-clear-information-contained-will-only-be-used-to-fight-covid-19 (Date of use:6 April 2020).

[3121] Interception equipment used by OIC was updated in 2002, JSCI Reports 2016 at 20, 21, 40, 46, 54, 55 and more particularly at 56; Parliament 'Annual Report of the Joint Standing Committee on Intelligence for the Financial Year ending 31 March 2017' at 4 and 10 (JSCI Report 2017); Hubbard, Brauti and Fenton *Wiretapping* 3-20.4a to 3-20.4c.

large extent, supposed to operate in secrecy, thus, the current practice turns an OCI court into another public court which generally exposes the *modus operandi* to the public since files are physically transferred to and from the court.[3122]

Some of the benefits of using an OCI are to conduct an investigation urgently and conveniently in terms of logistical advantage[3123] and obtain comprehensive information about a target in a short time, otherwise, the continued use of a physical and offline —paper-based— method of application in the conduct of an OCI in RICA regime defeats these purposes in the conduct of an OCI.[3124] However, as much as RICA provides for an oral application for the effective and efficient conduct of an OCI in deserving exceptional circumstances,[3125] ironically, RICA does not provide for an online method of application to conduct an OCI, which should inherently occur in an online communication-based form of investigation. What is 'claimed' to be provided in RICA —given that no such provision exists in RICA— is what is administered by the Office for the Control of Interception and Monitoring of Communications which in the offline world coordinates and processes the application submitted to and finalised by the designated judge.[3126]

The RICA regime enables the interception device to be configured in such a way that a LEO could unlawfully and unilaterally intercept a target without any technical caution or obstacle of proceeding further in an unlawful act in online communication. For example, the JSCI reveals that LEAs and LEOs install some grabber and other listening devices which by-pass the authorisation of a designated judge whereby facts are gathered within thirty-six hours of conducting an OCI.[3127]

Regrettably, thereafter, based on the information gathered from the grabber, a LEO presents an OCI application before the court with the unlawfully obtained information at hand to conduct an OCI and feigns to have the legitimate factual matrix in an OCI application.[3128] In some

[3122] *AmaBhungane v Minister of Justice* supra 39.
[3123] The convenience in this sense relates to the necessity principles in paras 6.5.2 - 6.5.7 of this chapter.
[3124] JSCI Reports 2016 at 20, 21, 54, 55 and more particularly at 56; JSCI 2017 at 4 and 10; Hubbard, Brauti and Fenton *Wiretapping* 3-20.4a to 3-20.4c.
[3125] Section 23 of RICA; Section 14 of HIPCAR *Interception of communication: 'Model policy guideline & legislative text* 2012.
[3126] JSCI Reports 2016 at 53.
[3127] JSCI Reports 2016 at 39 and 48.
[3128] JSCI Reports 2016 at 39; See also Jurgens and Savides 2015- 07-12 *Sunday Times* 1-2; Maphumulo 2016-08-30 *The Sunday Independent* at 1; Shaikh 2015-08-30 *The Sunday Independent* 3; Puren 2015-10- 29 *You* 136-

cases, the unlawfully obtained information from a grabber is used against a target, where such interception is privately conducted by a LEO for personal, retaliatory or witch-hunting purposes.[3129]

There are some developments in place to comply with societal demand in the conduct of an OCI. Such developments include the call by the JSCI for an electronic application in the conduct of an OCI (including the use of the mobile cellular telephone by Chief Registry Clerk and Administration Officer),[3130] the enhancement of pre-litigation practices to exchange o-mail communication and engagement in short telephonic judicial proceedings in the RSA.[3131] However, such proceedings are not provided for in RICA proceedings save in some other instances involving a Fixed Line Operator and the Office of the Interception Centre in the documentation and auditing purposes.[3132]

Nevertheless, international and foreign laws are positively responding to the development of technology to solve legal problems in their framework than RICA does. Firstly, the TOCC makes provision for video conferencing in its judicial proceedings (though a similar practice is done at the State of Capture Commission of Enquiry in the RSA), if a witness or victim cannot

137; Maphumulo 2015-11-03 *The Star* 2; Swart 28 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use:13 August 2016). Under the administration President G W Bush, he 'authorised the National Security Administration (NSA) to carry out warrantless electronic surveillance of international communications between persons in the U.S and other countries where the government suspected that at least one of the parties involved in the communication was a member of a terrorist organization. The surveillance was conducted outside the structures of FISA and without the approval of any court. The program remained a secret, however, until the New York Times disclosed its existence in 2005. Bush ultimately ended the TSP in 2007 in response to public pressure. A 2009 internal report by the inspectors general of the CIA, NSA and departments of Defense and Justice concluded that the program had resulted in ''unprecedented'' collection of data', Swire and Ahmad (eds.) *Introduction* 1, 13 and 14-15.

[3129] Swart H 'Secret state: How the government spies on you' https://mg.co.za/article/2011-10-14-secret-state/ (Date of use:12 December 2016 (Swart https://mg.co.za/article/2011-10-14-secret-state/ (Date of use:12 December 2016); JSCI Report 2016 at 40 and 41.

[3130] Although the request to have official mobile cellular telephones was made in in July 2013, however, as at December 2016, the request had not been granted, see JSCI Report 2016 at 20 and 56.

[3131] Drawing on the rationale in the case of *Pioneer Foods v CCMA* supra 17 and 48 to the urgency required to reach out to a party in a Con-Arb proceedings, it is submitted that where a CCMA commissioner placed a telephone call to a party in a Con-Arb proceedings in ADR to inquire about the absence of the representative of the party who explained what transpired for his absence and requested for postponement may amount to the hearing of an application in OCI proceedings; Wiese *ADR in SA* 123-124. Section 68(7)(d)(ii) of ECA. See also Kleve, De Mulder and Van Der Wees 1995 Vol. 4 No 1 *Computers & Artificial Intelligence* at 25-32. *Allen v Kirkinis* Case No. 20428/2014 para 51-52.

[3132] A FLO is expected to document and audit at all times receipt of an OCI directions from the OIC through a secure telefax or electronic signature in an encrypted email or other determinable messaging means agreed between the FLO and the IC, para 20 of Schedule A of RICA. Given the role of OIC, this means of communication is not required in the usual OCI procedure but where there is a petition that is handled by OIC which then requires the dispatch of a direction from the OCI to the FLO.

be heard physically by the judicial authority.[3133] Secondly, the CoE CoCC provides for the use of fax and o-mail only in an OCI application.[3134] Thirdly, in Canada, its judicial proceedings in the conduct of an OCI expressly allow the tele-warrant process, which is done through the use of fax messages only between a LEO and a judge.[3135]

In attempting to cure the defects in making an offline OCI application before the court in RICA, which is susceptible to and fraught with manipulations, compromises and unethical practices, this study conceptualises an OCI application practice and procedure, which is titled '*Popoola Quadripartite Techno-Legal Online Criminal Investigation'* ('*Popoola QOCI*') or '*unscripted* or *unwritten live* or *recorded telephone* or *audio-visual warrant*' protocol.

The process is executed through a complex interception device, which is techno-legally and specially designed and configured to suit the purpose it seeks to serve in this regard amongst the quadripartite namely: the LEAs, courts, Online Communication Service Providers and Interception Centre. Although other stakeholders play very important roles in the conduct of an OCI, however, an Authentication Service Provider, Cryptography Provider, Cyber Inspectors and Decryption Key Holder perform secondary technical and legal duties in the execution of an OCI.

Summarily, under *Popoola QOCI* protocol, the online application process for the conduct of an OCI is initiated with a verification process, which requires a LEO to apply online by logging into the interception device and producing an online technical communication code, token or clearance, as the first step in the application. Thereafter, the system sends a signal to the available designated judge(s) on duty, which simultaneously in some instances, serves as a pre-notice, and commencement of the hearing of an OCI application, without which an interception cannot proceed beyond this point.

In this type of configuration, a court can verify if an unlawful conduct of an OCI had already taken place before an official application is presented to the court.

[3133] Art 18(18) and 24(2)(b) and (4) of TOCC.
[3134] Art 25(3) of CoE CoCC.
[3135] Hubbard, Brauti and Fenton *Wiretapping* 3.20.4h. See para 6.11 of this chapter on the examination of the technical role of the court in 'tele-warrant' application and supervision.

The *Popoola QOCI* protocol, which operates in the following way, relies on the deployment of affordable, available and scalable devices, technologies, networks, applications and service. The *Popoola QOCI* protocol, which is developed from the general or ordinary use of multi-party video conference calls, 'WhatsApp' voice call and other similar technologies and systems —which include artificial intelligence such as machine learning technologies— is described as follows.

Firstly, as soon as the relevant 'reasonable ground' standard is established,[3136] a LEO requests and obtains a pin code from the interception device operated by an Online Communication Service Provider, and Interception Centre as the case may be,[3137] as the first technical step to initiate the conduct of an OCI in *Popoola QOCI* protocol. The device, technologies, networks, applications and services must be adequately safe and secure enough not to be intercepted and manipulated by unlawful interceptors such as the IMSI catchers.[3138]

Secondly, upon the technical satisfaction by the court, which must have received a signal that a LEA or LEO intends to make or is making an OCI application, the court grants a right of audience to the LEA or LEO, without which the court, LEO or anyone cannot technically proceed with the interception or application to intercept an online communication in *Popoola QOCI* protocol.

This stage requires or enables a LEA or LEO to have given a speedy and effective advance notice to the court on the administrative requirements of the application subject to the seriousness of an offence to be investigated. The consideration of a serious offence will include, for example, whether: there is a commission of a state of an emergency offence or an offence that poses an actual or potential national threat in the RSA,[3139] the effect of which may or may not be reversible. In the aforementioned specific instances only, it requires the consideration of at least, a minimum of three judges in a simultaneous adjudication; drawing on the Canadian law.[3140]

[3136] Paragraphs 6.4- 6.8 of this chapter.
[3137] See paras 6.2.2 – 6.2.6 of this chapter where some interceptions of online communication do not need a court order.
[3138] Swart 11-13 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use:13 August 2016).
[3139] See s 16(5)(a)(ii) and (iii) of RICA; Paragraphs 6.4.5, 6.4.6.1 and 6.4.6.2 of this chapter.
[3140] See relevant or similar provision in the US in ss 1801(a), (b), (c), (f) & (j), 1803 (a), (b) & (c), 1804, 1881A(a), (i)(3) & (c)(2), 1881B(d) & 1881D of 50 U.S.C.; Jimenez A (ed.) *Wiretapping* 59 and 64-66.

Thirdly, at the end of the *Popoola QOCI* proceedings, the court makes an order either approving or declining an OCI application. Regardless of the outcome of the OCI application, the judge —or court— inputs a pin code on the interception system, which instructs or informs the Online Communication Service Provider and Interception Centre of the outcome of the application by automatically acting or omitting to act.[3141]

In proceeding with the outcome of the *Popoola QOCI* protocol, several pin codes, which are techno-legally defined and configured, will be used to gain access to execute the outcome of the application according to the command configured in the codes.[3142]

Amongst the *several techno-legal principles* examined in this study and *other emerging cyber law principles* —which are *not extensively addressed* in this study due to the *delimitation rule* but very relevant to *Popoola QOCI* protocol— from which the codes are developed, derived or interpreted, the codes in *Popoola QOCI* protocol will include the following: intermittent OCI, which basically means that an OCI is conducted for two or three minutes and switched off for a minute while an OCI continues thereafter for same two minutes and so on, subject to the seriousness of an offence;[3143] 'OCI rejected', which may mean an outright rejection of the conduct of an OCI. Other codes are: OCI with caution'; 'absolute OCI', which may focus on bulk targets; 'partial OCI', which may stipulate that an OCI be conducted alongside non-OCI processes; 'delayed OCI' which will state when an OCI may commence; 'identity OCI'; 'content OCI'; 'meta OCI'; 'traffic OCI'; 'international OCI'; 'roaming OCI'; 'terrorist OCI'; 'professional communication OCI'; 'terrorist OCI', etc.

Fourthly, the outcome of the court is not activated until the LEO inserts the code generated by the interception device and given by the court in the *Popoola QOCI* protocol. It is only at this stage that a LEO would be able to conduct an OCI in online communication. It is noted that this study opposes the power granted to the Office of the Interception Centre as the interceptor in the RSA.[3144]

[3141] The role of the court can be likened to the provision of art 31(3)(e) of African Union Convention on Cyber Security and Personal Data Protection ('AUCCSPDA').

[3142] Regulation 4.5 of Schedule C of RICA.

[3143] *United States v Mansoori* No 99-1492 (7th Cir. 08/29/2002) para 27, Hubbard, Brauti and Fenton *Wiretapping* 4-43 to 4-44; Para 3.5.7.8 of Chapter 3 of this study.

[3144] Parliament of the Republic of South Africa 'Announcement, Tablings and Committee Reports' No 164 -2016 at 19 and 22; Para 7.6.3 of Chapter 7 of this study.

The *Popoola QOCI* protocol compellingly requires that LEOs, judges at all levels, court administrators in this regard, Online Communication Service Providers and members of the Interception Centre should have adequate certified knowledge or training in information and communication technology and the law regulating it before they can participate in the conduct of an OCI.[3145] The quadripartite process makes each role player dependent on each other to ensure the effective application of the principles of separation of powers and checks and balances in the conduct of an OCI.[3146]

However, in some interceptions that do not require interception direction from the court in sections 4, 5, 6, 7, 8, 9, 10 and 11 of RICA,[3147] a different protocol is developed which is different from the above recommended *Popoola QOCI* protocol. This is because of the nature of expediency in such instances, which form the exceptions to the tele-warrant application procedure, enable LEOs to apply straight to the Online Communication Service Provider or the Interception Centre for the interception.

Finally, although this study simplifies the obsolete application, hearing and execution processes of an OCI in the RSA, however, the design, configuration, development and deployment of *Popoola QOCI* protocol must be conducted with utmost care to prevent unnecessary, humongous and irreparable techno-legal liabilities in these processes. This caveat is due —largely and more importantly— to the complex and fluid nature and features of the emerging cyber law philosophy that this author has experientially considered in this proposal.

[3145] *Interscope v Duty* (05-CV-3744 PHX-FJM, D Ariz, 14 April 2006); *State v Miller* supra 38; *S v Terrence Brown* para 29; Section 180 (a) and (c) of the Constitution and art 29 of TOCC make provision for training programmes and technical assistance for judicial officers and the participation of non-judicial officers in the administration of justice including the *prevention*, *detection* and control of crime relating to the *methods of investigation*, *collection of evidence*, *methods used* at *free trade zones* and *ports*. Cyberlaw or criminal cyber law authors do not have knowledge or good knowledge in technologies, art 10 of Trafficking in Persons (TIP) *Annex II* of TOCC before applying the law in cyberspace, Koops and Goodwin 5/2016 83 *Tilburg Law School Research Paper* 44; Blackman and Srivastava (eds) *Telecommunication regulation handbook* 20. Relying on art 15(4) of UNODC 'Model Legislative provisions against organised crime 2012 which requires that infiltrators should be specially trained and designated, similar principle is necessary for all categories of LEAs conducting an OCI. Para 4.6 of Chapter 4 of this study.

[3146] Para 4.5 of Chapter 4 of this study.

[3147] Para 6.2.2 – 6.2.6 of this study.

6.12 RECOGNITION OF THE APPLICATION OF SECTION 205 OF THE CRIMINAL PROCEDURE ACT AND OTHER LAWS IN ONLINE CRIMINAL INVESTIGATION

Sections 15 and 59 of RICA recognise the conduct of an OCI under other laws on a non-ongoing basis[3148] in sections 17 and 19 of RICA only, which relate to the application for and issuance of direction in real-time and archived online communication. One such law which RICA recognises is section 205(1) of the CPA,[3149] which has been correspondingly applied in many instances by a magistrate —instead of a judge in RICA— in lieu of the general and more detailed provisions of RICA in conducting an OCI[3150] in respect of disclosure of meta data by a telecommunication service provider.[3151]

The proviso in section 205(1) of the CPA stipulates that where, before a court proceeding, a person supplies information to the court on the commission of an offence, the NPA has the right, power, and mandate to conduct a prosecutorial pre-trial investigation and tender such evidence in court in the absence of such a person who has made or obtained the statement. In the section 205 application, LEAs or LEOs bypass the judge by filing an OCI application in the Magistrate Court.[3152]

Although the Constitutional Court has declared that the application of section 205(1) of the CPA is consistent with the Constitution to conduct a preliminary investigation pursuant to section 35 of the Constitution,[3153] however, it is submitted that section 205(1) is defective or inadequate concerning the philosophy of RICA. Section 205(1) does not comply with the significant import of the substantive and procedural requirements in RICA —being the main

[3148] Section 15(2) of RICA.
[3149] See also the application of sections 81, 82(3) and (4), 83 and Chapter XII of ECTA in relation to the conduct of OCI; Basdeo 2012 2 *SACJ* 206.
[3150] See also the application of sections 81, 82(3) and (4), 83 and Chapter XII of ECTA in relation to the conduct of OCI; Basdeo 2012 2 *SACJ* 206. Section 205 of CPA; Right2Know 35 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).
[3151] Right2Know at 4 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).
[3152] Right2Know 35 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).
[3153] *Nel v Le Roux No & Others* Case No: CCT 30/95 paras 4, 6, 7, 8, 9, 10, 11, 14, 25 and 27 (*Nel*); *Haysom v Additional Magistrate, Cape Town and another* 1979(3) SA 155 (C) (*Haysom*) and *State v Matisonn* supra 302.

and authoritative law— which regulates the conduct of OCI in the RSA.[3154] Chief amongst the requirements in which the provisions of the CPA do not comply with RICA provisions is section 16(2)(e) and (5)(b) and (c) which requires that an OCI be conducted as an alternative method of investigation and not as a method of investigation in the first instance, save where certain exceptions apply thereto.

It is also claimed by some investigative journalists that RICA does not prohibit Online Communication Service Provider from issuing out a notice to target after the conduct of an OCI under section 205 of the CPA.[3155]

Aside from the suggestion that the NPA should be disqualified from primarily conducting an OCI because of conflict of interest of combining the functions of investigation and prosecution, which contravene the principle of separation of powers,[3156] section 205(1) of the CPA has been erroneously applied by NPA in conducting an OCI. In the case of *State v Naidoo*, an employee of an Online Communication Service Provider intercepted an online communication without an order of the court, believing it was lawful to do so simply because a LEO approached the employee to furnish the information.[3157] In an unreported case relayed by R2K of a bribe of R 3, 750, an MTN employee —who is now being tried in a Magistrate Court— supplied the phone records of a subscriber to a private investigator who is a former HAWKS employee.[3158]

Furthermore, although the OPP —a Chapter Nine Institution— revealed the location traffic data of some individuals accused of visiting the residence of the Gupta family in the State of Capture Report,[3159] the OPP must have relied on section 205(1) of the CPA to obtain this data through the NPA. This is because the OPP is not one of the applicants directly recognised to conduct an OCI in RICA. It is noted that the report does not refer to NPA as the source of this

[3154] Right2Know 4, 16, 35 and 39 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[3155] Right2Know 38-39 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[3156] Para 4.2 of Chapter 4 of this study.

[3157] *State v Naidoo* supra 521 B-E.

[3158] Right2Know 16 and 18-19 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018). In other instances, text messages and mobile cellular telephone billing records are obtained for personal reasons and benefits through a contact at CI-SAPS or Online Communication Service Provider, JSCI Reports 2016 at 39, 40 and 41.

[3159] Office of the Public Protector *State of capture report* No. 6 of 2016/17 at 84-85, para 5.21 at 99, para 5.22 at 100, para 5.23 at 100-104, para 5.24 at 104 – 106, para 5.96 at 122, para 5.97 at 122, para 5.98 at 123, para 5.100 at 123, para 5.101 at 124, 301, para (aa) at 301, paras (bb) – (cc) at 301-302 and paras (dd) - (ff) at 302-303 www.publicprotector.org (Date of use:15 October 2016) (OPP *State of capture report*).

information, thus raises questions on the methodology of information gathered by the OPP in the Report.

In summary, the provisions of RICA which are meant to strike a balance between the protection of the right to the SOC and the conduct of an OCI are rendered ineffective by the application of section 205(1) of the CPA, given that LEOs now resort to section 205(1) as a short-cut in the procedure in RICA or resort to an unethically preferred way of conducting an OCI.[3160]

However, although media reports say that section 205 be abolished because of its abuse and inadequate oversight,[3161] this study alternatively proposes that section 205(1) of CPA be amended[3162] to the effect that its provision complies with the provisions of RICA, being the main legislation that regulates the conduct of an OCI or the provision of section 205(1) is restricted to the gathering of offline evidence only.

6.13 APPLICATION FOR ONLINE CRIMINAL INVESTIGATION OF MASS TARGETS

A bulk or mass OCI is drawn on the offline concept of mass surveillance, which does not pose the same risk as the former does. Scholars have acknowledged that in the wake of technological development in contemporary society, we are in the precarious eon of 'wholesale surveillance'[3163] or bulk or mass interception and monitoring. This scenario occurs where there is an invasion of the right to the SOC of content and non-content data of an unknown or undetermined number of people in a group or team —of any form of identification or classification ranging from gender, status, belief, orientation to professionals— who may not be specifically identified before mass surveillance is conducted in geographical or non-geographic instances.

[3160] *State v Naidoo* supra 485 A-C, 516D-517D, 521A-J, 531C-J; *State v Agliotti* supra 135-137 and 146.1; *State v Miller* supra 15-26, 33, 34; *S v de Vries* supra 613**.** Parliamentary Committee No 164-2016 at 40; Swart https://www.msn.com/en-za/news/techandscience/your-cellphone-records-and-the-law-the-legal-loophole-that-lets-state-spying-run-rampant/ar-AAxyCpM?ocid=spartandhp (Date of use: 20 May 2018); Date of use: 27 November 2018) Hunter and Smith at 4 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use : 27 November 2018).

[3161] Right2Know at 35 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[3162] Basdeo 2012 2 *SACJ* 206.

[3163] Vlahos *Surveillance society: New high-tech cameras are watching you* 98.

In one of the descriptions of bulk or mass interception, it is an international technical acceptable practice where LEAs or LEOs insert cue or key phrases or words to carry out surveillance on international transactions involving South African residents in the RSA who use servers that are located outside the RSA,[3164] the use of which constitutes a great controversy in this study, though resolved in favour of the RSA.[3165]

RICA does not provide for the practice of bulk or mass OCI conduct generally[3166] or even in the statutes, neither is it regulated in some foreign jurisdictions.[3167] In *AmaBhugane*, the court held that it is erroneous to assume that the powers of SSA, SANDF and CI-SAPS in section 2A(5) of the NSIA is to conduct a mass OCI under the guise of carrying out a security clearance.[3168] Instead of conducting a mass OCI for security clearance purposes, a targeted OCI —the conduct of which must comply with the provisions of RICA as canvassed in this study for 'this limited purpose'— may be conducted for purposes of vetting people for security clearance.[3169] The court further held that it is erroneous to interpret that the provisions of section 2(2)(b)(i),(ii) and (iii) of the NSIA were meant to ward off any form of online communication insecurity and not meant to imply mass conduct of an OCI.[3170]

Historically, most of the use of mass surveillance started with the private sector, banks, insurance companies and communication entities, amongst others who conduct data mining on individuals for purposes of fraud detection by credit card companies, directing advertisements, purchase preferences or profiling individuals due to Internet sites visited by users, amongst others, with some much information gathered incomparable to that of an old dictator.[3171] Thus, although the intent for which surveillance is carried out is important, but there is no doubt that it may be wrongly used to harm an individual.[3172] Save in section 6 of RICA where a private or commercial entity records its online communication with its customers and other relevant

[3164] *AmaBhungane v Minister of Justice* supra 143, 144 and 145.
[3165] Para 2.8 of Chapter 2 of this study where this study strongly condemns the U.S. principle of 'no server, no law' upon which bulk surveillance is practised in this regard.
[3166] Right2Know at 8 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018); *AmaBhungane v Minister of Justice* supra 146 and 162-163.
[3167] Hubbard, Brauti and Fenton *Wiretapping* 4-42.1 to 4-42.2.
[3168] *AmaBhungane v Minister of Justice* supra 150-156.
[3169] *AmaBhungane v Minister of Justice* supra 150-156.
[3170] *AmaBhungane v Minister of Justice* supra 157-163.
[3171] Swire and Ahmad (eds.) *Introduction* 14-15; The Economist *Learning to live with big brother* 23.
[3172] Swire and Ahmad (eds.) *Introduction* 2-3.

instances propounded in this study,[3173] private entities are prohibited from intercepting an online communication in the RSA.

Governments —through the LEAs or LEOs— are more involved in mass surveillance in the contemporary society especially in the unpredictable age of global absolutism, extremism and terrorism, which compel governments worldwide —including the RSA— to desperately act proactively on anticipated attacks by profiling individuals.[3174] In the RSA, the NCC, which is under the control and management of SSA, conducts mass international incoming and outgoing communication surveillance,[3175] which is not recognised or regulated under any law in the RSA as one of the LEAs in RICA or other law, thus their activities and interceptions have been declared unlawful and invalid in *AmaBhugane*.[3176]

In addition, the bulk interception of online communication during the State Of the Nation Address ('SONA') at the National Assembly of South Africa was condemned by the court in *Primemedia v Speaker, National Assembly* where the state security agencies jammed the online communications of individuals and broadcasters attending and covering the SONA event.[3177] For these reasons, the media in the RSA is demanding that the mass interception should be abolished or be strictly regulated because it does not target anyone but everyone for investigation.[3178]

The United Nations has not only condemned the RSA on the conduct of mass interception,[3179] but other foreign jurisdictions have also been criticised by scholars and courts in this regard.

[3173] Paras 2.11.3 - 2.11.6 and 6.2 of this study.
[3174] The Economist *Learning to live with big brother* 26.
[3175] Para 2.10 of Chapter 2 of this study.
[3176] *AmaBhungane v Minister of Justice* case supra 165; Notice of Motion in *AmaBhungane v Minister of Justice* supra 1.6; Swart https://mg.co.za/article/2011-10-14-secret-state/ (Date of use:12 December 2016); Pillay V '13 reasons you should be very worried about your government spying on you' http://www.huffingtonpost.co.za/2016/12/22/13-reasons-you-should-be-very-worried-about-your-government-spyi_a_21633335/ (Date of use: 2 January 2017) (Pillay http://www.huffingtonpost.co.za/2016/12/22/13-reasons-you-should-be-very-worried-about-your-government-spyi_a_21633335/ (Date of use: 2 January 2017).
[3177] *Primemedia v Speaker, National Assembly* supra 84(1)-(4); Para 6.2.5 of this chapter.
[3178] Right2Know 35 and 36 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).
[3179] United Nations 'Concluding observations on the initial report of South Africa' CCPR/C/ZAF/ CO/1 para 42 at 8 https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fZAF%2fCO%2f1&Lang=en (Date of use:18 January 2019) (United Nations para 42 at 8 https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fZAF%2fCO%2f1&Lang=en (Date of use:18 January 2019); Michalson ' United Nations concerned about

Although the National Security Agency in the U.S. gathers more than 1.7 billion of all types of online communications each day to be proactive in crime detection,[3180] it is believed by some scholars that the gathering of the enormous information is overwhelming.

This is because the more LEAs are empowered to generally carry out mass surveillance on innocent people, the more time is wasted and the less crime is detected,[3181] the more insecure the society becomes[3182] and the more LEAs become paranoid because they will want to listen to everybody, which is not possible.[3183] This is because the trade-off of the right to the SOC for mass surveillance is not an automatic guarantee for security, since mass surveillance is in itself a 'major source of insecurity.'[3184]

In Canada, the Supreme Court of Canada observed in *R v Taylor* that should a court ask LEAs to conduct live monitoring of all online communications, one will be asking for too much from LEOs because of the frailties or complexity involved in live online communication monitoring as well as the inability of LEOs whose knowledge of the law cannot be compared with lawyers.[3185] However, mass interception is all now subject to the deployment of AI which largely and generally makes the impossible functions reasonably possible and in some cases, substantially possible, the function or output of which is close to perfection in identifying the commission of some offences.[3186]

Although mass surveillance may be conducted in non-judicial circumstances which do not

privacy and interception in South Africa' https://www.michalsons.com/blog/un-human-rights-committee-concerned-about-privacy-and-interc (Date of use:18 January 2019) (Michalson https://www.michalsons.com/blog/un-human-rights-committee-concerned-about-privacy-and-interc (Date of use: 18 January 2019); Swire and Ahmad (eds.) *Introduction* 14-15.

[3180] Greenwald G 'The digital surveillance state: Vast, secret, and dangerous' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 41 (Greenwald *Digital surveillance state: Vast, secret, and dangerous*); Vlahos *Surveillance society: New high-tech cameras are watching you* 97.

[3181] *Greenwald Digital surveillance state: Vast, secret, and dangerous* 14 and 41-42.

[3182] *Greenwald Digital surveillance state: Vast, secret, and dangerous* 41.

[3183] Right2Know 18-19 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[3184] *Greenwald Digital surveillance state: Vast, secret, and dangerous* 41-43.

[3185] The court in *R v Taylor* (1998) 121 C.C.C (3d) 353 para 18 referred to the earlier held decisions in *R v Thompson* [1990] 2 S.C.R 1111 at 1137 and 1138 or 59 C.C.C (3d) 225 and *R v Garafoli* [1990] 2 S.C.R 1421 at 1468 or 60 C.C.C (3d) 161, Hubbard, Brauti and Fenton *Wiretapping* para 4.4.1 at page 4-42.1 to 4-43.

[3186] Paras 2.11.4 and 6.4.9 of this study.

require a court direction before surveillance takes place,[3187] however, the compulsory conduct of a mass, bulk, blanket or passive OCI on the public, is, in other circumstances, illegal because no OCI application is made nor an OCI direction obtained from the court by LEAs as required in RICA.[3188]

Having earlier examined the non-judicial direction interception,[3189] the compulsorily inclined mass conduct of an OCI occurs in many circumstances where it is extremely difficult, if not impossible, to obtain information about a specific suspected individual in the environment, group, identity or team where there is a commission of an offence because great urgency is required by LEAs to prevent or control the commission of an offence or the spread of a pandemic disease such as the coronavirus, the effect of which is absolutely irreversible.[3190]

Some of the instances where there is compulsory conduct of mass OCI include amongst others: firstly, in an automatically or a robotically controlled OCI environment in any mechanically moving or stable object in the air, sea or on surfaced land, which is submerged by water, soil, dangerous wind or any other artificial or natural substance or disaster that poses same or similar risk in the air or sea;[3191] secondly, arguably and reasonably in a non-automatically controlled OCI environment involving users of online communication who are in an extreme combatant, militant, riotous and violent situation leading to the commission of a serious offence, the effect of which is absolutely irreversible; and thirdly, in geographical and non-geographical circumstances where a wind of the commission of a serious crime was discovered before the commission of the offence, the planning of which is monitored before the execution of the plan of the common-purpose to commit a serious crime.[3192]

[3187] Para 6.2.4 of this chapter. See sections 4, 5, 6, 7, 8, 9, 10 and 11 of RICA. It noted that s 9 requires some qualification involving privileged professional communication in correctional services facility, see para 6.15 of this chapter on the examination of this issue.

[3188] Mare and Duncan 11-13, 29, 30, 32 and 38 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf (Date of use:1 December, 2017); JSCI Report 2016 at 20- 21**;** Swart 2-5, 10-12, 19 and 20 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use: 13 August 2016).

[3189] Para 6.2.4 of this chapter.

[3190] Paras 6.2.4 and 6.3.3.4 of this chapter.

[3191] Paras 2.11.3 and 2.11.4 of Chapter 2 of this study and para 6.4.9 of this chapter.

[3192] *SABC v Thatcher* Case No: 8924/2004 paras 11; *Thatcher v Minister of Justice and Constitutional Development and Others* 2005 (4) SA 543 (C); [2005] 1 All SA 373 (C).

Mass OCI applies in the judgement in *State v Miller* where it is observed that every application made to obtain cell phone records under section 205 of the CPA was made in an OCI application involving many people.[3193] It is noted that section 205 does not fully comply with the requirements in RICA which is the main law in the conduct of an OCI.[3194]

Although mass online surveillance can be used to predict the criminal behavioural pattern of a group, however, its outcome is 'incredibly inaccurate' because there may not be any specific relevant factual matrix to link or establish the commission of an offence to or against each individual in the group for which an OCI is conducted.[3195] Save where there are CCTV or similar spontaneous video or audio monitoring systems, finding someone in an online communication tower is not a sufficient reasonable ground to arrest someone in the area of the murder scene[3196] because there is no further or specific proof that someone found in a tower is responsible for the commission of a serious offence,[3197] save where there is a disaster like the coronavirus pandemic.[3198] This is because there are many reasons that could necessitate some to be at a particular place since the right to freedom of movement is guaranteed.[3199]

Thus, the foregoing discussion generally highlights the difficulty of establishing the relevant reasonable ground standard to prove the commission of an offence in a mass OCI application against individuals.[3200] In sum, the overall relevant standard of proof to be considered by the court in an application to make the conduct of a mass OCI legal is set out in section 16(5)(a)(ii) and (iii) of RICA which includes and relates to whether the commission of a serious offence constitutes a state of emergency or an offence that poses actual or potential risks to the State or public health or safety,[3201] the effect of the commission of which offence is absolutely irreversible.[3202]

[3193] *State v Miller* supra 34.
[3194] Para 6.12 of this chapter.
[3195] The Economist *Learning to live with big brother* 26.
[3196] Cassilly *Geolocational Privacy and Surveillance Act* 267.
[3197] However, there is a reasonable conclusion to be made where there is a court order restraining the movement of an accused or convicted person who has been placed under some conditions for further investigation or custodial sentence where there is online communication device attached to the place, see paras 2.3 and 2.11.4.2 of Chapter 2 of this study.
[3198] Para 6.2.4 of this chapter.
[3199] Paras 2.3 and 2.11.4 of Chapter 2 of this study.
[3200] Paras 6.4 - 6.6 of this chapter.
[3201] Paras 6.3.3.2 - 6.3.3.5 and 6.4 - 6.6 of this chapter.
[3202] Para 6.3.3.4 of this chapter.

Although it is submitted that the mass conduct of an OCI is unlawful because of the absence of a regime that regulates it in the RSA, however, *inter alia*, a panel of three judges[3203] *only* should consider the conduct of a mass OCI in a single *Popoola QOCI* protocol[3204] and be mandated to issue a proportionate bulk GLT and non-GLT[3205] OCI direction in the offences aforementioned.[3206]

It is further argued that should the use of section 205 of the CPA be considered while considering mass conduct of an OCI, it should be sparingly applied because of the shortcomings of section 205.[3207] The precedent has shown that section 205(1) of the CPA application has been abused because it is seen as a short-cut or a 'rubber stamp' to conduct a mass OCI, which applies independent of the substantive and procedural requirements in section 16(2)(e) and (5)(b) of RICA.[3208]

6.14 RIGHT OF AN INNOCENT OR THIRD PARTY IN THE CONDUCT OF ONLINE CRIMINAL INVESTIGATION

As opposed to offline privacy which largely protects the third party right in an offline investigation, some lacuna exists in RICA because of the non-existence of the techno-legal configuration, operation and regulation of online communications respectively. The latter does not make provision for the divisibility of online communication that will exempt an innocent or third party in the conduct of an OCI where such third party is not a suspect in the commission of a serious offence.[3209]

[3203] Swart https://mg.co.za/article/2011-10-14-secret-state/ (Date of use: 12 December 2016); Hubbard, Brauti and Fenton *Wiretapping* 3-20.1 to 3-20.2 and 3-25.

[3204] Para 6.11 of this chapter. Although the pronouncement of the court in *State v Miller* supra 34 was earlier in this rubric referred to as unreasonable, however, it is herein cited as a recommendation in the conduct of an OCI. This is because there are two major differences between *State v Miller* supra 34 and the recommendation in this regard. In *State v Miller*, a magistrate presided over the pronouncement of a mass OCI conduct under section 205 of the CPA, while in this study, it is strongly argued that three judges must preside over the application for the conduct of a mass OCI under RICA, which is the main law, which considers other principles in the conduct of an OCI, as opposed to the CPA, which may not favourably consider the vital principles in RICA as examined in paras 6.4 - 6.6 of this chapter.

[3205] See para 2.8.3.3(a) of Chapter 2 of this study on the workability of GLT. In *State v Pillay* supra 427 G-J and *State v Naidoo* supra 485 A-B, the use of GLT assisted in obtaining information about the armed robbers since they used cellular telephones during the operation. See also para 2.6.2.1 of Chapter 2 of this study.

[3206] Paras 6.3.3.2 – 6.3.3.5 and 6.4 and 6.5 of this chapter.

[3207] Para 6.12 of this chapter.

[3208] Para 6.12 of this chapter. *State v Naidoo* supra 485 A-C, 516D-517D, 521A-J, 531C-J; *State v Agliotti* supra 136 and 146.1; *State v Miller* supra 15-26, 33 and 34; *S v de Vries* supra 613; Parliament 'Committee Report' No 164-2016 40.

[3209] Paras 2.3.1, 2.3.2, 2.3.3, 3.5.7.3, 3.5.7.6, 3.5.7.8 and 3.5.7.12 of this study.

Similarly, Canadian law allows the conduct of an OCI of a third party whose identity is not known and who is not a subject of the conduct of an OCI in either general or mass interception. However, the law does not exonerate a party whose interception of communication 'may afford evidence' in the commission of a serious offence by a target, which still invades the online communication of such third party.[3210]

In addition to the fact that the right of a third party is more protected in offline privacy than online privacy when an investigation is being conducted,[3211] a controversy on the protection of a third party in an online communication came to the fore in the Supreme Court Appeal in *Mngomezulu v NDPP*. In this case, a party complained about his name being included in an OCI direction which resulted in the conduct of an OCI of his online communication although his name was not on the list of drug dealers listed for investigation.[3212]

The case of *Mngomezulu v NDPP* highlights some of the instances of the breach of the right to the SOC of a third party in an online communication in which RICA does not make provision for the techno-legal protection of the right to the SOC of a third party when LEAs conduct an OCI of online communication,[3213] therefore, the following is recommended:

Firstly, any online communication number or identity in which an OCI would be conducted on should have been verified with the Telecommunication Service Provider to ensure that a third-party right is not infringed in accordance with RICA provisions even where such number is used by a proxy or in equity, otherwise, the essence of registration and keeping the records of users of mobile telephone telecommunication would be defeated;[3214]

Secondly, an affirmation that such verification of a third-party identity or right was conducted must be stated by the LEO in the affidavit in support of the application for an OCI;

[3210] *R v Chesson* (1988) 43 C.C.C (3d) 353, [1988] 2 S.C.R 148 paras 70-73; *R v Chow* [2005] 1 S.C.R. 384 para 34; Hubbard, Brauti and Fenton *Wiretapping* 4-2.6 to 4.2.8 to 4-2.8a and 4-2.14a.

[3211] Para 3.5.7.12 of Chapter 3 of this study.

[3212] *Mngomezulu v NDPP* [2007] SCA 129 (RSA) para 6.

[3213] Section 16(2)(a)(ii) & (d)(ii) of RICA; Para 3.5.7.12 of Chapter 3 of this study.

[3214] Sections 40(2), 62(6) and 62C of RICA; Paragraphs 3.9.4 and 7.3.5 of this study. De Vos P 'RICA: Is it unconstitutional?' https://constitutionallyspeaking.co.za/rica-is-it-unconstitutional/(Date of use: 12 June 2016).

Thirdly, relying on the two-minute duration of conducting an OCI,[3215] an innocent party may be a victim of the breach of the right to the SOC for this period in real-time communication, while in the case of an archived communication, the two-minute duration does not apply because the entire content is in the possession of the Online Communication Service Providers. Therefore the timing does not have any or much significance in terms of the duration needed to copy the content in an archived communication. In the contemporary society, it is imperative to design, develop and deploy an AI application that separates data in online communication.[3216] This application enables both the Online Communication Service Provider and the Interception Centre deploy a software application in the real-time and archived communication that will decipher and sift the irrelevant or key facts in the facts relating to the commission of a serious offence that is being investigated.

The deployment of an AI application attempts to exclude the communication of a third party. The use of AI (more particularly ML) helps to give the direction of the investigation, given that the relevant reasonable standard would have given a direction on the key words to watch out for, even where words may be deceptively coded by parties in communication. However, the findings may not be conclusive due to the indeterminability of the intended meaning of words used in communication.

One of the solutions to a deceptive coding in online communication is to simultaneously complement it with offline investigations in the conduct of an OCI by listening to the offline codes being used in the general public so that same codes are inserted into the AI-driven interception devices to assist in the conduct of an OCI.

In summary, it is submitted that an innocent or a third-party right be protected by ensuring that a LEO 'must take all reasonable steps to minimise the impact of' the conduct of an OCI on third parties[3217] who do not have any direct or indirect link or bearing in the commission of the serious offence that is being investigated in a non-privileged communication in some ways.

[3215] Para 3.5.7.8 of Chapter 3 of this study.
[3216] Paras 3.5.7.3, 3.5.7.6 and 3.5.7.8 of Chapter 3 of this study.
[3217] Section 17(3) of HIPCAR *Interception of communication: 'Model policy guideline & legislative text* 2012.

6.15 RIGHT IN A PRIVILEGED ONLINE COMMUNICATION IN THE CONDUCT OF ONLINE CRIMINAL INVESTIGATION

6.15.1 Setting the scene for the general protection of privileged online communication between a professional and non-professional

The concept of privileged communication, which is derived from the broad right to privacy.[3218] In recent time, the concept is premised on the position of Mathews who —in 1983— opined that there was a critical need to regard as secret the offline communication between a client and a lawyer; a patient and a doctor and a journalist —as an institution— and an informer, otherwise, it will be difficult, if not impossible, for these parties to function effectively if there was no legal guarantee that such communication will be a secret.[3219]

The literature on privileged communication between a lawyer and client will be preferred under this rubric because of the developed literature in this regard. However, this rubric reasonably applies to other similar or relevant privileged offline communications where there is a legal or professional expectation or a practice of utmost trust or fiduciary relationship between two parties, namely a professional and a non-professional who are donating and receiving a service respectively.[3220] Therefore, the philo1sophy of privileged communication between a journalist and an informer is relatively applied in this rubric aside from its thorough examination too.[3221]

The right to privileged online communication between an attorney and a client, on the one hand, and a journalist and an informer, on the other hand, is not protected by RICA.[3222] Nonetheless, the case of *AmaBhugane* has laid to rest the old law that rejected the protection of privileged offline communication between a journalist and an informer by establishing, and broadening the scope of protection of online privileged communication to include both an

[3218] Strauss *Legal professional privilege* 33.

[3219] Mathews *State secrecy* 36. It is noted that this study regards the work of an 'investigative journalist' as a public utility because journalism is the fourth realm or government in a democratic society as opposed to the private utility perspective that is found in client and lawyer and patient and doctor relationship because of the private trust interest that is served; *AmaBhungane v Minister of Justice* supra 109- 140.

[3220] Relationship with professionals include other professionals such as banker-client relationship and accountant-client relationships.

[3221] Privileged communication between a journalist and an informer is examined in this chapter, para 6.15.3 of this chapter.

[3222] Right2Know at 8 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

attorney and a client and an investigative journalist and an informer.[3223] In EU, an online communication —including telephone calls between a lawyer and a client— is guaranteed in art 8 of ECHR which should be regulated as a professional secret.[3224]

Section 5 of RICA, which deals with the interception of online communication with consent, is yet to be tested in court. However, some journalists submit that where a general consent is granted to intercept online communication, which 'inadvertently intercepts communications that are privileged', there is a breach of the rights to the SOC and fair hearing which will consider the circumstances surrounding the breach, including the parameters of the grant of the written consent and justifiability of the breach of the right.[3225]

Arguably, in section 86 of the POPIA which substantially regulates offline communication, only privileged offline communication between a client and an attorney is protected in the context of such communication being searched and seized as opposed to the online interception of privileged online communication between a client and an attorney which is not protected in the POPIA nor in RICA or any other law in the RSA. This is because, despite the definition of 'electronic communication' in the POPIA,[3226] the strict use of the term 'communication' or the exclusion of the term 'electronic communication'[3227] in section 86 confirms the absence of protection of privileged online communication between an attorney and a client, the privilege of which is difficult to determine, given the complexity and delicacy of online communication.

This confirmation further buttresses the earlier submissions which identify an offline communication as the main object of the protection in the POPIA as opposed to online communication, which is grossly and inadequately protected in the POPIA.[3228]

Worse still, in another vein, the POPIA is not only deficient in its scope in failing to cover online communication in relation to this study, but it is also inadequate in terms of its implementation by law professionals who are supposed to be ministers in the temple of justice. It is on record and ironic that lawyers who are not adequately equipped to implement the

[3223] *AmaBhungane v Minister of Justice* supra 109-140.
[3224] See Dirk Van Gerven 'Professional secrecy in Europe' in The Bar of the Brussels *Professional Secrecy of Lawyers in Europe* (2013) 1-23 (more particularly at 17 where Phone Tapping is discussed).
[3225] Luck R 'RICA' at 2 http://www.saflii.org/za/journals/DEREBUS/2014/6.html (Date of use: 27 June 2019.
[3226] Section 1 of the POPIA.
[3227] Online communication is a subset of electronic communication, para 2.2.1 of Chapter 2 of this study.
[3228] Paras 3.5.6.5 and 3.5.6.7 of Chapter 3 of this study.

provisions of the POPIA which deal with offline privacy[3229] are placed in a position to educate their clients in this regard concerning the provision of some education on the protection of privileged communication between a lawyer and a client. Consequently, lawyers are not equipped with the knowledge of privileged online communication between a client and a lawyer.

The privilege of secrecy in a privileged offline communication does not belong to the lawyer but is bestowed on the client, litigant or witness who is in search of help from the professional,[3230] the principle of which is same or similar to privileged online communication.[3231] Whether in or out of court in the modern lawyer-client privileged communication, there is an ethical duty of secrecy expected of a lawyer from voluntarily or compulsorily disclosing a privileged or evidentiary offline communication of a client, litigant or witness, even to court save where there is an element of criminality.[3232] Arguably, this principle is similarly applicable to privileged online communication, whether the lawyer is in or out of the correctional facility.

The client has a reciprocal duty not to disclose the offline communication that the lawyer relays to the client during the consultation,[3233] which is arguably applicable to privileged online communication.[3234] The essence of protecting privileged communication is to allow heart-to-heart felt discussion between a professional and non-professional, in arriving at an informed decision or solution.[3235]

In all of this, the privileged communication —arguably, whether in offline or online communication— must be made in anticipation of obtaining legal advice or relating to litigation[3236] in the professional capacity of a lawyer because there must be an intention to

[3229] Moorcroft J 'POPI and the legal profession: What should you know? http://www.derebus.org.za/popi-legal-profession-know/ (Date of use: 18 January 2019); Heyink M 'A guide to the Protection of Personal Information Act - De Stadler E and Esselaar P' October 2015 *De Rebus* 60 http://www.derebus.org.za/guide-protection-personal-information-act/ (Date of use: 18 January 2019).
[3230] Strauss *Legal professional privilege* 27.
[3231] *AmaBhungane v Minister of Justice* supra 114.
[3232] *AmaBhungane v Minister of Justice* supra 115 and 118, 119; Strauss *Legal professional privilege* 26 and 27.
[3233] Strauss *Legal professional privilege* 27.
[3234] *AmaBhungane v Minister of Justice* supra 114.
[3235] Schwikkard P J 'Private Privilege' in Schwikkard P J and Van Der Merwe *Principles of evidence* (2017) 158 – 165.
[3236] For other conditions of enjoying this right, see Strauss *Legal professional privilege* 27.

create a relation of confidentiality.[3237] The relation must be apparently or ordinarily inferred, thus, having a mere relation with a lawyer will not qualify a client to enjoy the privilege of confidentiality.[3238]

Where privileged communication is forcibly taken away from the possession of a lawyer or the client, the right to privileged communication is not lost.[3239] Similarly and arguably, where there is unlawful conduct of an OCI, though the LEOs may be indemnified in some instances,[3240] the right to privileged online communication is not automatically lost under the operation of s 36 of the Constitution.

Section 36 is specifically considered in the right to privileged online communication and in relation to the philosophy behind the concept of the SOC, which has been proven to be a complex and delicate right in contemporary society.[3241] Thus, 'once privileged, always privileged' principle exists or that privileged communication will occur perpetually —which is extended to successors in title— where the parties and the subject matter are the same.[3242] Privileged online communication between a lawyer and a client is forever privileged, more particularly that online communication agent has a perpetual duty to protect the data in online communication —which is automatically and technically conscripted— in pursuance of the protection of the right to the SOC.[3243]

However, where there is a waiver of the right to privileged communication, the right falls away[3244] like the right in an online communication equally falls away once consent to intercept an online communication is given by a party in RICA.[3245]

[3237] Strauss *Legal professional privilege* 29.
[3238] Strauss *Legal professional privilege* 29.
[3239] Strauss *Legal professional privilege* 30; *AmaBhungane v Minister of Justice* supra 116.
[3240] Para 6.16 of this chapter. In Marnewick C *Mediation practice in the Magistrates' Courts* (2015) 137, (Marnewick *Mediation in the Magistrates' Courts*), though a mediator has immunity in some areas, a mediator is not indemnified of 'corruption (accepting a bribe from a party), conspiring with a party to defeat or undermine the other or defeat the end of justice, failing to disclose an interest in the subject matter or outcome, failing to disclose a relationship with a party that could actually or potentially affect the appearance of impartiality'.
[3241] See generally chapters 2 and 3 of this study.
[3242] Strauss *Legal professional privilege* 29-30. In a way, the perpetual nature of privileged communication nullifies the provision in section 1 of ECTA on the definition of personal information which stipulates that the privacy of a deceased person is not protected or that it is not protected beyond twenty years, paras 3.5.6.3 and 3.5.6.5 of Chapter 3 of this study.
[3243] Paras 3.5.7.7 and 3.5.7.8 of Chapter 3 of this study; *AmaBhungane v Minister of Justice* supra 116.
[3244] Strauss *Legal professional privilege* 29-30.
[3245] Paragraphs 2.3.3 and 6.2.3 of this study.

While the address of a client is not protected in the offline privileged communication,[3246] it is submitted that the equivalence of a physical address is classified under mega or traffic data in online communication. It is further submitted that some online addresses may be protected under the right to the SOC if the online address of a client does not fall under the category of information that can be obtained in the public space or through CCTV camera, for example.[3247]

Negotiation on behalf of a client is one of the instances where the communication between an attorney and a client is not protected under the right to privileged communication between the duo.[3248] Where negotiation is openly carried out by a lawyer on behalf of a client, the client cannot turn around to claim the right to privileged communication with the lawyer in the negotiation involving a third party in the negotiation.[3249]

Similarly, in online communication, where a lawyer —on behalf of a client— negotiates with a third party in online communication, the right to privileged communication does not exist between the lawyer and the client concerning the issues raised in the negotiation with third parties. However, privileged communication is permissible where the negotiated issues fall under the operation and practice of the negotiating principle of 'without prejudice' which enables parties to freely negotiate outside the court proceedings in anticipation of settling the dispute, but the discovery of which proceedings is not admissible as evidence in subsequent court proceedings save where criminality is involved in the negotiation.[3250]

6.15.2 Right in a privileged online communication between an attorney and a client

6.15.2.1 Controversy in the determination of place of interception and communication

According to the Canadian case of *R v Taylor*, the court erroneously held that the location of interception is determined by the place of interception and not by the place of communication.[3251] Essentially, the court held that since the interception of the mobile cellular telephone communication took place at the cellular calls distribution centre, interception could

[3246] Strauss *Legal professional privilege* 29.
[3247] Para 3.8 of Chapter 3 of this study.
[3248] Strauss *Legal professional privilege* 29.
[3249] Strauss *Legal Professional Privilege* 29.
[3250] *KLD Residential v Empire Earth Investments* (1135/2016) [2017] ZASCA 98 paras 1-3, 7- 9, 11, 18 -20, 21 - 22, 24 -27, 29 - 35, 38, 39, 40, 42 - 43, 47, 53 - 60, 62 -70, 72, 75, 77 -83, 85 - 87, 89 - 90 and 92 - 94.
[3251] Hubbard, Brauti and Fenton *Wiretapping* 6-19 to 6-30.6.

not have been held in the office of a solicitor.[3252] This arguably means that all that is needed to be done by a LEA to justify the lawful interception of privileged online communication between a solicitor and a client is to wait for the solicitor to move away from the office of a solicitor.

The rationale behind the reasoning of the court must have arguably been based on the interception of offline communication, which is located at the physically permanent point of the investigation, the principle of which cannot be applied in online communication.

It is important to note that the case of *R v Taylor* contradicts the earlier submissions made in this study regarding the U.S. 'no server, no law' principle[3253] and highlights a controversy in the RSA on the protection of the right to privileged online communication between an attorney and a client in the conduct of an OCI in and out of a correctional facility, for example.

Arguably, pure mobile cellular telephone communication[3254] made from and to any place within the online communication territory of the RSA is made within the same and one jurisdiction, which is in the RSA. It follows therefore that the interception of a mobile cellular telephone is conducted within the RSA as one jurisdiction and not in any particular geographical area that will create multiple and complex jurisdictional issues in the general protection of the right to the SOC and the conduct of an OCI in the RSA.[3255]

In particular, if the Canadian precedent in *R v Taylor*[3256] is applied in the RSA, it impliedly and incongruously means that any privileged online communication gathered between an attorney and a client in or outside a correctional facility may be intercepted at cellular calls distribution centre outside the correctional facility without breaching both the right to the SOC and the privileged online communication. Consequently, the Canadian precedent nullifies the principle of the perpetuity of privileged offline and online communication that says once a privileged

[3252] Hubbard, Brauti and Fenton *Wiretapping* 6-19 to 6-30.6.
[3253] The U.S. principle of 'no server, no law' states that all countries save the U.S. must seek and obtain consent from the U.S. authorities before an OCI is conducted in an Internet based online communication of a serious offences committed in the RSA, para 2.8 of Chapter 2 of this study.
[3254] This type of communication excludes communication made under an Internet-based communication, see para 2.8 of Chapter 2 of this study.
[3255] Para 2.8 of Chapter 2 of this study.
[3256] Hubbard, Brauti and Fenton *Wiretapping* 6-19 to 6-30.6.

communication, it is forever a privileged communication,[3257] which this study contests as examined herein.

6.15.2.2 Privileged online communication between an attorney and a client in a correctional facility

Privileged communication in the correctional facilities in RSA is protected domestically[3258] and recognised internationally.[3259] A lawyer, who is a significant factor in the administration of justice cannot be compelled to disclose what has been communicated to him or her by a client, otherwise, the denial of this right would turn a lawyer to be a witness who gives evidence against his client or such a lawyer turns to an informer.[3260] Essentially, it arguably means that lawyers should not be unlawfully conscripted to waive the right to privileged online communication.

In the limitation of the right to the SOC of an attorney and a client in a correctional facility, a written authorisation is issued by the Head of a Correctional Centre to the correctional officer to, with the assistance of a LEA, intercept the communication —including letters and online communication— of an inmate and a member of the public during a visit of the latter to the Centre.[3261] However, such interception may not occur where it is privileged communication, which means that a privileged online communication is protected from being intercepted except according to the law of privileged communication.[3262]

In conducting an OCI of some offences in a correctional facility, LEAs or LEOs embark on the least restrictive measure in the circumstances[3263] to investigate the security of the Correctional

[3257] Strauss *Legal professional privilege* 29 - 30. Paras 3.5.6.3 and 3.5.6.5 of Chapter 3 of this study.
[3258] Sections 13, 17 of Correctional Services Act No 111 of 1998 and s 105 (5) & (6) of the COPA.
[3259] Section 33 of HIPCAR *Interception of communication: 'Model policy guideline & legislative text* 2012; Hubbard, Brauti and Fenton *Wiretapping* 6-8.6 to 6-18.
[3260] Strauss *Legal professional privilege* 33.
[3261] Regulation 8(4)(b)of Correctional Services Regulation; In *Thint* supra paras 183 and 184 the court held that although attorney-client privilege is a serious right, it is not an absolute one because other countervailing circumstances can outweigh this right; In *State v Tandwa and Others* 2008 (1) SACR 613 (SCA) paras 18 and 19, the court held that attorney-client privilege can be waived expressly, tacitly or by conduct which is sufficient to conclude that there is a waiver of this privilege by the client; Luck R 'RICA' at 2 http://www.saflii.org/za/journals/DEREBUS/2014/6.html (Date of use:27 June 2019).
[3262] Ibid.
[3263] Para 5.3.6 of Chapter 5 of this study.

Centre or safety of any person in the correctional facility,[3264] otherwise, other least restrictive measures are expected to be applied to investigate the above offences.[3265]

The conduct of an OCI is specifically authorised in correctional centres in the RSA in the exercise of the power conferred in the relevant Act or regulation in the RSA,[3266] which seems inadequate as follows.

Firstly, the reasonable ground standard required to intercept the privileged communication of suspects or inmates in the correctional facilities in the RSA is rigidly and contradictorily based on 'belief' standard that the communication 'contains or will contain' evidence of' which constitutes a security or safety threat to the facility or a person at the facility[3267] or the planning or commission of an offence in the facility.[3268]

The 'belief' requirement in the Correctional Services Regulation is problematic because it erroneously regards both the standards 'contains' and 'will contain'[3269] as the same and the Regulation does not consider the proportionality principle in accordance with various serious offences that may require low or high standards of proof of the commission of an offence.[3270] This is because, from the logical point of view, more particularly the evidentiary or probative value in the 'belief' standard,[3271] the standard of proof involved where the communication 'contains' evidence of the commission of an offence is classified under the belief standard, given that the standard reveals that the evidence obtained is at or above 50.1 % of the facts required to conduct an OCI.[3272]

The standard of proof involved where the communication 'will contain' evidence of the commission of an offence is classified under any of the lowest, lower and low standards levels

[3264] Regulation 8(4) (b) of Correctional Services Regulation.
[3265] Para 5.3.6 of Chapter 5 of this study.
[3266] Section 9 of RICA.
[3267] Regulation 8(4)(a) of Correctional Services Regulation.
[3268] Regulation 8(4)(a)(i) of Correctional Services Regulation; Paras 6.4.2.2, 6.4.2.3, 6.4.3 and 6.4.5 – 6.4.9 of this chapter.
[3269] Paras 6.4.1 - 6.4.9 this chapter.
[3270] Regulation 8(4)(a)(i) of Correctional Services Regulations. See para 5.3.6 of Chapter 5 of this study.
[3271] Para 6.4.8 of this study.
[3272] Para 6.4.8 of this study.

of merely reasonable suspicious ground, given that the evidence does not reveal sufficient evidence that will be at 50.1 % but only reveals evidence between 0.01 % - 30 %.[3273]

Secondly, given that a post-OCI written notice to which an inmate is required to make representation thereto is issued at a time that is 'reasonably practicable' subject to whether the OCI is on-going[3274] is unreasonable if the duration period of giving notice cannot be proportionally stipulated according to the seriousness of an offence.

Thirdly, though it is a trite offline principle that it is a client or patient —and not the professional— that reserves the right to waive the right to privileged communication, the non-issuance of post-OCI notice to a third party —such as a lawyer, medical doctor etc.— who, though acts in an official capacity at a correctional facility, is an invasion of the right to the SOC of such professional at a correctional facility. The invasion is premised on the fact that the covert nature of the conduct of an OCI automatically withdraws the right of waiver of the enforcement of online privilege communication every user has, which highlights the establishment of online conscription in the use of online communications.[3275]

Thus, a professional suffers from the indiscriminate use of an OCI and double jeopardy in a correctional facility in two ways. Firstly, the jeopardy arises from the fact that, ordinarily, an OCI is intrusive in the life of an ordinary user of online communications —including an attorney as a member of the public— and secondly, as a professional who conducts official and fiduciary functions. Thus, it is recommended that the online communication devices and number belonging to a professional are electronically registered as such at the entrance on arrival and electronically de-registered on departure from the facility as conditionally exempted devices and number through the use of advance or specific geo-location technology.

[3273] Paras 6.4.5, 6.4.6.1 and 6.4.6.2 of this chapter.
[3274] Regulation 8(5) of Correctional Services Regulation.
[3275] Paragraphs 2.3.3 of chapter 2 of this study.

6.15.2.3 Privileged online communication between an attorney and a client out of a correctional facility

Before the High Court judgement in *AmaBhugane*,[3276] RICA did not make a provision for the protection of privileged online communication outside the correctional centres relating to the divergent rights of a client on the one hand and an attorney on the other hand, especially where the target is inadvertently the client and not the attorney. The former has a greater right of protection in a privileged online communication than the letter who has a general right like any other private person in the society who can be investigated for any serious offence in an OCI, such as the conduct of an OCI against a lawyer for defrauding a client, for example, in which case, the status of a lawyer is irrelevant in the conduct of an OCI.[3277]

Furthermore, the court did not hold back from observing that large scale crimes are not committed without the aid of lawyers, aside from accountants who are also held responsible by the court in this regard, therefore, an attorney cannot be exonerated in a criminal investigation.[3278] The court went further to hold that should there be a windfall privileged online communication evidence derived from the conduct of an OCI on an attorney who is involved in a crime, an independent intermediary party or intervention process —such as an Anton Pillar order— is required to filter or sift an 'inadvertent disclosure' of privileged online communication or irrelevant evidence.[3279]

However, aside from the already existing statutory Office of the Inspector-General of Intelligence, which is a statutory authority that —amongst others— plays an intervening role in the breach of the right to the SOC, it is submitted that introducing a new party into the conflict management process in this regard unnecessarily exposes and re-classifies what is supposed to be a privileged communication to a public issue. Therefore, the court rightly held that instead of allowing a micro-management interception process such as inviting an intermediary party or intervention process aside from the already existing ones, LEAs or LEOs should fully and truthfully disclose in their affidavit that there is no windfall privileged online

[3276] *AmaBhungane v Minister of Justice* supra 114 and 116.
[3277] *AmaBhungane v Minister of Justice* supra 117-119.
[3278] *AmaBhungane v Minister of Justice* supra 117 - 119; Hubbard, Brauti and Fenton *Wiretapping* 6-19 to 6-22.1.
[3279] *AmaBhungane v Minister of Justice* supra 120 and 121.

communication evidence which entitles the court to make specific conditions and restrictions in this regard.[3280]

6.15.2.4 Conclusion

It is recommended that given the legal and technical difficulties of identifying the privileged online communication between an attorney and a client which will, in reality, identify and expose a client to unnecessary conduct of an OCI, a court, in addition to other conditions to justify the conduct of an OCI, is required to compel a LEO to swear to an affidavit in an OCI application. The affidavit must state that the target intended to be intercepted is not an attorney, which is in pursuance of the protection of the right to the privileged communication between an attorney and a client.

This is effected by a verification of the identity of the attorney on the general list of public subscribers from the Online Communication Service Providers in pursuance of RICA requirements,[3281] enforcement of the earlier recommendation on the protection of the third party in online communication[3282] and the verification from the list of registered attorneys and advocates in the RSA which should easily and freely —including free costs— be accessible to the public in online communication, more particularly LEAs.

One of the other conditions required by the court in protecting a privileged online communication is an undertaken by a LEO to personally, and officially indemnify the injured client, third or innocent party in the event of an erroneous investigation or judgement to conduct an OCI.

In addition, an undertaken in an affidavit made by a LEO in an OCI application to the effect that, should there be erroneous conduct of an OCI, such gathered communication is deleted immediately. Lastly, an undertaken is made in an affidavit by a LEO in an OCI application to the effect that immediately an erroneously gathered communication is deleted, a LEO compulsorily swears to an affidavit confirming the deletion of the windfall evidence.

[3280] *AmaBhungane v Minister of Justice* supra 122, 128,140 and 141.
[3281] Para 3.9.4 of Chapter 3 of this study.
[3282] Para 6.14 of this chapter.

6.15.3 Right in a privilege communication between an investigative journalist and a whistle blower

Journalists and journalism, whose roles are aimed at protecting the criminal and non-criminal interests of the public, are by practice generally regarded as the fourth realm of government and watch dog of the three arms of government and public and private entities in the society.[3283] Nevertheless, there has been general neglect of the protection of professional sensitivity and secrecy of the communication of journalists in the RSA[3284] which tends to silence journalists who have been spied upon by LEAs or LEOs[3285] or whose monitoring by the LEAs is tantamount to investigating the society at large.[3286] However, despite the foregoing, RICA did not make provision for the protection of privileged online communication between a journalist and an informer until the judgement of the court in *AmaBhugane*.[3287]

It is believed that the sources that journalists rely on are holy[3288] and as such, their right to privilege communication is a natural[3289] and absolute one,[3290] save in exceptional circumstances where the disclosure of a confidential source can be compelled, one of which

---

[3283] *Bosasa v Basson* supra 15, 16, 17, 25, 26, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 43 – 55; Para 3.1 of Chapter 3 of this study. Right2Know at 2, 5, 9, 11, 12, 15, 17, 18, 20, 21, 22, 24, 25, 26, 27, 29, 30 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018). There are many cases of unlawful interception by private persons against journalists, amongst which is that a private entity spied on a journalist whose cell phone records, unique IMEI phone no and credit report were released by MTN to the journalist. It is presumed that a judge in KZN under section 205 of the CPA ordered the interception under the presumption that the private entity must have worked with the NPA and SAPS to apply under section 205 of the CPA. In the same report, a former CI-SAPS employee, now a private entity, is being held to account for unlawfully obtaining warrants to intercept the mobile cellular telephones of many private persons for private purposes. Further, it is claimed that in the reported the private investigator alleged some facts against the journalist relating to his immoral marital and sexual issues on the website of an adversary who was being investigated by the journalist, Right2Know at 15-18 and 36 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018); JSCI Reports 2016 at 39 and 40; *AmaBhugane v Minister of Justice* supra 131-132.

[3284] Oosthuizen G C et al (eds.) *Professional secrecy in South Africa* (1983) at the Preface Page, which though is not numbered, but it is herein numbered as ix in accordance with international numbering system of introductory pages.

[3285] Right2Know at 2-3 and 13-15 (and generally this source) https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[3286] *AmaBhungane v Minister of Justice* supra 136.

[3287] *AmaBhungane v Minister of Justice* supra 130-131 and 135; See paras 8.5 and 13.4.5 of the Founding Affidavit in *AmaBhungane v Minister of Justice* supra.

[3288] Pakendorf H 'The Journalist and His Sources' in Oosthuizen G C et al (eds.) *Professional secrecy in South Africa* (1983) 71 (Pakendorf '*The journalist and his sources*'); *AmaBhungane v Minister of Justice* supra130.

[3289] Pakendorf '*The journalist and his sources* 68.

[3290] De Villeirs *Confidentiality and journalism* 64; *AmaBhungane v Minister of Justice* supra 129 and 131.

involves the commission of a crime by a journalist.[3291] In some cases, informers, who may be witnesses, deserve to be protected from intimidation from the people suspected of wrongdoing.[3292] If there is no guarantee that the information supplied by an informer will not be confidential, then there will be less supply of leaked information to the media, which is as good as kissing public monitoring and control of political institutions farewell.[3293]

In the RSA, LEAs conduct fishing expedition on journalists who are seen as the 'first, automatic and immediate' sources to obtain information about the source of disclosure of a State secret.[3294] In the U.S., although journalists are the last resort in sourcing the disclosure of State secret,[3295] government oppresses journalists in the absence of '…a shred of suspicion' of the commission of an offence[3296] and believes that a journalist would not be a target of government harassment, intimidation and victimisation if such journalist passively turns a blind eye to what government does without the interference of a journalist.[3297]

There is a breach of trust or confidence if a journalist reveals the source of information to 'save his or her own skin'.[3298] Other breaches occur where there is involuntary double jeopardy against a journalist which involves, firstly, where the disclosure occurs by the compelling conscriptive online communication[3299] between an investigative journalist and an informer and secondly, the jeopardy is due to no fault of the journalist because of the covert nature of the conduct of an OCI which reveals the privileged communication between an investigative journalist and an informer.

Sequel to the high level of harassment by LEAs; journalists in the RSA and U.S. resort not to use their mobile cellular telephones for fear of being monitored or physically searched to find

[3291] *AmaBhungane v Minister of Justice* supra 134 and 136.
[3292] Art 24 (1), (2)(b) of the TOCC; Right2Know at 13-14 and 22 and 23 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).
[3293] Pakendorf *The journalist and his sources* 70; *AmaBhungane v Minister of Justice* supra 129, 130 and 133.
[3294] *AmaBhungane v Minister of Justice* supra 138.
[3295] De Villeirs *Confidentiality and journalism* 63.
[3296] Greenwald *U.S. Filmmaker repeatedly detained at border* 188.
[3297] Greenwald *U.S. Filmmaker repeatedly detained at border* 188.
[3298] De Villeirs *Confidentiality and journalism* 67.
[3299] Para 2.3.3 of Chapter 2 of this study.

out about the source of information.[3300] In some cases, journalists in the RSA are threatened in many ways and instigated to compromise the investigation for financial and other compensations of status by the LEOs.[3301] Furthermore, in the U.S., a journalist enforced her right to enjoy privileged communication by refusing to answer some specific questions about the identity of the person she met during her trip.[3302]

However, the opposition to the right to privileged communication strongly believes that journalists should not be treated with kid gloves from the way other professions or professionals are treated in this regard.[3303] Arguably, this is because, should journalists be treated differently, it means that other professionals, trades, vocations and callings such as accountants, doctors, pastors and even domestic workers —who know more private or confidential information about the house that is managed— will open the floodgate for all to demand that their communications with their clients be classified as privileged communication.

It is argued that having an indiscriminate application of privileged communication will render the genuine underlying rationale behind the principle useless, therefore, journalists cannot be accorded a blanket protection. Such blanket protection includes the call by journalists that there should be 'an established channel of communication' between the Online Communication Service Providers and their association (SANEF) through which journalists can confirm if their online communication had been intercepted.[3304] However, this suggestion is problematic because of the following:

Firstly, an Online Communication Service Provider is empowered to have direct conduct of an OCI and operate an internal dispute management mechanism between users and its entity for expediency purposes. However, for an Online Communication Service Provider to act as a player in its own game by addressing grievances of unlawful criminal conduct of an OCI tabled by an investigative journalist contravenes the principle of separation of powers. Rather, such grievances should be handled by the OIGI, which though is not independent because there is a

---

[3300] Greenwald *'U.S. Filmmaker repeatedly detained at border* 182-183. Right2Know 11 and 13 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use:27 November 2018); *AmaBhungane v Minister of Justice* supra 137.

[3301] Right2Know at 27–28 and 30-32 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[3302] Greenwald *'U.S. Filmmaker repeatedly detained at border'* 182.

[3303] Pakendorf '*The journalist and his sources*' 70.

[3304] Right2Know at 39 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

level of control by the SSA,[3305] is in a better position to neutrally handle the impasse because it is not initially involved in the subject matter that creates the grievance.

Secondly, accordingly, an Online Communication Service Provider cannot be a judge in their case, given that an Online Communication Service Provider is initially involved in the creation of the problem of the unlawful conduct of an OCI.

Furthermore, the opposition to the protection of privileged communication between a journalist and an informer believes that the earlier the media wakes up from their slumber of absolutism, the more realistic for them to realise that they are not above the law because they do not occupy an exalted or reverend position in the society; though they have played diverse unparalleled and significant confrontational or revolutionary roles against the governments and society since time immemorial as journalists, editors and publishers.[3306]

After all, journalists are not infallible. To support this infallibility, the High Court in *EFF v SANEF*[3307] declined to grant a prayer by some journalists and their association that EFF, a political party in the RSA, be denied their right to freedom of expression or speech against journalists. The journalists were accused by EFF of not investigating a prominent politician and cabinet minister who was allegedly accused of using his daughter as a proxy in conducting business with the government, amongst other issues.[3308]

In some other instances, journalists have been found wanting by contravening their ethical codes, therefore, it is believed that they do not deserve the right to privileged communication.[3309]

Firstly, two journalists, on behalf of Sunday Times, falsely reported some information about the rendition of some Zimbabweans.[3310]

[3305] Para 7.6.4 of Chapter 7 of this study.
[3306] De Villiers *Confidentiality and journalism* 64.
[3307] *SANEF & ors v EFF and ors* 90405/18 para 106 and 107.
[3308] Cowan K 'Here is the EFF's 'evidence' on Gordhan's daughter - and why their claims are bogus' https://www.news24.com/SouthAfrica/News/here-is-the-effs-evidence-on-gordhans-daughter-and-why-their-claims-are-bogus-20181122 (Date of use: 30 November 2019).
[3309] De Villiers *Confidentiality and Journalism* 66-67.
[3310] ANA 'Sanef to start probe over Sunday Times 'fake news' https://citizen.co.za/news/south-africa/2023805/sanef-to-start-probe-over-sunday-times-fake-news/ (Date of use:12 December 2018 (ANA

Secondly, Sunday Times apologised for wrongly acting on the forged Auditor-General's report implicating the former acting CEO of PRASA for irregularly hiking his salary by 350%.[3311]

Thirdly, a senior journalist was reported at the State of Capture Commission of Enquiry to have allegedly shared out of the slush fund meant for CI-SAPS.[3312]

Fourthly, in 2019, a top cabinet minister of government and chairperson of the biggest political party claimed that he paid an amount of R70, 000 to two journalists to make the story on his extra marital sex scandal disappear but he later denied the payment of the said amount.[3313]

It flows therefore that LEAs should not be prohibited from breaching the right to the SOC of journalists to genuinely verify the truth in a communication made by a journalist if a serious crime has been committed by the disclosure by a journalist.

In conclusion, given that journalists —as the fourth realm of government with public-private interests, mandate and power—[3314] are between the devil and the deep blue sea in either disclosing secret information about the public or against the government or private or turning a blind eye to protect their jobs, personal and family lives and safety (on the one hand) and lock their conscience of telling the truth (on the other hand), a balance should be struck between this catch-22 scenario in the following ways.

---

https://citizen.co.za/news/south-africa/2023805/sanef-to-start-probe-over-sunday-times-fake-news/ (Date of use:12 December 2018).

[3311] ANA 'Former Prasa acting CEO to break silence on 350% salary hike claims' https://www.iol.co.za/business-report/companies/former-prasa-acting-ceo-to-break-silence-on-350-salary hike-claims-18528550 (Date of use:18 December 2018) (ANA https://www.iol.co.za/business-report/companies/former-prasa-acting-ceo-to-break-silence-on-350-salary-hike-claims-18528550 (Date of use:18 December 2018).

[3312] ENCA 'Journalist Ranjeni Munusamy on special leave amidst slush fund payment claims' https://www.enca.com/news/journalist-ranjeni-munusamy-placed-special-leave-amid-state-capture-revelations (Date of use:18 September 2019) (ENCA https://www.enca.com/news/journalist-ranjeni-munusamy-placed-special-leave-amid-state-capture-revelations (Date of use:18 September 2019).

[3313] News24 Wire 'Sanef shocked by allegations Mantashe paid reporters for sex story to 'go away'' https://citizen.co.za/news/south-africa/politics/2196647/sanef-shocked-by-allegations-mantashe-paid-reporters-for-sex-story-to-go-away/ (Date of use:28 October 2019); Citizen Reporter 'Mantashe admits to paying journalists R70K to make sex scandal go away–Ndlozi' https://citizen.co.za/news/south-africa/social-media/2196611/mantashe-admits-to-paying-journalists-r70k-to-make-sex-scandal-go-away-ndlozi/ (Date of use: 28 October, 2019; News24 'Mantashe denies bribing journos R70K to make sex scandal go away' https://citizen.co.za/news/south-africa/politics/2197320/mantashe-denies-bribing-journos-r70k-to-make-sex-scandal-go-away/ (Date of use: 11 November 2019).

[3314] This is opposed to attorney-client relationship that is more likely to be private as examined above.

Firstly, it is submitted that not all journalists may be accorded an umbrella privileged communication protection for themselves and informers because not all journalists are investigative journalists, neither are all informers credible or impeccable.[3315] The public may approach anyone that is known to be working in a media house or space or related field to blow the whistle. However, the principle of privileged communication will be extended too far if all journalists —who are not statutorily but self-regulated— are accorded this broad power without regulating journalism for proper accountability purposes as other professions are professionally registered and regulated. Such registered professions include attorneys, advocates, doctors and accountants, amongst others.

Instead, it will be expected that where a non-professional investigative journalist is approached by an informer, he or she may refer the matter to a registered and licensed investigating journalist to protect the informer. This is because it will be too broad to protect anyone who identifies himself or herself as a journalist in a profession that is not statutorily registered, licenced and regulated as opposed to the professionals aforementioned who are issued a licence to practice subject to periodic renewal provision.[3316]

Therefore, granting umbrella protection for privileged communication between an ordinary journalist and an informer will be protecting non-qualified persons in the field of communication or journalism who are not statutorily accountable, though not in terms of the pending draconian PSIB (or 'Secrecy Bill') that seeks to shutout the voice of journalists in revealing the necessary State secret.[3317]

Secondly, as a corollary to the first recommendation above, in every OCI application, a LEO is expected to compulsorily declare in the affidavit or oath that the target of an OCI is not an

---

[3315] ANA https://citizen.co.za/news/south-africa/2023805/sanef-to-start-probe-over-sunday-times-fake-news/ (Date of use: 12 December 2018; ANA https://www.iol.co.za/business-report/companies/former-prasa-acting-ceo-to-break-silence-on-350-salary-hike-claims-18528550 (Date of use: 18 December 2018); ENCA https://www.enca.com/news/journalist-ranjeni-munusamy-placed-special-leave-amid-state-capture-revelations (Date of use:18 September 2019).

[3316] However, it is noted that journalists belong to a body of voluntary professionals that regulates their activities or affairs, but the body does not have penal powers.

[3317] Right2Know at 6 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018); Ferreira E New secrecy bill recalls the failings of the old https://www.iol.co.za/news/politics/new-secrecy-bill-recalls-the-failings-of-the-old-17106869 (Date of use: 25 September 2018).

investigative journalist or that the journalist is not investigating a matter that is of public criminal interest.[3318] This measure is to ensure that a LEO is not maliciously motivated to conduct a retaliatory OCI against such journalist, save where the investigative journalist is being investigated under the various laws that prohibit disclosure of classified information.

This caveat is to make a LEO accountable for breaching the right mentioned in the first conclusion above, which implies that a LEO will be criminally penalised and not be indemnified, should false information be furnished to the court.[3319] This approach also enables the court to impose other conditions in every OCI application or direction which will ensure that the confidentiality of an informer is protected in the online communication between an investigative journalist and an informer.

Aside from the general provisions and criminal sanctions provided in the various laws in the conduct of an OCI or which are reinstated herein,[3320] such conditions or enquiries include amongst others the distinct, though in some instances interdependent and consequential facts that:

a) a LEO or LEA is aware that the right to be limited in online communication is a unique, delicate and complex right to the SOC, which creates the awareness or consciousness amongst LEAs and LEOs that the right in online communication is not a right that can be equated with offline communication or privacy but a classification of personality right at a higher level, which is the right to the SOC;[3321]

b) no previous OCI had been conducted on the target by the same LEA or LEO on the same facts, which necessitate a check by the LEO of the records of the particular LEAs with the Online Communication Service Providers and Interception Centre. This measure seeks to ensure that double conduct of an OCI is avoided, should it come to the attention of the LEO that same or another LEA had conducted an OCI on the same target on the same matter;

[3318] Para 6.1 of this chapter.
[3319] *AmaBhungane v Minister of Justice* supra 20.
[3320] Para 3.10 of Chapter 3 of this study.
[3321] See generally chapter 3, more particularly paras 3.3, 3.4, 3.5, 3.8 and 3.10.

c) the online communication identity of the target is not erroneously, falsely or maliciously obtained and supplied in the application;

d) the LEO has conducted a due diligence search that the name of the target —investigative journalist— is not found on the proposed list of registered investigative journalists in the RSA that requires protection in this regard. It is noted that the court in *AmaBhugane* did not advert its mind to the recommendation on the statutory registration of journalists to make the right to the protection of privilege online communication between a journalist and an informer effective;[3322]

e) that the LEO or LEA making the application has not had any direct or indirect physical or online contact, course or interaction whatsoever on the target save for the first time in the current application and if there was a previous contact, full facts must be supplied by the LEO in the OCI application;

f) that an illegal interception of the target had not been carried out before the launch of the current OCI application which now maliciously motivates the decision for the current application;

g) there is no conflict of interests whatsoever in the current application.

In conclusion, in the relevant instances, the defence of lack of knowledge of the facts in the foregoing paragraphs above by a LEA or LEO will be strictly considered on merit by the court in an OCI application, whether such defence will qualify as an indemnity or not to exonerate a LEO who contravenes the provisions of RICA and the mechanisms developed in this study.

6.16 INDEMNITY FROM PROSECUTION OF LAW ENFORCEMENT OFFICERS ENGAGED IN AN UNLAWFUL ONLINE CRIMINAL INVESTIGATION

In RICA, an indemnity from prosecution for the unlawful conduct of an OCI is granted to a LEO who acts in good faith in assisting an authorised person to execute an OCI direction and

[3322] *AmaBhungane v Minister of Justice* supra 109.

who reasonably believes that such an authorised person acts in pursuance of a direction, yet there is an unlawful pre and post conduct of an OCI.[3323]

In *State v Naidoo*, no LEO or employee of MTN —one of the Telecommunications Service Providers in the RSA— was charged with an offence of contravening the law on the conduct of an OCI.[3324] The court erroneously held that the LEO (Capt. Van der Vyver) acted in good faith by obtaining an online communication before the issuance of a subpoena simply because the MTN employee was willing to furnish such information without a direction of the court under section 205 of the CPA, consequently, the LEO was exonerated by the court despite the overwhelming evidence.[3325]

The principle of indemnity can also be illustrated from another perspective which is the indemnity of liability of Online Communication Service Providers in the conduct of an OCI. This perspective relies on the study carried on an ISP in transmitting a sound recording in online communication which does not hold ISPs liable for turning a blind eye in the breach of the right of a sound recording owner through the use of a DP2P file-sharing application by a user of a DP2P software application.[3326]

Chapter XI of the ECTA —including section 78— provides for the limitation of liability of ISPs in the breach of online content. However, a study by the author of this thesis —in his LL.M degree level— reveals that the liability of Internet Service Providers should not be limited in some circumstances including the protection of sound recording, given the obvious exclusive technical obligation of an Internet Service Provider to filter, identify and detect an unlawful transmission of sound recording.[3327]

This issue is now being addressed in the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017, which introduces the liability of Internet Service Providers in breach of an obligation to filter, identify and detect an unlawful transmission of online communication in DP2P file-

[3323] Section 51(7)(a)-(b) of RICA.
[3324] *State v Naidoo* supra 531.
[3325] *State v Naidoo* supra 531.
[3326] Popoola *Liability of ISPs* at ii, 1, 2, 6, 16, 17, 18, 85, 86, 90, 91, 92, 94, 106, 144, 184, 185, 192, 206 and 208; Section 79 of the ECTA provides for the deviation of liability of OSP provided in the ECTA.
[3327] Popoola *Liability of ISPs* at ii, 1, 2, 6, 16, 17, 18, 85, 86, 90, 91, 92, 94, 106, 144, 184, 185, 192, 206 and 208; Section 79 of ECTA provides for the deviation of liability of OSP provided in ECTA.

sharing application.[3328] Similarly, the Online Communication Service Providers should not be indemnified from liability where there is unlawful and intentional conduct of an OCI.

Should an indemnity of liability be granted to LEO or any relevant stakeholder for the unlawful conduct of an OCI, it should be proportionately considered in relation to the nature —whether intentional or premeditated or not— and the seriousness of the act of omission or commission of the obligation to protect the right to the SOC or to what extent is the indemnity principle applicable to a LEO or relevant stakeholder. Essentially, liability may not be averted in some instances where it is obvious that a LEO or relevant stakeholder may not be exonerated in the breach of the right to the SOC in the conduct of an OCI. Therefore, the more serious an unlawful conduct of an OCI by a LEO or relevant stakeholder is, the less consideration is given to the application of the indemnity principle granted to a LEO or relevant stakeholder to protect the future or further breach of the right to the SOC by a LEO.

Where an indemnity is extended to some authorities or persons without justification or extended to persons who are not qualified to conduct an OCI,[3329] the extension of indemnity indirectly aggravates the breach of the right to the SOC in the conduct of an OCI because such persons are not objectively, statutorily, adequately and directly held responsible for their role in the duty of care to protect the right to the SOC. There is practically no basic understanding of the operational, legal and ethical standards of the conduct of an OCI by such persons to ensure strict compliance with the provisions of RICA. However, once a duty of care is allocated to a stakeholder in the administrative, supervisory and operational conduct of an OCI according to the described office, function, responsibility or role; a liability is invoked as canvassed in this study.[3330]

One such instance of unjustifiable indemnity is where there is a limitation of liability of the State, minister or employee of the State on any act of omission or commission in good faith and without holding such officers grossly negligent in the performance of the functions in ECTA,[3331] which may have a direct or indirect impact on the conduct of an OCI. It is important

[3328] Section 20 of the CCB B-2017, which is replaced with section 21 of the Cybercrime Bill 2018-Amendments Proposed to Bill B6-2017.
[3329] Paras 2.11 and 4.2 of this study.
[3330] Paras 3.9 and 3.10 of Chapter 3 of this study. The Foreign Services Act B35B 2015 which professionalises the deployment of ambassadors, high commissioners and consuls to foreign countries, which hitherto was not professionalized, is still pending before Parliament.
[3331] Section 93 of ECTA.

to note that liability arising from the unlawful conduct of an OCI may be excluded against a LEO who is not contributory to the liability arising from the conduct of an OCI by a ROCITOR.[3332]

Furthermore, the application of the indemnity principle is subject to the consideration of whether such evidence which is obtained from the unlawful conduct of an OCI by a LEO is admissible under section 35(5) of the Constitution. Given the stringent substantive and adjectival requirements for the conduct of an OCI,[3333] it is less probable that an OCI can be mistakenly conducted, more particularly relying on the *Popoola QOCI* protocol.[3334]

This process can only be breached intentionally due to the compulsory interdependent techno-legal roles of stakeholders; therefore, indemnity may not be granted, neither is the evidence obtained unlawfully regarded as admissible where the unlawful conduct of an OCI is intentional.[3335]

6.17 CONCLUSION

An interception of online communication occurs in many instances without a direction of the court in non-consensual party intercept, consensual party intercept, emergency intercept, online criminal interception under the CSA and technical maintenance and monitoring intercept while a direction is required in the general online criminal investigation, where the latter is the gravamen of this study.[3336]

This study reveals the prominence of the indispensability of the proportionality principle in the conduct of an OCI of serious offences. In pursuance of this principle, this study conceptualises six degrees of serious offences —in each of the four criteria for a specific classification of fluid serious offences— with six corresponding Popoola mathematical and non-mathematical formulae, which should be incorporated in a legislation. These formulae are required in the substantive and adjectival standards of proof required of a proportionately competent LEO in

[3332] Para 2.11.4 of Chapter 2 of this study.
[3333] Paras 6.3 - 6.5 of this chapter.
[3334] Para 6.11 of this chapter.
[3335] Para 7.8 of Chapter 7 of this study.
[3336] Para 6.2 of this chapter.

an oral or written ex-parte and arguably, the proposed motion on notice and intervening application before a magistrate, judge or designated judge in a *Popoola QOCI* protocol.[3337]

Although not supported by legislation in the RSA, in some special circumstances, an artificially intelligent LEO —with machine learning capability— or ROCITOR, which has its merits and demerits, can be used to determine the various standards of proof to conduct an OCI in the RSA.[3338]

Section 205 of the CPA, which has been generally sanctioned by the Constitutional Court, is incongruous in the conduct of an OCI because it does not comply with the object and provisions of RICA as the main legislation in the conduct of an OCI. Therefore, section 205 of the CPA should alternatively be amended to incorporate the provisions of RICA, expunged from RICA or be applicable to offline investigation only.[3339]

Also, the absence of regulation of mass OCI in RICA or in any other law is anathema in the conduct of an OCI, which should be proportionately regulated according to the degree of serious offences, irreversibility of the effect of the commission of a serious offence and other circumstances.[3340]

This chapter also reveals that privileged online communication between an attorney and a client, investigative journalists and an informer or whistle-blower and other similar relationships exists. However, this communication was not protected in RICA or any other law in the RSA until the judgement of the High Court in *AmaBhugane* which is on appeal before the Constitutional Court but in the interim now protects privileged online communication between an attorney and a client and an investigating journalist and an informer.[3341]

It is revealed in this chapter that the indemnity from prosecution of a LEO for the unlawful conduct of an OCI in RICA does not proportionately consider the level of the intention of breaching RICA provisions by a LEO while conducting an OCI and the nature and seriousness

[3337] Paras 6.3 - 6.11 of this chapter.
[3338] Paras 6.4.9 of this chapter.
[3339] Para 6.12 of this chapter.
[3340] Paras 6.3.3 and 6.13 of this chapter.
[3341] Para 6.15 of this chapter.

of an offence *vis-a-vis* the admissibility of such intentionally and unlawfully obtained evidence in the investigation of a serious offence.

Finally, in considering the complexities of the issues raised in this chapter, it is concluded that the most appropriate, rational and reasonable decision to make is to incorporate the mandate to conduct an OCI in the Constitution of the RSA.[3342]

[3342] Chapters 2 – 7, particularly paras 2.2.2.2 and 2.3.1 - 2.3.3, 2.4, Chapter 3 of this study, more particularly para 3.11 and Chapter 8, more importantly para 8.6 of this study.

While I am alive and even after death when I should be left alone resting in perfect and eternal peace as the bee hummingbird in my supposedly tranquil nest, I am crushed by the covert online surveillance web of the eagles. Alas, my secret is perpetually scattered and wandering around in the wilderness of the eagles who are equally fallible beings. What an unforgiving society that I live in that I am perpetually crucified even if God or nature forgives me.

CHAPTER 7: EXECUTION AND POST-EXECUTION OF AN ONLINE CRIMINAL INVESTIGATION

7.1 INTRODUCTION

Further to the examination of previous chapters, more particularly the chapter on the application for and issuance of an OCI direction,[3343] this chapter examines the role of stakeholders between the pre and post-execution of an OCI[3344] to conclude the process involved in the conduct of an OCI in the RSA.

7.2 *DELEGATUS POTEST NON DELEGARE* OF LAW ENFORCEMENT OFFICERS

The principle of *delegatus potest non delegare* states that an already delegated power cannot further be delegated in some special circumstances because of the unique, complex and sensitive nature of the duty.[3345] Arguably, these circumstances include the delegation of authority of the conduct of an OCI which is a unique, complex and sensitive form of investigation and the further delegation of this authority to another LEO or a role player —save in some special circumstances where it is expedient to do so— may constitute an infringement

[3343] Chapter 6 of this study.
[3344] The *AmaBhungane v Minister of Justice* supra 31, 33, 40 - 56, 84 -91, 93 -108 and 167 substantially deals with some of the issues that are raised in this chapter.
[3345] Business Dictionary '*delegatus potest non delegare*' http://www.businessdictionary.com/definition/delegatus-non-potest-delegare.html (Date of use: 23 August 2019).

of the right to the SOC, because not restricting access to online communication is as good as exposing the right holder to the public.

RICA recognises the significance of an aspect of the application of the principle of *delegatus potest non delegare* which requires the higher authorities to delegate the powers of the conduct of an OCI to specific LEOs who are in charge of the operational conduct of an OCI.[3346] Nonetheless, RICA does not strictly apply it in the OCI application and execution of direction,[3347] thus leads to an infringement of the right to the SOC. This is because RICA does not restrict the sub-delegation of power to conduct an OCI amongst delegated LEOs.

If the courts were to strictly apply the principle of *delegatus potest non delegare*, RICA partially complies with the application of the principle concerning the requirement that there must be a written authorisation of delegation from the initial applicant to a subsequent LEO in the operational conduct of an OCI by IPID.[3348] In other categories of LEAs comprising: the CI-SAPS, the DI-SANDF, the SSA, the HAWKS and ID-NPA; RICA does not provide for written authorisation of delegation of authority from one LEO to another when delegating such authority to execute an OCI direction.[3349]

The latter scenario makes it possible —for instance— for a junior official to be held liable for the sin of the senior officer where no requirement places on record the lawful delegation from the top to the bottom, which should impliedly and proportionately hold the senior officer responsible for the unlawful conduct of an OCI. A junior official —who was a captain— was held liable in CI-SAPS for the unlawful conduct of an OCI of the mobile cellular telephone of some investigative journalists and a former Commissioner of Police and Minister of Police.[3350]

[3346] Section 1 of RICA for the definition of 'applicant'.
[3347] See 'applicant' in section 1 of RICA and section 26(1) (a) (i) &(ii) & (b), (2) and (3) of RICA.
[3348] Section 26(1)(a)(i) & (ii) and (b) of RICA.
[3349] Section 26(1)(a)(i) & (ii) & (b), (2) and (3) of RICA; Also, even s 22(3)-(9) of IPIDA 1 of 2011 which deals with delegation of authority does not make any reference to the delegation of authority regarding OCI procedure in RICA. Also, in art 16(10) of UNODC 'Model Legislative provisions against organised crime' 2012, there no provision for special requirement to be a LEO, either as an officer or an individual. In s 16(1) of ITU 'Interception Policy & Legislative Text' (2012), it does not seem to encourage delegation of authority to make final report to the court by the initial LEO.
[3350] Right2Know 'Spooked- Surveillance of Journalists in SA' at 13-14 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018 (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

The captain was convicted by the Pretoria Commercial Crimes Court in 2017 for the unlawful conduct of an OCI with a three-year suspended sentence.[3351]

It is therefore recommended that the principle of '*delegatus potest non delegare*' should be adequately sanctioned and enforced to ensure compliance with the requirements of professionalism, integrity, competence and accountability in the conduct of an OCI. This principle requires that the OCI application powers given to a LEO by the head of such LEA should not be unjustifiably, irrationally and unreasonably sub-delegated to another LEO other than the initially designated LEO on record under RICA provisions.[3352] However, the principle of '*delegatus potest non delegare*' may not apply where Automatic and Special online criminal investigators are involved provided the 'delegatee' complies with other requirements of conducting an OCI, such as the competence to conduct an OCI. In addition, a register of LEOs or other officers, with professional practice number, must be created by a central body to enforce accountability and checks and balances.

7.3 CONDUCTING ONLINE CRIMINAL INVESTIGATION BY EXECUTING AUTHORITIES AND ENTITIES

7.3.1 Introduction

This study identifies four key role players in the *Popoola QOCI* operational conduct of an OCI[3353] which are the LEAs,[3354] court,[3355] Online Communication Service Providers and Interception Centre some of which are examined under this rubric below.[3356] However, RICA and the U.S. authorities argue that technical support and assistance is needed from other Online Communication Service Providers in the execution and post-execution of the conduct of an

[3351] Right2Know 'Spooked- Surveillance of Journalists in SA' at 13-14 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018 (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[3352] Chapter 1 of Para 2(1)(a) and (2) (a) -(c) of Regulation 7797 Notice No 1505 Gazette No 25592 titled 'Ministry for Intelligence Services' provides for the regulation of the delegation of authority and limitations thereof from the minister to the D-G, CEO or members of SSA. See also section 10 of IPIDA on delegation.

[3353] Para 6.11 of Chapter 6 of this study.

[3354] The role of LEAs in the execution and post execution of the conduct of an OCI is examined throughout this study but with emphasis in paras 4.4, 4.5, Chapter 5 and paras 6.11, 7.4 and 7.5 of this study.

[3355] The role of the judiciary in the execution and post-execution of an OCI is generally examined in this study, more particularly paras 6.11, 7.4, 7.6.6, 7.7 and 7.8 of this study.

[3356] Organisations under Interception Centres are examined in paras 7.3.4 and 7.3.6 herein.

OCI,[3357] which is simultaneously examined below with the oversight by and of these role players, the adequacy or otherwise of which directly, and indirectly impacts on the conduct of an OCI.

7.3.2 Role and management of the affairs and activities of a Decryption Keyholder, Cryptographer and Authentication Service Provider in conducting online criminal investigation

7.3.2.1 Introduction

Decryption Keyholder,[3358] Cryptography Provider and Authentication Service Provider[3359] are intermediaries who assist the main authorities and entities charged with the responsibility of conducting an OCI while executing their duties.

7.3.2.2 Description and appointment of Decryption Keyholder, Cryptography and Authentication Service Provider

a. Description and appointment of a Decryption Keyholder

A Decryption Keyholder is a 'person who is in possession of a decryption key', 'mathematical formula, code, password, algorithm or any other data which is used to allow access to encrypted information' or 'facilitate the putting of encrypted information into an intelligible form'.[3360] The key is used 'for purposes of subsequent decryption of encrypted information relating to indirect communications'.[3361]

However, this definition is inadequate because it does not include the word 'authorised' or similar word to separate authorised and non-authorised persons in having possession of a

[3357] Some of the Online Communication Service Providers are examined in paras 7.3.2., 7.3.3, 7.3.5, see RICA Directives 2005; Caproni *Lawful electronic surveillance* 210.
[3358] Sections 1 and 29(1) (a) &(b), (2) (a) -(c), 3(a) &(b), 4(a) & (b), 5(a) & 6(a)&(b), 7(a)-(c) and 8 (a)& (b) 31(2)(b)(i) & (ii) of RICA.
[3359] Sections 1 and Chapters V and VI of the ECTA.
[3360] Section 1 of RICA.
[3361] Section 1 of RICA.

decryption key, given the delicate and sensitive nature of a decryption key.[3362] However, the criminalisation of unauthorisation of the functions in RICA addresses this inadequacy.[3363]

In the engagement of a Decryption Keyholder, there is no provision for the appointment of a Decryption Keyholder in terms of academic, practical or experiential requirement, thus fails to comply with the employment requirements and principles laid down in this study relating to LEOs, the appointment requirements of which include the principles of separation of powers and checks and balances of appointment of LEOs.[3364] It is therefore recommended that same or similar recommendations made regarding the appointment of LEOs be considered for the appointment of a Decryption Keyholder.[3365]

b. Description and appointment of a Cryptography Provider

A cryptography service or product is provided or is proposed to be provided by a Cryptography Provider to assist a sender, receiver of or anyone storing online data.[3366] A Cryptography Provider 'facilitates the use of cryptographic techniques' which serve the following purposes of a) accessing or putting such data in an intelligible form only by authorised persons; b) verifying the authenticity or integrity of data; c) maintaining the integrity of data; d) correctly ascertaining the source of data.[3367]

In the engagement of a cryptography provider, there is no provision regulating the appointment of a Cryptography Provider in terms of qualification, experience, skill or other forms of quality assurance when appointing a provider.[3368] At best, the Director-General of the Department registers all cryptography providers for an administrative fee in a register and maintains same based on the little information obtained from such a person such as the name and address of the person, the type of cryptographic services to be registered for etc.[3369]

[3362] Section 51 of RICA.
[3363] Section 51 of RICA
[3364] Paras 4.3.2 - 4.3.7 of Chapter 4 of this study.
[3365] See para 4.4 of this study titled 'Specialised staff and training of law enforcement agencies in online criminal investigation' and see generally the other role players who are involved in the conduct of OCI in para 6.3 of this study.
[3366] Section 1 of the ECTA.
[3367] Section 1 of the ECTA.
[3368] Chapter V of the ECTA.
[3369] Sections 29(1) and 30 (1) & (2) of the ECTA.

Nevertheless, there is a strict obligation for a Cryptography Service Provider to ensure compliance with the non-disclosure of information or trade secret gathered in the course of performing the cryptographic services.[3370]

In summary, it is recommended that the same or similar recommendations made regarding the appointment of LEOs be considered for the appointment of a Cryptography Provider.[3371]

c. Description and appointment of an Authentication Service Provider

An Authentication Service Provider is a 'person whose authentication products or services have been accredited' or recognised by the ACA to 'identify the holder of an electronic signature to other persons'.[3372] However, this description is inadequate because it limits the description of this office holder to accreditation requirement only without highlighting the functions performed by the provider.

While the Director-General of the Department of Communication acts as the ACA for the Authentication Service Providers,[3373] the Director-General, upon consulting with the Minister of Communication, may appoint employees of the department as deputy Accreditation Authorities and officers.[3374]

The Minister of Communication is empowered, on condition stated in the Gazette, to recognise the accreditation granted to a Foreign Authentication Service Provider, service or product by a foreign jurisdiction.[3375] The provision of conditions in the Gazette reiterates the enforcement of the cyber territorial sovereignty of the RSA, which in another perspective rejects the U.S. principle of 'no server, no law'.[3376] This principle obstructs the effective and efficient conduct of an OCI because the principle requires that the LEAs in the RSA must seek and obtain consent

[3370] Section 29(3), 31 and 32 of the ECTA.
[3371] See para 4.4 of this study titled 'Specialised staff and training of law enforcement agencies in online criminal investigation' and see generally the other role players who are involved in the conduct of OCI in para 6.3 of this study.
[3372] Sections 1, 37 and 40 of the ECTA.
[3373] Authentication products or services mean 'products or services designed to identify the holder of an electronic signature to other persons while Authentication Service Provider means 'a person whose authentication products or services have been accredited by the ACA under section 37 or recognised under section 40, see section 1 of the ECTA.
[3374] Section 34(1) & (2) of the ECTA.
[3375] Section 40(1) of the ECTA.
[3376] Para 2.8 of Chapter 2 of this study.

from the authorities in the U.S before the former conduct an OCI in an Internet-based platform.[3377]

However, although there is no requirement for the appointment of an Authentication Service Provider in terms of qualification, experience, skill or other forms of quality assurance when appointing a provider,[3378] some corporate requirements, which are substantially adequate, must be met by the applicant to qualify for this appointment.[3379] Also, it is recommended that same or similar recommendations made regarding the appointment of LEOs be considered for the appointment of an Authentication Service Provider.[3380]

7.3.2.3 Obligation, power, operation and oversight by and of a Decryption Keyholder, Cryptographer and Authentication Service Provider

a. Obligation, power, operation and oversight by and of a Decryption Keyholder

Reiterating part of the earlier definition,[3381] a Decryption Keyholder is empowered to use any decryption key in his or her possession,[3382] execute or assist in the execution of a decryption direction, which is handed to the Decryption Keyholder by an authorised person in the conduct of an OCI,[3383] without which there is a delay in obtaining the required information in an OCI.

In the U.S., for example, because the LEA did not obtain permission from the Department of Justice as the authorised or legal authority that grants such order in the U.S. or the authority that would have provided a Decryption Keyholder to conduct an OCI, the LEA used a month to decode a WhatsApp communication in the investigation of a murder case without any assistance from the service provider.[3384]

[3377] Para 2.8 of Chapter 2 of this study.
[3378] Chapter VI of the ECTA.
[3379] Sections 38(2) (a)-(g), (3) (a) -(d), (4) (a) -(h) and (5) and 39-41 of the ECTA.
[3380] See para 4.4 of this study titled 'Specialised staff and training of law enforcement agencies in online criminal investigation' and see generally the other role players who are involved in the conduct of OCI in para 6.3 of this study.
[3381] Para 7.3.2.2(a) of this chapter.
[3382] Section 29(3)(a) of the RICA.
[3383] Section 29 (1) of the RICA.
[3384] Glover S 'Facebook's refusal to help police on murder case proves it is morally callous' http://www.dailymail.co.uk/debate/article-6132479/STEPHEN-GLOVER-Facebooks-refusal-help-police-murder-case-proves-morally-callous.html (Date of use: 5 September 2018).

The failure or refusal of the LEA in the U.S in this regard does not only result in unnecessary waste of time of the LEA to benefit from the urgency needed in the conduct of an OCI,[3385] but it is a breach of the right to the SOC because the issuing authority for an OCI direction, which would have put the precautionary measures of protecting the right to the SOC in place, was by-passed.

An authorised person may use the decryption key only in respect of the encrypted information in the conduct of an OCI.[3386] Within the period specified in the direction, the Decryption Keyholder must disclose the decryption key' or 'provide the decryption assistance 'which is necessary to obtain access to' and convert the encrypted information into 'an intelligible form' in the conduct of an OCI.[3387] The keyholder may disclose the decryption key or assist the authorised person only in the conduct of an OCI.[3388]

In emphasising the unreasonableness of the use of 'wind fall evidence' derived from the conscriptive online communication,[3389] the keyholder may not disclose any other information of a customer which is not stated in the direction to conduct an OCI,[3390] which the court did not address in the judgement in *AmaBhugane*[3391] in highlighting the inadequacy in RICA in this regard. It is noted that the right of a third party is not provided for in this regard,[3392] perhaps the omission of the protection of a third party in the Act was not intended.

Where a decryption key holder is 'not in possession of the decrypted information' or is incapable of fully complying with the decryption direction in the conduct of an OCI, he or she is encouraged, to the best of his or her ability, comply with the direction issued by the court,[3393] though the compliance must be within the general law of the RSA.

Where the key holder is in possession of different or combination of decryption keys in the conduct of an OCI, it is unnecessary to disclose the 'windfall decryption keys' if the initial key

[3385] Para 6.5 of Chapter 6 of this study.
[3386] Section 29(8)(a) of RICA.
[3387] Section 29(1)(a) & (b), (2)(a), (4) (a) &(b) of RICA.
[3388] Section 29(2)(b) and (3)(b) of RICA; *AmaBhungane v Minister of Justice* supra 98.
[3389] Paras 2.3.3 and 7.8 of this study.
[3390] Section 29(2)(c) of RICA; *AmaBhungane v Minister of Justice* supra 98.
[3391] *AmaBhungane v Minister of Justice* supra 98.
[3392] Para 6.14 of Chapter 6 of this study.
[3393] Section 29(5) (a) & (b) of RICA.

obtained is sufficient to access the encrypted information.[3394] In this instance, a keyholder is at liberty to select what key or combination of keys to disclose in complying with a decryption direction.[3395]

In the conduct of an OCI, a Decryption Keyholder must disclose to the authorised person 'all such information' which has been in his or her possession or some of such information which is no longer in the possession or such remaining information in the possession of the keyholder again[3396] due to the impossibility of the Fixed Line Operator providing routing and duplicating services to the Interception Centre.[3397]

Although not stipulated as the duty of a Decryption Keyholder, it is submitted that it is an aberration that, where a data is lost in transit in the custody of a Fixed Line Operator in the conduct of an OCI, there is no consequence for the impossibility of duplication and routing by the Fixed Line Operator of the entire results of the routing and duplication of the communication to the Interception Centre.[3398] The reason for lack of consequence is because the law condones the fact that the remainder of the data is still acceptable for communication to the Interception Centre by routing and duplication,[3399] thus constitutes a breach of the right to the SOC and creates a challenge in carrying out an oversight function on a Decryption Keyholder.

However, one of the oversight functions carried out on a Decryption Keyholder in the conduct of an OCI occurs where there is a criminal sanction against a Decryption Keyholder who acts in the dereliction of duty by failing or refusing to safely record, keep and disclose in full a decryption key in his or her possession to an authorised person.[3400]

[3394] Section 29(6)(a) of RICA; Paras 2.3.3 and 7.8 of this study.
[3395] Section 29(6)(b) of RICA
[3396] Section 29(7)(a)-(c) of RICA.
[3397] Para 7.14 of Schedule A of RICA Directive of Notice 1325 of 2005 of Gazette No 28271 of 2005 (RICA Directive 2005).
[3398] Para 7.14 of Schedule A of RICA.
[3399] Para 7.14 of Schedule A of RICA.
[3400] Section 51(4)(a) and (b) of RICA.

b. Obligation, power, operation and oversight by and of a Cryptographer

A Cryptographer may not provide services or products in the RSA without registering his or her particulars in the register.[3401] Although the word 'may' is used in this regard which is not mandatory, the word is however qualified in section 29 of the ECTA, which makes it mandatory because section 29 requires a Cryptographer to comply with some requirements before such services can be provided in the conduct of an OCI in the RSA.

In the operational conduct of an OCI by a Cryptographer, the register of Cryptographers, which contains the details and location of the Cryptographers and type of cryptography services rendered by a Cryptographer[3402] must not be disclosed, save to the employees of the Department of Communication who keep the register of Cryptographers.[3403] Such information can only be disclosed: in pursuance of a criminal investigation; in the enforcement of the Promotion of Access to Information Act; to a Cyber Inspector and; in any civil proceedings relating to the services provided by a Cryptographer.[3404]

A Cryptographer must operate within the RSA and render service to a person or business present or doing business in the RSA when the service or product is being used,[3405] thus guaranteeing and ensuring the sovereignty of the conduct of an OCI in the RSA against the U.S. principle of 'no server, no law'.[3406]

A Cryptographer is prohibited from disclosing confidential information or trade secret relating to the cryptography services or products in the conduct of an OCI.[3407]

One of the oversight provisions regulating the activity of a Cryptographer in the conduct of an OCI is the imposition of liability on a Cryptographer for contravening any of the provisions examined above.[3408]

[3401] Section 30 (1) of the ECTA.
[3402] Section 29 (2)(a)-(c) of the ECTA.
[3403] Section 31(1) of the ECTA.
[3404] Section 31(1) and (2)(a)-(d) of the ECTA.
[3405] Section 30(3)(a)-(c) of the ECTA.
[3406] Para 2.8 of Chapter 2 of this study.
[3407] Section 29(3) of the ECTA.
[3408] Section 32(2) of the ECTA.

c. Obligation, power, operation and oversight by and of an Authentication Service Provider

Although the accreditation of authentication services or products may be voluntary,[3409] however, an Authentication Service Provider must, in a reasonable way, execute their obligations and exercise their powers in supporting the conduct of an OCI in the following ways.[3410]

Firstly, in preventing intrusion and abuse in the conduct of an OCI, an Authentication Service Provider must reasonably provide security for the hardware and software systems and procedure of processing of services and products.[3411]

Secondly, an Authentication Service Provider must reasonably provide a 'level of availability, reliability, and correct operation' of the hardware and software systems and procedure of processing of services and products in the conduct of an OCI.[3412]

Thirdly and finally, an Authentication Service Provider must, in the conduct of an OCI, generally adhere to the security procedures accepted in contemporary society.[3413]

In supporting the conduct of an OCI, an Authentication Service Provider has a statutory obligation not to falsely hold out their products or services as accredited if not accredited, otherwise, such misrepresentation constitutes a criminal offence.[3414] Consequently and arguably, the criminalisation of the acts or omissions impliedly means that accreditation of services or products is not voluntary but compulsory,[3415] therefore, secures the integrity of the right to the SOC and the conduct of an OCI.

When accrediting an authentication service or product for purposes of supporting the conduct of an OCI, the ACA discretionally imposes any condition or restriction that is necessary for its

[3409] Section 35 of the ECTA.
[3410] Sections 38(2) (a) -(g), (3) (a) -(d), (4) (a) -(h) and (5) and 39 - 41 of the ECTA.
[3411] Section 38(2)(b) & (c) and (3)(a) of the ECTA.
[3412] Section 38(2)(b) &(c) and (3)(b) of the ECTA.
[3413] Section 38(2)(c) & (c) and (3)(d) of the ECTA
[3414] Sections 37(3) and 40(2) of the ECTA.
[3415] Section 35 of the ECTA.

operation.[3416] For example, for an Authentication Service Provider to be qualified to operate an online communication, certain accreditation criteria must be fulfilled in the accreditation of the authentic service or product. Amongst others,[3417] the criteria include the following: the financial and human capital capacity; *modus operandi* of processing of its products or services; 'the availability of information to third parties relying on the authentication of products or services'; 'regularity and extent of audits by an independent body' and any other factor which may be necessary[3418] to be considered for the safety and security of the SOC and conduct of an OCI.

Furthermore, in support of the conduct of an OCI, where an Authentication or Certification Service Provider provides services or products, the ACA may, before the accreditation of the authentication service or product, regulate in the following ways: 'the technical and other requirements which certificates must' comply with; 'the requirements for issuing certificates'; 'the requirements for certification practice statements'; 'the responsibilities of the certification service provider'; 'the liability of the certification service provider'; 'the records to be kept and how the length of time for which they must be kept'; 'requirements as to adequate certification suspension and revocation procedures' and 'requirements as to adequate notification procedures relating to certificate suspension and revocation'.[3419]

These requirements, if effectively implemented, would strengthen the integrity and security of the protection of the right to the SOC and the conduct of an OCI.

In supporting the conduct of an OCI by an Authentication Service Provider, the ACA has the discretion to suspend or revoke an accreditation upon satisfying that there is a breach of the condition for granting accreditation in section 38 and 40 of the ECTA.[3420]

In the suspension or revocation process, the ECTA provides for the following principles and practices: observance of due process; adequate notice of suspension or revocation; immediate notice of suspension for urgent matters, provided that there is an unlikelihood of an irreparable loss in online communication, the suspension of which does not exceed 90 days and right of

[3416] Section 38(5) of the ECTA.
[3417] Section 38(1)(a)-(e) of the ECTA.
[3418] Section 38(2)(a), (c)-(e) and (g) of the ECTA.
[3419] Section 38(4)(a) - (h) of the ECTA.
[3420] Section 39(1) of the ECTA

reply by an Authentication Service Provider; amongst others.[3421] These provisions ensure the protection of the right to the SOC and the conduct of an OCI.

Subject to pre or post accreditation conditions, an Authentication Service Provider is at liberty to terminate the accreditation issued by the ACA,[3422] thus the unilateral power to terminate an accreditation does not lie in the ACA alone, thus highlights —in another perspective— the principle of checks and balances, in lieu of the oversight of the ACA.

However, what is arguably concerning is the great risk posed in the discontinued services in an online communication if an Authentication Service Provider terminates the accreditation. The effect of the discontinuation is that absolute security and safety of data is required even after the termination of the accreditation by any of the parties. This is because the existing data will be in the hands of the party that terminates the contract, which can be used for other purposes for which the data was gathered. Therefore, it is recommended that the termination of accreditation should be the last resort or sparingly done and where it is done, the already acquired data by an Authentication Service Provider must immediately be taken over by another Authentication Service Provider under certain conditions.

In support of the operation of an OCI by an Authentication Service Provider, the minister is empowered to make regulation relating to the following, all of which is relatively adequate to ensure safe and secure conduct of an OCI regarding the: right and obligation of persons connected to the provision of accredited products or services; *modus operandi* on the administration and supervision of how the ACA makes the persons connected to the provision of accredited products or services comply with the obligation; practice and procedure for granting, suspending and revoking accreditation; accreditation fees to be paid; requirements or guidelines for information security; any other relevant issue that is necessary or expedient for the proper implementation of the chapter relating to the regulation of Authentication Service Provider.[3423]

However, it is noted that these provisions are inadequate in the following ways. Firstly, the word ‘may’ should be interpreted as ‘shall’, which is clear and unambiguous to anyone who

[3421] Section 39(2) (a)-(c) and (3) of the ECTA.
[3422] Section 39(4) of the ECTA.
[3423] Section 41 (a)-(f) of the ECTA

carefully reads the provision, given the necessity for strict compliance with the requirements in conducting an OCI. Secondly, there is no provision that the regulation be approved by the National Assembly before enforcement, which denies the National Assembly the power to serve as an oversight body in the performance of the function of the Minister of Communication while regulating the Authentication Service Provider in their intermediary role in the conduct of an OCI.

The ACA has an oversight function on the Authentication Service Provider in supporting the conduct of an OCI. Firstly, the ACA has the discretion to monitor the conduct, systems and operations of an Authentication Service Provider in order to comply with section 38 and other provisions of the ECTA.[3424] Secondly, temporary suspension of an Authentication Service Provider may be carried out by the ACA.[3425] Thirdly, in compliance with section 38 and other obligations of an Authentication Service Provider in the ECTA, the appointment of an independent auditing firm may be made by the ACA to carry out periodic audits of the Authentication Service Provider.[3426]

Finally, the public performs an oversight duty on both the Authentication Service Providers and the ACA.[3427] There is a publicly accessible database maintained by the ACA relating to recognised authenticated services or products, revoked accreditation and other information,[3428] which ensure the protection of the right to the SOC and the conduct of an OCI.

7.3.3 Role and management of the affairs and activities of a Cyber Inspector in conducting online criminal investigation

7.3.3.1 Introduction

RICA does not provide for the general powers of a recognised individual to conduct an inspection of an online communication save the power of a Decryption Keyholder, who deals with special cases.[3429] However the ECTA makes provision for the appointment and exercise

[3424] Section 36 (1)(a) of the ECTA.
[3425] Section 36(1)(b) of the ECTA.
[3426] Section 36(1)(a) - (c) of the ECTA.
[3427] Section 36(2) of the ECTA.
[3428] Section 36(2) of the ECTA.
[3429] Section 29 of RICA.

of powers of a Cyber Inspector who conducts both online and offline investigations of electronic communications,[3430] although this study places emphasis on the online function of a Cyber Inspector.

7.3.3.2 Description and appointment of a Cyber Inspector

A Cyber Inspector generally investigates and monitors any unlawful activity committed online and offline.[3431] The power of a Cyber Inspector to investigate is also performed on Cryptographic and Authentication Service Providers for general non-compliance and misrepresentation of *status quo*.[3432] Additionally, a Cyber Inspector performs an audit on the critical database administrator.[3433]

The Director-General of Communication may appoint a Cyber Inspector from the Department of Communication, the appointment of which is confirmed by a certificate signed by or on behalf of the Director-General in an advanced electronic signature.[3434] However, there is no statutory provision for the appointment of a Cyber Inspector in terms of academic, practical or experiential requirement.

In the engagement of a Cyber Inspector, the following observations are made concerning the appointment of a Cyber Inspector in the conduct of an OCI.

Firstly, it may be argued that appointing an outsider as a Cyber Inspector may invite infiltration into the sensitive terrain of online intelligence. However, limiting the appointment of inspectors to the Department of Communications only appears to be limiting the pool of resources that may be solicited outside the Department, thereby, adversely affecting the competitive competence of the inspectors that are protecting the right to the SOC and the conduct of an OCI.

[3430] Sections 80(4)(b)(i), 82(1) of the ECTA.
[3431] Sections 81(1)(a), (b)(i), (c)(i) &(ii) & (d), 82(1)(a)- (h) and 83(2)(a), (3)(a), (4) & (5) of the ECTA.
[3432] Section 81(1) (b) &(c) of the ECTA.
[3433] Section 81(1)(d) of the ECTA.
[3434] Section 80(1), (2) and (3) of the ECTA.

Secondly, it is submitted that given the high levels of risks involved in protecting the SOC and conducting an OCI, the power to sign the certificate of appointment of a Cyber Inspector[3435] should not be delegated to any other authority other than the Director-General to prevent abuse by other authorities in the Department of Communication. Accordingly, it is recommended that the National Assembly must be informed before the appointment of such a Cyber Inspector to ensure oversight on the appointing authority.

7.3.3.3 Obligations, powers, operations and oversight by, and of Cyber Inspectors

The powers of a Cyber Inspector include: accessing and searching information systems, extracting copies from the records in an information system, accessing and operating the operation of any computer, mandating a person in control of information to render technical assistance and making enquiries on the compliance of the provisions of the ECTA, amongst others.[3436] Anyone who obstructs or refuses to cooperate with the performance of any of these powers by a Cyber Inspector commits an offence.[3437]

It further appears in the powers of a Cyber Inspector that where LEAs rely on section 81(2) of the ECTA to conduct an OCI, such LEAs would be bypassing the Interception Centre, which, in accordance with the submission in this study, the Interception Centre is supposed to have the sole obligation, power or responsibility of technically intercepting an online communication for OCI purposes in the RSA.[3438] The fact that the ECTA and RICA do not contain any harmonious provision in this regard creates some serious doubt about any inter-working relations or recognition of the role of each other in the conduct of an OCI in the ECTA and RICA. Therefore, there is a tendency for abuse of power in section 81(2) of the ECTA, which requires the necessary harmonisation of the ECTA and RICA as section 82(3) of the ECTA is harmonised with the CPA.

Furthermore, in the operational conduct of an OCI by a Cyber Inspector, the provisions on the performance of the function of a Cyber Inspector in the ECTA do not comply with the object of RICA, especially because the ECTA does not provide that an OCI be conducted in respect

[3435] Section 80(2) of the ECTA.
[3436] Sections 82(1) (a), (c), (f), (g), (h) &(i) of the ECTA.
[3437] Section 82(2) of the ECTA.
[3438] Para 6.11 of Chapter 6 of this study.

of serious offences *only*[3439] as provided by RICA.[3440] Given that an OCI is conducted in respect of serious offences *only*[3441] (including instances of 'ascending serious offence' theory),[3442] the non-identification or non-definition of an offence in the ECTA[3443] creates a lacuna if a Cyber Inspector conducts an OCI in respect of such offences. This is because the conduct of an OCI by a Cyber Inspector will be *ultra vires* of the powers of the inspector based on the philosophy of RICA as the major legal framework in conducting an OCI of serious offences *only*.

Importantly, in the operation of a Cyber Inspector, the ECTA provides for the inspection, search or seizure by 'any statutory body',[3444] which is too broad in the context of the application of the provisions of RICA. This is because the phrase 'any statutory body' includes other statutory bodies other than the LEAs recognised by RICA and bodies that do not fall under the category of independent authorities recommended in this study to be listed under RICA as OCI applicants.[3445]

However, it is submitted that the ECTA provisions should be applicable to the groups recommended in this study which include Chapter Nine Institutions in the Constitution, some State departments, independent statutory bodies and private entities.[3446]

The ECTA accords a magistrate the power to grant a warrant concerning both the conduct of an OCI and a non-OCI.[3447] However, it is submitted that the issuance of a warrant concerning the conduct of an OCI be limited to a judge who shall be statutorily certified to have undergone an accredited training in Electronic Investigation[3448] and is designated to issue such a warrant as prescribed in RICA.[3449] This is because courts themselves have admitted to the existence of dearth of knowledge of cyber law by judges in adjudicating on the conduct of an OCI.[3450]

[3439] Chapter XII of ECTA.
[3440] Para 6.3.2 of Chapter 6 of this study.
[3441] Paras 6.3.2 of Chapter 6 of this study.
[3442] Para 6.3.1 of Chapter 6 of this study.
[3443] 81(2) (a) and (b) of the ECTA.
[3444] Section 81(2) of the ECTA.
[3445] See the definition of 'applicant' in section 1 of RICA and para 4.2 of Chapter 4 of this study.
[3446] Para 2.11 of Chapter 2 and 4.2 of Chapter 4 of this study. Although RICA does not allow the Financial Intelligence Centre (FIC) to directly conduct an OCI, however, it is already doing by submitting applications to the designated judge to conduct an OCI, JSCI Reports 2016 at 46.
[3447] Section 83 of the ECTA.
[3448] Paras 4.3.8 and 4.6 of Chapter 4 of this study.
[3449] Para 6.9 and 6.10 of Chapter 6 of this study.
[3450] *AmaBhungane v Minister of Justice* supra 106.

In the U.S., fear is also expressed that judges who have been on the bench for decades are 'technology illiterates' who may not understand the striking difference of a search of a suitcase at the airport and copying and storing of the content of a laptop and cell phone by LEAs.[3451]

One of the instances of accountability of a Cyber Inspector in the conduct of an OCI is that an inspector is required to produce the certificate of appointment in the performance of the relevant function of the office of a Cyber Inspector,[3452] thus ensures checks and balances on a Cyber Inspector in this regard.

Furthermore, there is an existence of check and balance on the powers of and oversight by a Cyber Inspector on LEAs.[3453] This is because statutory authorities —including the LEAs examined in this study—[3454] do not directly conduct an online investigation under the ECTA through the assistance of a Cyber Inspector without a conditional approval from the Department of Communication which provides the oversight function on Cyber Inspectors and LEAs in this regard.[3455]

Nevertheless, granting such administrative powers to the Department of Communication to determine which statutory authority —including LEAs in RICA— is assisted by a Cyber Inspector and under which conditions such statutory authority is assisted[3456] sweeps away the independence of the statutory authority that is seeking for such assistance from the Cyber Inspector in the administrative process. This is because this provision circumvents the overall object of RICA which does not place the conduct of an OCI in any administrative body but a judicial authority.[3457]

It is important to note that this study even questions the rationale for including a magistrate court —which is not an administrative authority— as part of the judicial authority that exercises jurisdiction over the conduct of an OCI, more particularly section 205 of the CPA, the application of which is examined in this study.[3458] Therefore, the sanctity of judicial

[3451] Greenwald *U.S. Filmmaker repeatedly detained at border* 185 and 187.
[3452] Section 80(4) of the ECTA.
[3453] Para 2.11 of Chapter 2 and Chapter 4 of this study, more particularly para 4.2.
[3454] Para 2.11 of Chapter 2 and Chapter 4 of this study, more particularly para 4.2.
[3455] Section 81(2)(a) & (b) of the ECTA.
[3456] Section 81(2) (a) & (b) of the ECTA.
[3457] Para 6.2.7 of Chapter 6 of this study.
[3458] Paras 6.7 and 6.12 of Chapter 6 of this Chapter.

adjudication in conducting an OCI is tampered with where the Department of Communication first of all censors the LEAs in the conduct of an OCI.

Finally, it is implied that a Cyber Inspector is accountable to the Director-General of the Department of Communication. However, it is submitted that a Cyber Inspector should be obliged to submit periodic reports to the National Assembly to ensure greater accountability and oversight because the Director-General appoints the Cyber Inspector. Worse still, both the Cyber Inspector and Director-General are in the same executive arm of government, which may prove difficult to ensure checks and balances.

7.3.4 Role and management of the affairs and activities of the National Communication Centre in conducting online criminal investigation

The role and management of the affairs and activities of the NCC are not stipulated in the constitutional, statutory or regulatory provisions creating and guiding its operation to conduct an OCI unlike the SSA, which is a creation of the Constitution and recognised by RICA as one of six applicants to conduct an OCI in the RSA. The NCC is one of the four units under the SSA.[3459]

It is on record that the NCC has been impeccably reported and confirmed by the authorities and the public that it has been conducting indiscriminate, unfettered, unreasonable, irrational and unjustifiable specific and bulk interceptions[3460] of territorial in-coming and out-going online communications in the RSA without complying with the provisions of RICA or any other relevant law.[3461]

[3459] Others are: a) Domestic branch of SSA (formerly known as 'National Intelligence Agency'), c) Foreign branch of the SSA (formerly known as 'South African Security Service') and c) Office of the Interception Centre ('OIC'), Swart H Communication 'Surveillance by the South African Intelligence Services' at 1 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use:13 August 2016); JSCI Report 2016 at 20 - 21.

[3460] It is noted that 'interception' is a broad word which is used as such for both civil and non-civil and technical and non-technical purposes. However, OCI is a specific and narrow form of interception, which is conducted in relation to the commission of a serious offence, see para 2.5 of Chapter 5 of this study.

[3461] Parliament of the Republic of South Africa 'Announcement, Tablings and Committee Reports' No 164 -2016 para 4.7.3 at 20 (JSCI Report 2016); Swart H 'Government spies on you'; Swart H Communication 'Surveillance by the South African Intelligence Services' 2016 at 3 -4, 7, 8, 9, 28 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use:13 August 2016); State Security Agency 'About Us' http://www.ssa.gov.za/AboutUs.aspx (Date of use:15 April 2016).

It is important to note that the conduct of an OCI includes investigation conducted in online communication that has Internet and non-Internet based operating systems in which territorial in-coming and out-going online communications occur on the Internet.[3462] Consequently, given the almost indispensable operation of the interoperability or convergence principle in Internet technology, which requires cross-border communications channels before the communication is delivered to the recipient in the RSA,[3463] it is submitted that virtually all online communications are subject to online interception by NCC. This is because NCC unlawfully conducts online interception of incoming and outgoing communications in the RSA.

Despite the recommendation in 2010 by the JSCI of Parliament that the operations of NCC should be properly legislated[3464] and adequately regulated because it usurps the function of SSA and other LEAs in the conduct of an OCI, no attempt has been made till date nor is there any solution in sight to regulate the activities of NCC.

Therefore, this makes it difficult to enforce any form of accountability and oversight principle against NCC for the unlawful conduct of an OCI in the RSA.[3465] Therefore, the following is recommended:

Firstly, NCC and its operation should be abolished because NCC is an illegal authority or operates illegally, given that the umbrella body, which is the SSA, has the constitutional and statutory authority to conduct an OCI in the RSA. The abolishment of the NCC and its operation are premised on the fact that the function performed by the LEAs recognised in RICA is duplicated by the NCC.[3466]

Put differently, each LEA —including the SSA, which has some sub-units within which domestic and cross border investigations are conducted— is capable of making an application to conduct an OCI in out-going and in-coming online communications and in purely domestic online communications without any necessity to assign this function to NCC.[3467]

[3462] See paras 2.8 of Chapter 2 of this study.
[3463] Paras 2.3.2 and 2.8 of this chapter.
[3464] Para 4.10.3 of Annual Report of the Joint Standing Committee on Intelligence for financial year ending 31 March 2010.
[3465] Swart 'Communication surveillance by the South African Intelligence Services' 2016 at 28 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use:13 August 2016).
[3466] Paras 4.3.5 and 4.4.5 of Chapter 4 of this study.
[3467] Paras 4.3.5 and 4.4.5 of Chapter 4 of this study.

In the worst-case scenario that may warrant the temptation of allowing NCC usurp the function of the SSA, the latter may make an application under the first class and stage of crime commission which is the 'lowest reasonable suspicious' standard of investigation for an offence posing '*severe* national risk'[3468] to address what NCC would have addressed. Therefore, there is no legal, ethical or technical justification to condone or retain the operation of NCC in the conduct of an OCI in the RSA.

Secondly, in the alternative, although without conceding to its retention, however, should NCC be retained under SSA, it should be reformed[3469] and merged with the domestic and foreign divisions of SSA and that the same or similar regime that governs the role and management of the affairs and activities of LEAs and organs of government or entities involved in the conduct of an OCI should also govern the operation of NCC.[3470] If the NCC is solely charged with the responsibility of conducting territorial in-coming and out-going OCIs,[3471] it takes away almost the whole functions of SSA because the NCC will be usurping the functions of the domestic and foreign ID-SSA[3472] by virtue of the fact that the NCC is not regulated by any law.

Nevertheless, it is noted that the power that may be granted to the NCC should not be mistaken with the cross-border OCI power granted to SAPS, HAWKS and SSA under the MLA agreement in section 16(3)(c) and (5)(a)(iv) of RICA. This provision deals with the conduct of cross-border OCI, which is not within the exclusive jurisdiction of the RSA or any foreign country.

In conclusion, since the NCC is an illegal authority, it is inconceivable to consider the oversight by and of NCC because is it tantamount to legitimising its authority and operations.

[3468] Paras 6.3.3.2 (b)-(d), 6.3.3.3(e), 6.3.3.4(b), 6.3.3.5(b)-(d) and 6.4.5 of Chapter 6 of this study.
[3469] Right2Know at 36 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).
[3470] See generally Chapter 4 of this study.
[3471] This will include roaming services.
[3472] Para 4.3.5 of Chapter 4 of this study.

7.3.5 Role and management of the affairs and activities of Online Communication Service Providers in conducting online criminal investigation

While a Telecommunication Service Provider —as provided in RICA— is a narrow description of online communication agents,[3473] a broader description which is 'Online Communication Service Provider' is adopted in this study which includes Mobile Cellular Operators, Fixed Line Operators and Internet Service Providers whose direct and indirect roles impact on the right to the SOC and conduct of an OCI. An Online Communication Service Provider performs many roles in the conduct of an OCI,[3474] some of which are as follows.

Firstly, an Online Communication Service Provider must install a system that has an interception solution, otherwise, its failure or refusal to do so constitutes a criminal offence.[3475]

Secondly, an Online Communication Service Provider in conducting an OCI must receive an OCI direction and 'route the duplicate signals' of real-time or archived communication or 'make available the necessary assistance' to the 'designated Interception Centre'.[3476]

Pursuant to the effect of section 205 of the CPA, an Online Communication Service Provider intercepts a metadata and delivers the same to the LEAs without going through the Interception Centre.[3477] In the case of real-time communication, an Online Communication Service Provider '*immediately*' routes the duplicate signals of the communication to the concerned designated Interception Centre or '*immediately*' provides the communication to the concerned LEA.[3478] In the case of an archived communication, an Online Communication Service Provider routes the duplicate signals *within the specified period* in the direction to the concerned designated Interception Centre or provides the communication '*within the specified period*' to the concerned LEA.[3479]

[3473] Popoola *Liability of ISPs* at para 2.4.
[3474] Swart 'Communication surveillance by the South African Intelligence Services' 2016 at 3-4 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use: 13 August 2016).
[3475] Sections 30(1) (a), (2)(a)(i)&(ii)(aa)&(bb), (3)(i)-(v), (4),(5)(a)(i)&(b) and 51(3)(a)(i)&(ii),(3A)(a), (5)(b) & (bA)(i) of RICA; Caproni *Lawful electronic surveillance* 204.
[3476] Section 28(1) (b) (i) &(ii) and 30(1)(a) of RICA; Para 4.7.2 of JSCI Report 2016 at 19.
[3477] Para 5.11 of this study titled 'Application of section 205 of the CPA and other law'.
[3478] Section 28(2) (a) (i) &(b)(i) of RICA.
[3479] Section 28(2) (a) (ii) &(b)(ii) of RICA.

However, there is a general non-intelligence or non-investigative oriented nature of the operations, administration and supervision of an Online Communication Service Provider, leading to the compromising stance of its employees in the integrity and security of data in the case of *State v Naidoo*.[3480] Also, there is the need to ensure reasonable centralisation of the management of data in online communication, more particularly in terms of the management of storage; sorting, copying and sharing; using; examining, and destruction of data. For these foregoing reasons, it is submitted that an Online Communication Service Provider should not be involved in dealing directly with the LEAs or LEOs as described above.[3481] Rather, reliance should be placed on the operation of a *Popoola QOCI* protocol which reasonably cures the defects in the conduct of an OCI application and direction in RICA provisions.

Thirdly, the duty of an Online Communication Service Provider is to provide storage facility of online communication for buffering and non-buffering purposes.[3482] In managing the activities of an Online Communication Service Provider in conducting an OCI and storing an online communication, an Online Communication Service Provider must, not less than *three months*,[3483] comply with the directive issued by the relevant ministers and amended or withdrawn in like manner in which effect can be given to the services and security of interception and storage of data.[3484]

Although there is provision for wide consultation in this regard (which excludes consultation with licensed Online Communication Service Providers regarding the issuance of the directive in section 30(2)(a)(i)-(iii) of RICA), the non-inclusion of National Assembly to serve as a check and balance in this process is inadequate.

RICA sets out the contents of the Directive implemented by the relevant ministers which are examined as follows:[3485]

[3480] *State v Naidoo* supra 521 B-E; Right2Know 16 and 18-19 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).
[3481] Section 28(2) (a) (i) &(ii) &(b)(i) & (ii) of RICA.
[3482] Paras 1, 4.1(a), 4.6, 8.2(a), 8.4, 10.1, 10.2, 10.4, 10.5, 10.7(a), 10.8 of Schedule A of RICA.
[3483] Section 30 (2)(b) of RICA.
[3484] Section 30(2)(a) & (6) of RICA.
[3485] Section 30(2) of RICA.

i) RICA stipulates how an Online Communication Service Provider provides facilities that are capable of intercepting and storing online communication.[3486] However, the authorities have not complied with the technical requirement of updating the interception devices in the RSA.[3487]

For example, it is argued that the current system used by MTN —one of the Telecommunication Service Providers in the RSA— to verify the fraud of unlawful access to the right to the SOC by an erring employee under the fraud management system. The system requires an employee under the fraud management unit to, first of all, access the phone record of a subscriber without deploying software to conduct the fraud investigation and without breaching access to the online communication[3488] is obsolete and constitutes a secondary breach of the right to the SOC.

This is because if the interception devices had been updated, an internal fraud investigator from MTN would not have conducted a physical investigation in the manner it was conducted in MTN case. Thus, the end result is that a subscriber is in a double jeopardy condition because of a breach of the right to the SOC by the internal fraud investigator in MTN the second time after an unknown intruder had initially done so, necessitating the internal investigation by MTN.

In ameliorating this problem, an Online Communication Service Providers should be compelled to develop internal protection rules in their contract with subscribers to address all issues of breaches of the right to the SOC including the: security measures protecting users especially the number or identity of subscribers; competence, independence and security status of employees entitled to conduct an OCI in this regard.[3489] Such rules must be subject to techno-legal approval by the ICASA, Department of Justice and National Assembly.

[3486] Section 30(2)(a)(i) of RICA.
[3487] JSCI Report 2016 at 20.
[3488] Right2Know 'Spooked- Surveillance of Journalists in SA' 18-19 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018 at 7 (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).
[3489] Right2Know at 39 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

ii) RICA provides for the 'security, technical and functional requirements of the facilities and devices' for the interception and storage of online communication by Online Communication Service Providers,[3490] which are implemented in RICA Directive.[3491] Nevertheless, the authorities have not considered the issuance of a directive to Online Communication Service Providers to compel the configuration of their internal online communications in a compartmentalised and pass-worded compartmentalised manner in the protection of the right to the SOC[3492] and the effective conduct of an OCI despite the existence of such legal framework.[3493]

Furthermore, the authorities have failed or refused to take advantage of this provision to configure a system that will operate *Popoola QOCI* protocol,[3494] which will put an end to the techno-legal problem of unlawful interception of online communication by unauthorised Online Communication Service Providers, Interception Centres or at any other point in an online communication protocol without a direction from the court.
[3495]

iii) RICA, through the various relevant ministers, sets out the type of online communication that must be stored between *three and five years*,[3496] the period of which is objected to by the United Nations and the court.[3497] The period also contradicts the recommendation of the JSCI of Parliament that the minimum period for storage in a mobile filing system in the conduct of an OCI is five years in pursuance of the Archival Act[3498] while some jurisdictions consider a maximum of two years and for some others, it is one and half years.[3499]

Nonetheless, although section 30(8) of RICA enables the relevant ministers to apply the proportionality principle in section 30(2)(a)(iii) of RICA relating to the period of storage of data, however, the former provision is inadequate for the following reasons.

[3490] See s 30(2)(a)(ii) (aa) and (bb) of RICA.
[3491] Para 7.7 of Schedule A of RICA Directive 2005.
[3492] Paras 2.2, 2.3.1 and 2.3.2 of Chapter 2 of this study.
[3493] Paras 7.3, 7.4, 7.7, 7.11 and 7.22 of Schedule A of RICA Directive 2005.
[3494] Para 6.11 of Chapter 6 of this study.
[3495] Para 5.10 of this study titled 'Techno-legal quadruple application'.
[3496] Section 30(2)(a)(iii) of RICA; *AmaBhungane v Minister of Justice* supra 33 and 85.
[3497] *AmaBhungane v Minister of Justice* supra 91, 93, 95 and 96.
[3498] JSCI Reports 2016 at 56.
[3499] *AmaBhungane v Minister of Justice* supra 89(1), 93.

Firstly, the provision on the application of the proportionality principle regarding the period of storage of data is ambiguous in section 30(8) or generally in RICA, because it is not clear on whether the principle applies to the conduct of an OCI *prospectively* or *retrospectively*,[3500] thus, infringes the right to the SOC because of the disproportionate conduct of an OCI.

Secondly, no specific guideline exists or is published to determine the merit of the application of Online Communication Service Providers to reduce the period of storage of intercepted data from five years to any other period of interception,[3501] thus, renders the principle of proportionality irrelevant.

Nevertheless, in *AmaBhugane*, the High Court held that the minimum period of storage of data should be six months instead of the minimum three years,[3502] though the position of the court is vehemently contested in this study based on the proportionality principle.[3503] However, it is noted that whatever proportionality principle that is applied, the concept of online conscription which perpetually records and stores online communication overrides any form of the proportionality principle.[3504]

iv) RICA prescribes that its Directive must contain the following or any other matter that may be deemed necessary for the conduct of an OCI:[3505] capacity required for conducting an OCI; requirements for the technical operation of the system for the conduct of an OCI and storage of data obtained; requirements expected from Online Communication Service Providers to connect with Interception Centres; manner of how Online Communication Service Providers route duplicate signals of online communications to the Interception Centres in terms of section 28(1)(b)(i) of RICA; manner of how Online Communication Service Providers route real-time or archived online communication to the Interception Centres in terms of section 28(2)(a) of RICA.[3506]

[3500] Para 2.3.3.7 of Chapter 2 of this study.
[3501] Section 30(2) & (8) of RICA.
[3502] *AmaBhungane v Minister of Justice* supra 40, 93, 95 and 96.
[3503] Paras 5.3.4, 5.3.6 and 5.4 of Chapter 5 of this study.
[3504] Para 2.3.3 of Chapter 2 of this study.
[3505] Section 30(3)(a)(i)-(v) & (b) of RICA.
[3506] Section 30(3)(a)(i)-(v) of RICA.

Although government authorities do not bear the technical, investment, maintenance and operating costs of interception devices by Online Communication Service Providers,[3507] the compensation payable by government to Online Communication Service Providers and Decryption Keyholder are the direct costs incurred in hiring personnel and administration,[3508] which assist in ensuring effective and efficient conduct of an OCI. These personnel and administration costs must be related to making a facility, device or telecommunication system available and disclosing decryption key and provision of decryption assistance.[3509] The provision for compensation is adequate in terms of subjecting the approval of the directive on the costs to be paid to the authorities or powers of the National Assembly.[3510]

Finally, aside from the executive checks and balances of an Online Communication Service Provider by the relevant ministers[3511] in the areas examined above and the functions that an Online Communication Service Provider performs, failing which its accountability is raised by the persons, entities and authorities on the other side of the divide; it is regrettable that no provision requires an Online Communication Service Provider to submit a report to National Assembly on the record or statistics of the conduct of an OCI, including the non-judicial interception.[3512]

7.3.6 Role and management of the affairs and activities of interception centres in conducting online criminal investigation

7.3.6.1 Obligation of interception centres

RICA provides for the creation of one or more Interception Centres which functions are central to the broader conduct of interception of communication —more specifically the conduct of an OCI— the communication of which is required to be routed by an Online Communication Service Provider to the Interception Centres in the RSA. However, some interceptions are not routed to the Interception Centres but directly made available to the LEAs or LEOs that request for the interception,[3513] which this study opposes the direct interception due to its abuse.

[3507] Section 30(5) (a) (i) &(ii) & (b) of RICA.
[3508] Section 31(1)(a)(i), (3) of RICA.
[3509] Section 31(2)(a)(b)(i)-(ii) of RICA.
[3510] Section 31(4) of RICA.
[3511] Section 30(2) of RICA.
[3512] Para 6.2 of Chapter 6 of this study.
[3513] Sections 28(1) (b) (i) &(ii), (2) (a) (i) &(ii) & (b)(i)(ii) and 32(1) of RICA; Para 7.3.5 of this chapter.

7.3.6.2 Establishment of interception centres

RICA provides for a multi-ministerial authority to establish Interception Centres[3514] as examined below.

Firstly, given that online communication and interception occur remotely or virtually and that the only Interception Centre which exists in the RSA covers the entire cyber sovereignty of the RSA which can be coordinated from one Interception Centre due to the unimaginable advanced technological development, it is techno-legally unnecessary to establish more Interception Centres because it will amount to duplication of functions, interceptions and resources, which will adversely impact on the effectiveness, efficiency and funding of the LEAs in conducting an OCI.[3515]

Secondly, in light of the complexities and uncertainties involved in power-sharing among political parties, political differences and interference and indiscriminate display of unilateralism of some members of the executive arm of government in adversely influencing some LEAs and government policies in recent time,[3516] the exercise of multi-ministerial authority to techno-legally and merely establish one or more Interception Centres is unnecessary and cumbersome. However, this multi-ministerial authority may be necessary in in other functions where the exercise of multi-ministerial authority may be required for accountability and oversight and cooperative governance purposes, amongst others. One of the reasons for the condemnation of these complexities and uncertainties is that the mere establishment of one or more Interception Centres should not create an unnecessary ceremony or protocol.

Another reason for opposing these complexities and uncertainties is that there is an emerging unlikelihood of the unity of purpose, where cabinet ministers and other public officials in the same and even the majority political party have openly, blatantly and publicly opposed each other on issues of national interests that require urgent attention. For example, a cabinet minister of communication —who is part of the establishing authority of the Interception

[3514] Section 32(1)(a) of RICA.
[3515] State Security Agency 'National Communications Branch' http://www.ssa.gov.za/AboutUs/Branches/NationalCommunications.aspx (Date of use: 12 January 2018)
[3516] See generally Chapter 4 of this study.

Centre—[3517] refused to comply with the instruction of its party to deploy the long-overdue digital broadcast technology in the RSA to comply with the compulsory international standards.[3518]

In addition, a cabinet Minister of Finance of a governing party (who is part of the establishing and management authority for the Interception Centre)[3519] threatened on Twitter —an online social platform— to withhold budgetary allocation to Gauteng Province —run by its party— for reasons that are not justifiable in fact and law.[3520] The threat by the Minister of Finance was based on the opposition to the inconclusive debate on the cancellation of o-toll collection in Gauteng Province.[3521] The minister, in his personal capacity, regarded as conclusive and unilaterally and severally opposed to its further public debate against the collective decision of his political party which earlier on declared the debate open and called for consultative conflict management approach on o-toll collection.[3522]

These two illustrations may not absolutely be conclusive to reject the exercise of a multi-ministerial authority to establish one or more Intercept Centres. However, the illustrations can, at the same time, not be dismissed to hold that the exercise of a multi-ministerial authority in this regard to establish one or more Interception Centres as absolutely unnecessary.

In conclusion, it is recommended that the establishment of the Interception Centre should not be left to the whims and caprices of any individual in government —including the Minister of State Security. Rather, the Interception Centre should constitutionally be protected in an Act of Parliament as a single, separate and unique intelligence service. The Interception Centre should also be categorised on the same or similar legal pedestal or status with SAPS, and SSA[3523] and listed under Chapter Nine Institutions,[3524] which do not require presidential or

[3517] Section 32(1)(a) of RICA.
[3518] Gedye L 'Faith Muthambi likely to bear brunt of the backlash over digital fail' https://mg.co.za/article/2016-06-02-backlash-likely-over-digital-fail (Date of use: 29 September 2017).
[3519] Section 32(1) of RICA.
[3520] Omarjee L 'Mboweni vs Makhura: Tense standoff over e-tolls' https://www.fin24.com/Economy/mboweni-vs-makhura-tense-standoff-over-e-tolls-20190705 (Date of use: 5 September 2019) (Omarjee L https://www.fin24.com/Economy/mboweni-vs-makhura-tense-standoff-over-e-tolls-20190705 (Date of use: 5 September 2019).
[3521] Omarjee https://www.fin24.com/Economy/mboweni-vs-makhura-tense-standoff-over-e-tolls-20190705 (Date of use: 5 September 2019).
[3522] Omarjee https://www.fin24.com/Economy/mboweni-vs-makhura-tense-standoff-over-e-tolls-20190705 5 September 2019).
[3523] Sections 199 (1) and 209 (1) of the Constitution.
[3524] Chapter Nine of the Constitution.

cabinet fiat in terms of their establishment and other incidental matters. In this way, the online interception executing authority, function and operation of the Interception Centre will not be compromised.

A centralised online interception system, as a Chapter Nine Institution, creates an easy, effective and efficient supervision and regulation of the OCI environment. A centralised online system of interception further justifies the application and practice of an OCI as a non-physical method of investigation, which it is supposed to be used as an OCI procedure, in pursuance of the execution of the proposed audio and audio-visual tele-warrant and *Popoola QOCI* protocol principles in the conduct of an OCI.[3525]

7.3.6.3 Appointment and specialised skill for interception centres

Firstly, the requirements of consent and security clearance from a prospective seconding LEO —as a substantive or acting head and members of the Interception Centre—[3526] and the constitutional principle of cooperative governance[3527] from another perspective[3528] generally enrich the invaluable pool of human resource available in an OCI environment.

However, given the complex and intrusive nature of the conduct of an OCI in online communication, there is no requirement that LEOs who are seconded from other LEAs must have a special skill, knowledge, expertise or experience in the field of conducting an OCI, as a professional activity unlike accounting, law, medicine etc. which are guided by minimum practising requirements. It is therefore recommended that the activity and actors involved in the conduct of an OCI be recognised as a professional activity and experts or professionals who are expected to have some certified knowledge in OCI as earlier examined in this study.[3529]

Secondly, the strict provision that, on request by the Minister of SSA, the head of the Interception Centre is appointed only by secondment by four authorities[3530] is arguably deficient. Essentially, the provision for appointing an in-house person only from the pool of

[3525] See para 6.11 of this chapter.
[3526] Section 34(1), (3), (4)(a) & (b) and (5) (b)&(c) of RICA.
[3527] Chapter 3 of the Constitution. Section 35(3) and 36 (4) of RICA.
[3528] See the principle of cooperative governance from another perspective in the first point in 6.3.5.3 of this study.
[3529] Paras 4.3.8 and 4.6 of Chapter 4 of this study.
[3530] Sections 34(4) (a) (i) -(v), 36(1) of RICA.

resources in the security cluster might be beneficial to the intelligence cluster because of the effective utilisation of its in-house resources and institutional knowledge. Nevertheless, the downside of this regime is that it impliedly excludes anyone outside the immediate environment of LEAs —who may have an abundant pool of resources— from aspiring to become the head of Interception Centre.[3531]

Another adverse implication of this regime is that the unnecessary, personal and subjective loyalty to the appointing authorities in the appointment of in-house persons[3532] is inherent, which has the tendency of adversely affecting the competence, independence and the accountability of a LEA or LEO in conducting an OCI.

However, it is submitted that given that the Interception Centre is one of the technical engine rooms for the conduct of an OCI, which must be independent; the appointment by secondment of the head of the Interception Centre should be abolished. Rather, the appointment should be conducted according to the normal or a publicly open recruitment process that will avail every internal and external qualified candidates the opportunity of being considered for appointment as the head of the Interception Centre.

Furthermore, the appointment of the head of the Interception Centre should not be left in the hands of any sole appointing political executive authority but in conjunction with Parliament. Accordingly, the Director of the OIC appoints the head of Interception Centre from the list of most qualified, competent and independent candidates presented by Parliament from a publicly open recruitment process. In the appointment process, the fact that the incumbent will undergo security clearance[3533] allays the fear that the incumbent might be an infiltrator.

[3531] For example, the banking sector secured the services of former director general of Home Affairs. Although the two sectors have different units which might be related, if the banking sector had stipulated that any one gunning for the top position in the bank must recently have worked in the banking sector in the last five years must have undermined the invaluability of wealth of experience that will be brought from the Home Affairs Department to the banking sector, see online source, Pijoos I 'Home Affairs DG Mkuseli Apleni resigns' https://mg.co.za/article/2018-07-23-home-affairs-dg-mkuseli-apleni-resigns (Date of use: 24 August 2018).

[3532] News24 'Loyalty to factions vs the state: A blurring of lines' https://www.news24.com/Columnists/GuestColumn/loyalty-to-factions-vs-the-state-a-blurring-of-lines-20190407 (Date of use: 4 August 2019).

[3533] Section 34 (5)(c) of RICA.

7.3.6.4 Operation and funding of interception centres

Firstly, in the effective and efficient operation of the Interception Centre, the provision that the Minister of State Security enters into SLAs with the relevant ministers concerning the provision of services by the Interception Centre should be made mandatory between the Executive Director of IPID, National Commissioner of SAPS (because of the long standing historic experiential tensions between the duo), the National Director of NPA and the Director of the OIC.[3534]

These provisions assist in the implementation of the constitutional principle of cooperative governance[3535] in the conduct of an OCI. For example, in resolving the retaliatory investigations between SAPS and IPID[3536] (wherein the latter is the watchdog of the former), both parties signed an MoU with the mediating role of the court[3537] on the need to address 'conflict of interest' on investigations between the two institutions.

The MoU is to the effect that any member of the two institutions who is criminally implicated and is being reasonably and justifiably investigated cannot be a part of a team to investigate the other institution,[3538] which complies with the natural law of '*nemo judex incau sa sua*'. Accordingly, the head and leadership of the Interception Centre should enforce the principle of cooperative governance by having a similar MoU with other institutions that have statutory or equitable power to conduct an OCI to address the foregoing tensions between or among the LEAs.

Secondly, in the operation of the Interception Centre, RICA empowers several relevant ministers[3539] to share in the responsibility of equipping, operating, maintaining and

[3534] There is the need to expunge the word 'may' in the later provision, see section 32(4) and (5) of RICA. It is noted that though the word 'may' be mandatory in some circumstances, however, in order to avoid erroneous interpretation, the word 'shall' is appropriate.
[3535] Chapter 3 of the Constitution.
[3536] Both agencies are empowered to conduct OCI in RICA, para 4.2 of Chapter 4 of this study.
[3537] Para 7.7 of this chapter.

[3538] Bateman B 'SAPS, IPID working to avert conflict of interest in cases' http://ewn.co.za/2018/07/05/saps-ipid-working-to-avert-conflict-of-interest-in-cases (Date of use: 15 July 2018).

[3539] Section 32 (1) of RICA.

administering one or more Interception Centres.[3540] The ministers are also empowered to share in the responsibility of 'acquiring, installing and maintaining connections' between Online Communication Service Providers and Interception Centres. However, the Minister of State Security is empowered to exercise final responsibility in terms of the administration and functioning of Interception Centres.[3541]

Although the supervisory departments —such as SSA, Treasury, Communication and Telecommunication— are for a while statutorily empowered to establish the Interception Centres, which is, anyway, rebutted above,[3542] the Interception Centre is generally and regrettably not independent of the aforementioned departments in terms of the powers mentioned herein and below. This is because there is no statutory power granted to the head of the Interception Centre herein but derives its function from the whims and caprices of the Minister of State Security who takes 'final responsibility' over the administration and function of Interception Centre.[3543]

Worse still, the provisions that the head and members of the Interception Centre may exercise powers and functions conferred or imposed upon or assigned to the head of Interception Centre by the Director of the OIC or under RICA and that such functions must be 'subject to the control and direction of the Director' of the Office for Interception Centre[3544] highlight the substantial absence of independence of the Interception Centre. The application of these provisions spells doom for the protection of the right to the SOC and justifiable conduct of an OCI.

However, the provision for power-sharing formula between the Director of the OIC and head of the Interception Centre on the imposition of functions on members of the Interception Centre[3545] seems contradictory and ineffective in the conduct of an OCI. This is because direct and general instructions emanate from parallel government departments in many instances. However, it seems practicably difficult for members of the Interception Centre to faithfully or

[3540] Section 32(1)(a), (b) and (d) of RICA.
[3541] Section 32(2) of RICA.
[3542] Para 7.3.6.3 of this chapter. It is also noted that the Department of Telecommunication, which is primarily in charge of the technical supervisory aspect of the establishment of the infrastructure of interception devices, is not expressly mentioned in section 32(1) of RICA.
[3543] Section 32(2) of RICA.
[3544] Section 36(2) & (4)(a) & (b) of RICA.
[3545] Section 36(5) of RICA.

loyally obey a direct command from two superior authorities in this regard especially where there is no vacuum created in the office of the head of the Interception Centre in section 36(3) of RICA that would warrant the substitution of the other authority.

The fact that the performance of the function of the Interception Centre is subject to the 'control and directions' of the head of the Interception Centre in the power-sharing formula with the Director of the OIC[3546] does not remedy the erosion of the independence of the Interception Centre.

This is because it is unlikely that the imposition of the function of interception on Interception Centre by the head of Interception Centre would override the imposition of the function of interception on the Interception Centre by the Director of the OIC, who is superior to the former in their power-sharing formula. These provisions directly or indirectly take away the independence of the Interception Centre because the performance of the functions of the Interception Centre is still at the whims and caprices of the Director of OIC whose power is determined based on 'impository' and dictatorial principles.[3547]

In summary, it is therefore recommended that the powers stipulated in section 32(1)(b)-(d) of RICA should be vested in the head and management of the Interception Centre only to ensure its independence, competence and accountability. While the Minister of State Security should serve as the political and ceremonial authority overseeing the activity of Interception Centre, the Director of the OIC should —with legal responsibility or liability as earlier proposed for other political appointees—[3548] serve as the civil or public service supervisory authority only in section 35(1)(d),(f) and (g) of RICA. These roles must be performed without taking away the independence of the Interception Centre. This lays the foundation for the criticism on the deficiency in the allocation of powers, functions and duties of the Director of the OIC in section 35(1)(a)-(c) and (e) of RICA relating to the operations of the Interception Centre.[3549]

Thirdly, the Director of the OIC is given the power to regulate the practice and procedure of the Interception Centre in terms of the prescription of information to be kept[3550] relating to an

[3546] Section 36(5) & (6) of RICA.
[3547] Section 36(2), (4) & (5) of RICA.
[3548] Para 3.9.2 of Chapter 3 of this study.
[3549] Para 7.6.3 of this chapter.
[3550] Section 37(1) of RICA.

OCI application and direction, the outcome of the execution of an OCI direction and the prescription of the manner on how the record is kept and period of keeping the information.[3551]

Although no document on the practice and procedure in this regard has been specifically developed or published thus far by the office of the Director of Office for Interception Centre, however, representatives of one of the Respondents in *AmaBhugane* claimed in an affidavit that an internal procedure had been drafted by the SAPS, which was not produced in the hearing of the matter.[3552] The court in its decision in *AmaBhugane* quoted the United Nations High Commission for Human Rights by stating that 'secret rules and secret interpretations-or even secret judicial interpretations' cannot be regarded as law.[3553]

It is important to note that where the Director of the OIC has not developed a regulation on the practice and procedure for the Interception Centre in terms of the prescription of information to be kept,[3554] general reliance can be placed on Schedules A-C of RICA Directive 2005 published by the Minister of Communications which is acknowledged by the court in *AmaBhugane*.[3555] Although Schedules A-C of RICA Directive 2005 substantially covers the issues raised by the court, however, the Schedules are still inadequate in specific terms as highlighted by the court.[3556] However, it is recommended that the practice and procedure in Schedules A-C of RICA Directive 2005 should further be developed, overseen, ratified and approved by the National Assembly to address other issues raised by the court.[3557]

Fourthly, on the funding of the Interception Centre, it is submitted that placing and sharing the cost of interception service provision in the hands of and between public and private stakeholders and not solely in the government itself[3558] will cripple the independence of Interception Centre. This is because the latter will operationally exist at the mercy of these stakeholders who may claim financial instability and forestall the effective operation, independence and survival of the Interception Centre.

[3551] Section 35(1) (d), (f)&(g) and 37 (1) of RICA.
[3552] *AmaBhungane v Minister of Justice* supra 88 and 101. The court highlights the incapacity of SAPS in conducting an OCI, *AmaBhungane v Minister of Justice* supra 94.
[3553] *AmaBhungane v Minister of Justice* supra 89(2).
[3554] Section 37(1) of RICA.
[3555] *AmaBhungane v Minister of Justice* supra 87; RICA Directives 2005.
[3556] *AmaBhungane v Minister of Justice* supra 98.
[3557] *AmaBhungane v Minister of Justice* supra 98.
[3558] Sections 30(4), 31 (1) (a) (i) &(ii), (b)(i) &(ii) & (3) and 32(5) of RICA.

Instead, the routing of online communication by Online Communication Service Providers to the Interception Centre or the making available of online communication by the Online Communication Service Providers directly to LEAs[3559] should be regarded as a public utility like other essential services to the public. In addition, the funding of Interception Centre be sourced and appropriated from the direct National Assembly monetary allocation to maintain its independence as an institution that it is meant to be.[3560] This view is drawn on the phenomenon of a foreign jurisdiction which observes that the costs of online communication interception are expensive, which must be borne through other public sources.[3561]

7.3.6.5 Accountability and oversight by and of interception centres

Aside from the issues raised under different headings above concerning the Interception Centre, some of which constitute accountability and oversight measures by and of the Interception Centre, the following discussion further highlights other accountability and oversight measures by and of the Interception Centre that can be adopted in this study.

Firstly, RICA requires the head of Interception Centre to keep proper records relating to OCI application and direction and outcome of the execution of an OCI direction.[3562] In addition, the head of the Interception Centre must submit to the Director of OIC a routine quarterly or urgent report on records kept above, petitions of abuses relating to the execution of directions by LEAs or LEOs, which the head of Interception Centre is aware of[3563] and defects in online communication system or operation or any activity assigned by Online Communication Service Providers to the Interception Centre relating to the provisions of RICA.[3564]

Thereafter, the Director of the OIC simultaneously submits the reports to the Minister of State Security and the Chairperson of the JSCI in Parliament.[3565] It is important to note that the provision for submission of special reports relatively satisfies the implementation of the

[3559] Section 28(1) (b) (i) &(ii), (2) (a) (i) &(ii) & (b)(i)(ii) of RICA.
[3560] Nicolson G 'State capture: Madonsela needs funds to investigate as Jonas speaks out again' https://www.dailymaverick.co.za/article/2016-06-08-state-capture-madonsela-needs-funds-to-investigate-as-jonas-speaks-out-again/ (Date of use: 9 May 2018).
[3561] Landau *Lawful electronic surveillance in the face of new technologies* 231.
[3562] Sections 35(1)(f) and 37(1) of RICA.
[3563] Italics mine.
[3564] Section 37(2)(a) and (b) of RICA.
[3565] Section 37(3) of RICA; JSCI Report 2016 para 5 at 35.

principle of 'proportionality of urgency of reporting the seriousness of abuse' by the Interception Centre.[3566]

However, the provision that the head of the Interception Centre submits reports to the Director of the OIC on abuses relating to the execution of directions by LEAs or LEOs based on the condition that the head of the Interception Centre is aware or has knowledge of such abuses [3567] creates an unjustifiable defence for the head of Interception Centre in the submission of such reports. As such, the defence of awareness or knowledge largely and impliedly exonerates the head of the Interception Centre from the liability of reporting such abuses, which the head of the Interception Centre has a wide and unfettered discretion to feign knowledge or remain silent on the knowledge of the abuse no matter how serious the abuse may be.

The silence is encouraged by the absence of a statutory provision that requires the head of the Interception Centre to, along with the required routine and special reports, submit the online log report of the petitions submitted by a complainant to the head of the Interception Centre. Worse still, there is no statutory requirement that stipulates that such complaints by the public be submitted in online communication to guarantee proper online audit. Consequently, in all this, the oversight of the Interception Centre is compromised.

The head of the Interception Centre keeps records of abuses relating to the execution of directions[3568] for onward submission of reports relating to such abuses to the Director of the OIC, Minister of State Security and Chairperson of the JSCI of Parliament, thus enables adequate check and balance in this regard.

In summary, given that the IGI is constitutionally empowered to monitor the activities of LEAs[3569] and is statutorily regarded as the intelligence ombudsperson,[3570] it is submitted that

[3566] Although this form of proportionality is not examined in this study because there are several forms of proportionality principle that apply in this study, however, see generally Chapter 5 of this study where the proportionality principle, which is a major and an indispensable principle in this study, is examined.
[3567] Section 37(2)(a)(ii) of RICA.
[3568] Section 37(2)(a)(ii) of RICA.
[3569] Section 210(b) of the Constitution.
[3570] Serrao A and Mitchley A, N 'DA calls on Inspector General of Intelligence to probe alleged 'Project Wonder' plot' https://www.news24.com/SouthAfrica/News/da-calls-on-inspector-general-of-intelligence-to-probe-alleged-project-wonder-plot-20170827 (Date of use: 26 July 2018).

such powers should include the mandate to embark on an ADR,[3571] or better still, as practicably propounded in this study, ADM[3572] mechanisms.

Applying an ADM mechanism will be part of the oversight responsibilities by the Inspector-General of Intelligence in addressing the issues on the abuses relating to the execution and post-execution of the conduct of an OCI by the Interception Centre. The ADM mechanism includes the hierarchical manpower or implementation of mediation, conciliation and arbitration before considering other legal options, which may include civil, and criminal claims.

7.4 PROGRESS REPORT ON AND REVIEW OF THE EXECUTION AND POST-EXECUTION OF ONLINE CRIMINAL INVESTIGATION

RICA provides that a designated judge may, at any time and at such intervals determined by the designated judge, require a LEO who made the application to the former, submit a report in writing on the progress made by a LEO in achieving the objectives of the OCI direction or any matter that the judge may deem necessary in conducting an OCI.[3573]

However, the fact that section 24 of RICA uses the word 'may', the judge is not, at the point of issuance of an OCI direction or at any other time during the conduct of an OCI, compelled to request a LEO to submit a report on the effectiveness of the conduct of OCI,[3574] which, in a way, undermines the supervisory and oversight function of the judge and the principle of checks and balances. However, where the court applies its discretion, it is binding on the LEO.

In two instances of interception without a direction, a LEO who makes an oral emergency request to an Online Communication Service Provider is required to, as soon as practicably possible thereafter the interception, submit a written confirmation of the request to the Online Communication Service Providers containing the facts adduced by the LEO for the conduct of an intercept.[3575] Thereafter a LEO submits to the designated judge a copy of the written confirmation and an affidavit setting out the information, result and recording of the

[3571] Para 7.7 of this chapter.
[3572] Para 7.7 of this chapter.
[3573] Section 24(a) of RICA.
[3574] It is submitted that the word 'may' is not mandatory in this circumstance, see section 24 of RICA.
[3575] Sections 7(3) and (4) (a) -(c) and 8(4)(a)-(c) of RICA.

interception.[3576] In the U.S., the courts expect a LEO to submit 'regular progress updates',[3577] which are both specific and aggregate.[3578] The specific content contains the personal details of targets and is not expected to be publicly disclosed.[3579]

In a way, the requirement of submission of a periodic report to the judge in RSA reiterates the implementation of one aspect of the principle of proportionality which bothers on the urgency of reporting the seriousness of abuse[3580] in the conduct of an OCI and emphasises the supervisory or oversight function of the conduct of an OCI by the judge.[3581]

At the United Nations level, the provision that a report on the conduct of an OCI is submitted by the head of LEA to the A-G not later than six months of the conclusion of the conduct of an OCI and to the Parliament on an annual basis[3582] is disproportionate. A maximum period of six months is stipulated. However, it is arguably disproportionate to both the effect of the seriousness of the commission of an offence and the high levels of risks and urgency involved in the intrusion or protection of the right to the SOC that should be considered accordingly. Arguably, this is because LEAs usually misinterpret a maximum period as the minimum period, therefore, LEAs wait till the end of the sixth month before a report is filed, which demonstrates the disproportionality in this instance.

As part of the progress report process, RICA makes provision for the application of a review of an OCI direction, which must be in writing.[3583] A review could be in form of cancellation,[3584] an extension of time and amendment of an existing OCI direction as follows.[3585]

Firstly , RICA provides that a designated judge may cancel the execution of the OCI direction where a LEO has, in terms of section 24 of RICA, failed to submit a report or failed to achieve the objectives of the OCI direction.[3586] Also, RICA provides that a designated judge must

[3576] Sections 7(3) and (4) (a) -(c) and 8(4)(a)-(c) of RICA.
[3577] Caproni *Lawful electronic surveillance* 209.
[3578] Crump *Geolocational Privacy and Surveillance Act* 287.
[3579] Crump *Geolocational Privacy and Surveillance Act* 287.
[3580] Chapter 5 of this study, more particularly para 5.4 for the other forms of proportionality principle.
[3581] See para 7.3.6.4 of this chapter; See s 37(1), (2)(a) and (3) of RICA.
[3582] Art 16 (14) of the UNODC 'Model legislative provisions against organised crime 2012.
[3583] Section 20 (1) & (2) of RICA.
[3584] Section 25 of RICA
[3585] Section 20 of RICA.
[3586] Section 25 (1) (a) & (b)(i) of RICA.

cancel the execution of an oral direction[3587] where a LEO fails to submit a written application after 48 hours of the issuance of an oral direction emanating from an oral application,[3588] given that an OCI application and direction are generally issued in writing.[3589] In any form of cancellation above, the judge must, in writing, inform the LEO of the decision to cancel,[3590] but does not require the judge to furnish a reason for the cancellation.

Secondly, RICA provides for the extension of the period or amendment of the execution of an existing OCI direction[3591] which complies with the general proportionality principle[3592] between the seriousness of an offence and the risks levels in the duration of intrusion of the right to the SOC in the conduct of an OCI.

The application for extension or amendment, which must be in writing, must indicate the proposed extension of time or amendment that is required.[3593] The application must specify the reasons and circumstances to justify the extension or amendment.[3594] The application must contain an affidavit stating the outcome of the existing OCI direction and 'reasonable explanation of the failure' of a LEO in obtaining the desired results.[3595]

The application for the amendment or extension of directions under section 58 of RICA must comply with the additionally required conditions or directives.[3596] An amendment may be raised in respect of any issue in the conduct of an OCI. In the U.S., a LEA is expected to prove afresh the relevant reasonable ground standards before the direction is renewed,[3597] the principle of which it is submitted should also apply in the RSA in this regard.

[3587] Section 23 (3) of RICA.
[3588] Sections 23(4) (b), (7) and (8) (b) and 25 (2) (a) & (b) of RICA.
[3589] Sections 16(2), 17(2), 19(2) & (5), 20 (2), 21(2) and 23(5) of RICA.
[3590] Section 25(3) of RICA.
[3591] Section 20(1), (2)(b)(ii), (3)(b), (4), (5) and (6) of RICA.
[3592] Paras 5.3.4 - 5.3.6 and 5.4 of Chapter 5 of this study.
[3593] Section 20(2) (b)(i)-(ii) of RICA.
[3594] Section 20(2)(a) of RICA
[3595] Section 20(2)(c) of RICA. It is important to note that there is no contradiction in the submissions between ss 20(2)(c) and section 24 of RICA because the submission made earlier in section 24 under this rubric deals with the exercise of the discretion of the judge relating to the non-compellability of the judge to request for a report from a LEA or LEO on the effectiveness of the conduct of an OCI while section 20(2)(c) takes away the exercise of the discretion of the judge on the request for the reasonable explanation for the amendment or extension of the existing direction. Further, while section 24 deals with progress report, section 20(2)(c) deals with amendment or extension of an OCI direction, which are two different scenarios.
[3596] Section 20(2)(d) of RICA.
[3597] Caproni *Lawful electronic surveillance* 209.

The extension or amendment is granted with necessary changes upon the satisfaction of the judge that it is necessary to achieve the objectives of the directions, which must not be more than 'three months at a time', in the case of an extension.[3598] However, drawing on the fact that 1-month offline entry and search warrant is required to conduct an investigation in the COPA[3599] buttresses the point that 3-month maximum review period for the conduct of an OCI is disproportionate[3600] between the seriousness of an offence and the risks levels in the duration of intrusion of the right to the SOC in the conduct of an OCI. Furthermore, aside from the *two-minute* duration of the conduct of an OCI in the U.S.,[3601] a *three-day* period has been established to be sufficient to conduct an illegal OCI by LEOs in the Parliamentary JSCI 2016 report in the RSA.[3602]

It is therefore recommended that RICA should borrow a leaf from the United Nations principle that provides for the 'reasonableness and proportionality in all circumstances' in the conduct of an OCI, including the renewal of OCI direction.[3603]

7.5 MANAGEMENT OF DATA IN ONLINE CRIMINAL INVESTIGATION

7.5.1 Introduction

Further to the examination of the role of stakeholders in the protection of the integrity and security of online communication and interception devices and the examination of the imposition of sanctions thereof[3604] which directly or indirectly highlight the various forms and versions of management of data in the conduct of an OCI, there are concerns expressed in some quarters. The concerns include the arguably and partially erroneous decision of the High Court

[3598] Section 20(4) & (6) of RICA.
[3599] Section 103(3)(d) of the COPA. It is noted that relying on this provision does not diminish the arguments canvassed earlier in favour of the right to the SOC as opposed to non-online privacy communication, see para 3.4.4.12 of this study titled '*Determinable period of investigation in online criminal investigation*'.
[3600] Paras 3.5.7.8, 6.5.2 and 7.4.4 of this study on the proportionality of interception duration principle.
[3601] Paras 3.5.7.8 and 6.5.2 of this study.
[3602] JSCI Report 2016 para 8 at 39.
[3603] Art 16 (7) & (8) (a) &(b) of the UNODC 'Model Legislative Provisions Against Organised Crime' 2012 at 82.
[3604] See more particularly paras 3.5.6, 3.5.7, 3.9, 3.10, 4.4, 5.2, 6.3.4, 6.4- 6.7, 6.9 - 6.13, 7.3 and 7.4 of this study.

in *AmaBhugane* on the deficiencies of the various forms of management of data[3605] by the relevant executing entities and the role players at the four stages of the conduct of an OCI.[3606]

These concerns include the inadequacies in the regulation of almost every task involved or step taken in the techno-legal integrity, safety and security of the pre and post-management of the conduct of an OCI relating to: an online[3607] and offline gathering of fact (pre-execution); duplicating, routing[3608] and provisioning (execution); storage, sorting, copying or further duplicating and retrieving (technical post-execution); examining (investigative post-execution) and deletion (conclusive post-execution) of data.[3609]

These tasks or steps are performed by different role players in specific[3610] direct, and indirect capacities in the execution and post-execution of the conduct of an OCI in RICA regime.[3611] For example, a Telecommunication Service Provider or better still, an Online Communication Service Provider primarily, technically and legally has the obligation to make provision for direct interception of online communication to LEAs —which is opposed in this study,[3612] duplicate and route online communication to the Interception Centre, store and delete online communication. An Interception Centre is secondarily, technically and legally obliged to store, retrieve and delete an online communication in the execution and post-execution of the conduct of an OCI.[3613]

[3605] *AmaBhungane v Minister of Justice* supra 89, 98, 99 and 108. 'RICA is silent about what procedures officials should follow when examining, copying, sharing, and storing the intercepted data. When intercepted data is not relevant to an investigation, there is no prescribed procedure for it to be destroyed', Right2Know at 8 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[3606] Paras 5.2.2.2 - 5.2.2.5 of Chapter 5 of this study. For example, the JSCI recommends that an electronic filing system for the conduct of an OCI should be created which will be stored for at least five years in compliance with the provisions of the Archival Act No 43 of 1996, which contradicts the position being held in this study, see para 7.3.5 of this study and JSCI Reports 2016 at 56.

[3607] Aside from the information published in the public domain, preliminary information needed to trigger the conduct of an OCI can also be obtained in an online communication without breaching the right to the SOC, Popoola *Liability of ISPs* ii.

[3608] In routing an online communication to the IC, an Online Communication Service Providers is required to duplicate the online communication, should there be any form of buffering in the protocol, which is duplication and a form of storage or recording, paras 1, 4.1(a), 4.6, 8.2(a), 8.4, 10.1, 10.2, 10.4, 10.5, 10.7(a), 10.8 of Schedule A of RICA.

[3609] *AmaBhungane v Minister of Justice* supra 98, 105 and 108.

[3610] It is noted management of data might have been dealt with in other segments of this study, this rubric herein deals with the specific areas of the pre-execution and post-execution of an OCI.

[3611] Chapter 2 (more particularly para 2.11), chapters 4 and 5, Chapter 6 (more particularly paras 6.3 - 6.13) of this study.

[3612] Para 7.3.5 of this chapter.

[3613] Para 7.3.5 of this chapter.

Another illustration of the diverse functions of role players is that Authentication Service Providers, Cryptography Providers, Cyber Inspectors and Decryption Keyholders have respective primary and secondary techno-legal duties in the execution and post-execution of an OCI direction.[3614] Respecting a LEA[3615] and the court; although they perform a primary legal function, however, they play secondary and tertiary technical roles in the execution and post-execution of the conduct of an OCI.[3616]

7.5.2 Management of data at the pre-execution of online criminal investigation

7.5.2.1 Introduction

The management of data at the pre-execution of an OCI involves the online[3617] and offline activities of gathering facts before a techno-legal execution of an interception or OCI occurs where:

a) an OCI direction is not required to be issued under special circumstances in RICA in cases of emergency, correctional facility environment[3618] and other related circumstances, though an OCI is ultimately executed in the relevant circumstances;

b) an OCI direction is required to be issued by a court in general OCI circumstances;[3619]

c) a ROCI sends a signal to the Online Communication Service Provider and finally to an Interception Centre to conduct an OCI without the requirement of a direction from the court.[3620]

The management of data at the pre-execution of an OCI in the regime under RICA occurs in paragraphs (a) and (b) above, while RICA does not cater for paragraph (c), which is propounded in this study.[3621]

[3614] Paras 7.3.2.2, 7.3.2.3 and 7.3.3 of this chapter.
[3615] Para 2.11 of Chapter 2 of this study.
[3616] Chapter 2 (more particularly para 2.11), chapters 4 and 5, Chapter 6 (more particularly paras 6.3 - 6.13) of this study.
[3617] Popoola *Liability of ISPs* ii.
[3618] Regulation 8(4) (a) (i) &(ii) & (b) and (5) of Correctional Services Act (111/1998) (Correctional Services Regulation); Chapter 2 Part 1 of RICA; Paras 6.2.4 and 6.2.5 of Chapter 6 of this study.
[3619] Para 6.2.7 of Chapter 6 of this study.
[3620] Paras 2.11.4 of Chapter 2 of this study.
[3621] Para 2.11.4 of Chapter 2 of this study.

Aside from the examination of the role and management of the affairs and activities of an Online Communication Service Provider in conducting an OCI,[3622] this rubric highlights the general role of Online Communication Service Providers. The stakeholders in an Online Communication Service Provider comprise, amongst others, Fixed Line Operators, Mobile Cellular Operators and Internet Service Providers which provide same or similar core or primary technical dependent or interdependent online communication services in the pre-OCI conduct.

It is noted that in some illustrations, a specific Online Communication Service Provider may be mentioned —such as Fixed Line Operators, Mobile Cellular Operators and Internet Service Providers— to address some distinctive techno-legal functions. In the RICA regime, non-Online Communication Service Providers —such as clerical or administrative officers attached to the court—[3623] and LEAs are also involved in the pre-execution of an OCI. These stakeholders play independent and interdependent roles in the management of data in the pre-execution of an OCI.

7.5.2.2 General management of data at the pre-execution of online criminal investigation

In pursuance of the various responsibilities carried out by stakeholders, roles players manage data at the pre-execution of an OCI in the following ways, amongst others.

Firstly, generally, anyone who conducts or attempts to conduct an OCI has the responsibility to manage and account for the data gathered in the offline, and online regimes.[3624]

Secondly, since a LEO makes a request to an Online Communication Service Provider to intercept, the written records of which are kept by the former, the duo is responsible for management and accountability of data in these regards[3625] including the designated judge who receives a written confirmation submitted by a LEO.[3626]

[3622] Paras 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11.4, 3.5.7, 3.8, 3.9.2.6(a), 3.9.4, 6.11 and 7.3.5 of this chapter.
[3623] JSCI Report 2016 at 20, 21, 54, 55 and more particularly at 56; Parliament 'Annual Report of the Joint Standing Committee on Intelligence for the Financial Year ending 31 March 2017' 4 and 10 (JSCI Report 2017).
[3624] Section 2of RICA.
[3625] Sections 7(1)-(3) and 8(1), (3) and (4)(a) of RICA.
[3626] Section 8(4)(b) of RICA.

Thirdly, LEAs, LEOs and the designated judge, High Court judge, regional magistrate and magistrate respectively manage and account for the data submitted for real-time and an archived OCI application or combination applications and data stated in an OCI direction or its supplements.[3627]

Fourthly, LEAs, LEOs and the designated judge manage and account for the data submitted in the amendment, extension or cancellation of an existing OCI direction.[3628]
The fifth responsibility is that LEAs, LEOs, decryption key holder and designated judge manage and account for the data involved in the application and issuance of a decryption direction.[3629]

The sixth role is that LEAs, LEOs and designated judge manage and account for the data involved in the oral application and issuance of a direction for the conduct of an OCI.[3630]

The seventh responsibility is that LEOs, LEOs and Online Communication Service Providers respectively manage and account for the data relating to the recording of user personal details required for the activation of a mobile online communication device by a user.[3631]

Finally, a user, LEA and LEO manage and account for the data relating to the report of loss, theft or destruction of a mobile cellular phone or SIM card.[3632]

[3627] Sections 16(2) (a) (i) -(iii),(b) - (h) and (5) - (8), 17(2)(a)-(g), (4) &(5), 18(2)(b)(i) and 19(2)(a),(3), (4), (5)(a)-(d) and (7) of RICA.
[3628] Sections 16(10) and 20(2) (a) &(c) and (5) of RICA.
[3629] Sections 21(2) (a) (i)-(iii), (b)-(e), (f)(ii) and (3)- (5) of RICA.
[3630] Section 23 (1),(2)(a)-(c), (3),(4)(a)&(b), (5)-(12) of RICA; Luck R 'RICA' at 2 http://www.saflii.org/za/journals/DEREBUS/2014/6.html (Date of use: 27 June 2019).
Art 27(3) and Forward page of TOCC at iii.
[3631] Sections 39 (1)-(4), 40 and 62C of RICA.
[3632] Sections 41, 52, 53 and 55 of RICA.

7.5.3 Management of data during the execution of online criminal investigation

After the pre-execution stage, the execution of an OCI begins, which comprises the duplicating,[3633] routing, and provisioning[3634] of real-time and archived online communication in the conduct of an OCI, the management of some of which tasks are highlighted below.
Firstly, generally, a LEA, LEO, court, authorised person, Online Communication Service Provider and Interception Centre respectively manage and account for the real-time and archived data during the execution of an OCI direction.[3635]

Secondly, a LEA, LEO, Decryption Keyholder, Online Communication Service Provider and Interception Centre respectively manage data during the assistance in the decryption of an encrypted key in online communication.[3636]

Thirdly, an Online Communication Service Provider and their employees manage and account for the data during the interception or conduct of an OCI or an attempt thereof in the recording services provided by an Online Communication Service Provider.[3637] This is in pursuance of the compliance by an Online Communication Service Provider with the directive by the minister on both the service installation on the manner on how data is intercepted and stored and on the determination of security, technical and functional requirements of the facilities for interception and recording capabilities issued by the relevant ministers.[3638]

Fourthly, given that the Minister of State Security administers the Interception Centre, it is arguable that the Minister directly or indirectly manages and accounts for the data during the conduct of an OCI at the Interception Centre,[3639] otherwise, the verb 'administer' should be amended to read either 'oversee' or 'supervise' to exonerate the Minister who is not required to have any form of techno-legal professional proficiency in the conduct of an OCI.

[3633] According to the definition of 'archived communication-related information', duplicating can interchangeably be used to mean recording or storage. However, despite the fact that duplicating occurs during the execution of an OCI, recording or storage can occur at the post-execution stage too as expressed in para 7.5.4 of this chapter.
[3634] Para 7.3.5 of this chapter. See generally Schedules A-C of RICA Directives 2005.
[3635] Sections 26(1)-(3) and 28(1) (b) (i) &(ii), (2) (a) &(b) of RICA.
[3636] Section 29(1) (a) &(b), (2)-(8)(a) of RICA.
[3637] Section 30(1)(a) & (b), (2)(a) & (b)(a) & (b), 7(a) & (b) and (8) and 50 (1) and (2) of RICA.
[3638] Section 30(1)(a) & (b), (2)(a) & (b)(a) & (b), 7(a) & (b) and (8) and 50 (1) and (2) of RICA.
[3639] Section 32(1)(d) of RICA.

Fifthly, although the court in *AmaBhugane* held that the Director of the OIC is responsible for the 'storage and management' of data in the conduct of an OCI,[3640] nevertheless, it is submitted that this decision is erroneous. This is because the Director of the OIC only administers, controls and manages the affairs and activities of the Interception Centre only.[3641] The Director of the OIC who is not required to have any form of techno-legal professional capacity or proficiency in the conduct of an OCI does not engage in the business of storage of data.[3642]

In addition, what the Director of the OIC does is to issue prescription which relates to the type of data to be kept, the manner in and period for which such data is kept by the head of the Interception Centre on the application, directions and outcomes of an OCI.[3643]

Finally, although there are some deficiencies in the provision for duplicating, routing, and provisioning of data during the conduct of an OCI under RICA and its Directives, the non-consideration of or non-referral to RICA Directives 2005 in the judgement of the court in *AmaBhugane*[3644] is a grievous error of judgement in which the court denies itself the opportunity of administrating proper justice to some of the issues raised in this study.

7.5.4 Management of data at the post-execution of online criminal investigation

Contrary to the partially erroneous decision of the High Court in *AmaBhugane*,[3645] RICA and its Directive make some provisions in the management of data at the post-execution of an OCI.

The management of data at the post-execution of an OCI includes the management of storage and buffering[3646] (though RICA does not provide for the secret sealing of the post-OCI application as the Canadian authorities do),[3647] sorting, copying or duplicating and extracting

[3640] *AmaBhungane v Minister of Justice* supra 85.
[3641] Section 35(1)(c) of RICA.
[3642] Section 35(1) of RICA
[3643]Section 35(1)(a) - (g) of RICA.
[3644] *AmaBhungane v Minister of Justice* supra 98 and 108.
[3645] *AmaBhungane v Minister of Justice* supra 98 and 108.
[3646] Storage includes buffering, para 7.3.5 of this chapter. *AmaBhungane v Minister of Justice* supra 98(1) and (3) -(6).
[3647] Section 187(1) of the Canadian Criminal Code, *R v Blizzard* (2005), 65 W.C.B. (2d) 579, 2005 NBQB 224, at para 3, Hubbard, Brauti and Fenton *Wiretapping* at 3.20.4h.

or retrieving of data facilities provided by an Online Communication Service Provider.[3648] It is noted some of these tasks occur simultaneously, depending on the task to be performed per time (for example, copying and retrieving occur spontaneously), thus it makes it difficult to determine which task occurs earlier. The following, amongst others, highlights the management of data at the post-execution of an OCI.

In the management of data at the post-execution of an OCI, an Online Communication Service Provider is required to take reasonable steps in ensuring the physical, environmental and logical integrity and security of recorded or stored data.[3649] An Online Communication Service Provider[3650] stores and manages the records of real-time calls made in the conduct of an OCI[3651] and transfers the data in its record by taking steps to ensure the integrity and protection of the real-time data from being compromised in a recorded and an archived storage facility.[3652] Where there is a transfer of real-time communication to an archived communication storage system, all the data must be transferred without compromising the integrity and protection of the communication.[3653]

Under the management of data at the post-execution of an OCI, the information relating to the manner of implementation of storage measures of data by an Online Communication Service Provider must not be revealed to an unauthorised person who may not need to access the document as held by the court in *AmaBhugane*.[3654] This raises the question whether a superior officer who delegates or donates the power of attorney to a LEO to conduct an OCI in RICA[3655] still has the power to access an OCI application or direction as examined below under the broad principle of duty of or due care.

This is because there is an agreement of confidentiality of the installation and implementation of storage measures of real-time and archived communication between an Online

[3648] Paras 10.1, 10.4, 13.1, 13.3 and 13.4 (a) of Schedule A of RICA Directive 2005; *AmaBhungane v Minister of Justice* supra 98 (2) - (8).
[3649] Paras 11.7, 15.6 & 15.7 of Schedule A of RICA Directive 2005.
[3650] Aside from the provision of Schedule A of RICA Directive 2005 to regulate a FLO, schedules B and C of RICA also regulate the various technical- techno-legal issues in this study.
[3651] Para 10.1 of Schedule A of RICA Directive 2005; *AmaBhungane v Minister of Justice* supra 98(1) & (3).
[3652] Para 10.9 (a) & (c) and 11.6 of Schedule A of RICA Directive 2005.
[3653] Para 13.6(a) & (c) of Schedule A of RICA Directive 2005.
[3654] Paras 11.1, 15.1 & 15.2 of Schedule A of RICA Directive 2005; *AmaBhungane v Minister of Justice* supra 98(2) and (3) - (6) and 105.
[3655] Section 1 of RICA where the word 'applicant' is defined; Para 7.2 of this chapter.

Communication Service Provider and manufacturers of the technical installation of storage measures,[3656] the agreement of which should clarify the residual power of the donor to make a final endorsement or otherwise of the outcome of the conduct of an OCI by a delegate. This agreement or arrangement must be exercised with due care in installing a telecommunication operation[3657] which includes or excludes a donor of the power of attorney in the delegation.

In the management of data at the post-execution of an OCI, the duty of or due care principle must have regard to the following provisions, amongst others: the necessity of protecting data;[3658] the number of targets who are or were subject of real-time OCI direction and the applicable periods of conducting an OCI;[3659] the need to restrict the minimum number of employees of an Online Communication Service Provider who implement and operate the storing measures in real-time communication[3660] and the need for an Online Communication Service Provider to take reasonable steps to ensure that records are secure and accessible to specific nominated staff only.[3661] However, RICA does not stipulate that the requirements for managing such members must be in accordance with the same or similar requirements like the proposed requirements for the management of the affairs and activities of LEAs.[3662]

In the management of data at the post-execution of an OCI, RICA and it's Directive make provision for ensuring the management of clear delimitation of functions for authorised staff members; the protection of the right to privacy of the third party in the storage process, which is accessible by authorised staff members only;[3663] the prohibition of access to or misuse of handover interface to unauthorised persons;[3664] the full recording from the beginning to the end of the activation or application of the technical function of telecommunication installation of storing a 'given identity' and the full recording of the 'authenticator ' that is used in identifying the operating staff.[3665]

[3656] Paras 11.3 and 15.3 of Schedule A of RICA Directive 2005.
[3657] Para 11.4 of Schedule A of RICA Directive 2005.
[3658] *AmaBhungane v Minister of Justice* supra 98.
[3659] Para 11.4(a) of Schedule A of RICA Directive 2005.
[3660] Para 11.4(b) of Schedule A of RICA Directive 2005; *AmaBhungane v Minister of Justice* supra 98(2) -(6).
[3661] Paras 11.5 and 15.5 of Schedule A of RICA. See comment on para 11.4(b) of Schedule A of RICA Directive 2005; *AmaBhungane v Minister of Justice* supra 98(2)-(6).
[3662] Paras 4.4 - 4.6 of Chapter 4 of this study.
[3663] Para 11.4(c) of Schedule A of RICA Directive 2005; *AmaBhungane v Minister of Justice* supra 98(2) -(6).
[3664] Para 11.4(e) & (f) of Schedule A of RICA Directive 2005; *AmaBhungane v Minister of Justice* supra 98(2)-(6).
[3665] Paras 11.4 (l) (i) - (v) and 15.4(l)(ii) of Schedule A of RICA Directive 2005; *AmaBhungane v Minister of Justice* supra 98(2)-(6).

Although any measure aimed at solving a problem can be improved upon in primary and subsidiary laws such as RICA and its Directives, however, it is noted that the court in *AmaBhugane* did not explicitly address some of these reasonable provisions in RICA Directive 2005,[3666] hence the fallacy in the decision of the court in this regard.

While the head of the Interception Centre keeps, manages and accounts for the data as may be directed by the Director of the OIC, the JSCI of Parliament and the Minister of State Security supervise the management of data kept by the Interception Centre.[3667]

In the management of data at the post-execution of an OCI, an Online Communication Service Provider informs the Interception Centre of any change in the storage system, the configuration of storage of data and the temporary unavailability of stored data.[3668] The configuration of the storage system must be executed with no or minimal involvement of third parties.[3669] It is however noted that the online communication in the RSA has generally not compartmentalised and passworded the compartmentalised online communication.[3670]

Where an Online Communication Service Provider makes use of and cooperates with a Telecommunication Service Provider in providing storage service (which is one of the steps in the post-management of data in the conduct of an OCI), an OCI direction must be served on each party in the execution process.[3671] Where two or more OCI directions for real-time communications are issued and processed, an Online Communication Service Provider 'shall take reasonable precautions' to protect the identities of the LEAs and 'ensure the confidentiality of the investigations and information' is not compromised.[3672]

In the management of data in the post-execution of an OCI; a LEA, LEO, Online Communication Service Provider and designated judge respectively manage and account for the written confirmation, affidavit of the results and outcome obtained in the interception and recordings, transcripts or note made by a LEO.[3673]

[3666] *AmaBhungane v Minister of Justice* supra 98 and 108.
[3667] Section 37(1), (2) & (3) of RICA.
[3668] Paras 12.6 (a) & (b) and 16.6(a) & (b) of Schedule A of RICA Directive 2005.
[3669] Paras 12.7 and 16.7 of Schedule A of RICA Directive 2005.
[3670] Para 2.3.1 of Chapter 2 of this study.
[3671] Paras 12.8 and 16.8 of Schedule A of RICA Directive 2005.
[3672] Paras 12.13 and 16.13 of Schedule A of RICA Directive 2005.
[3673] Sections 7(3) & (4) and 8(5) (a) &(b) of RICA.

An Online Communication Service Provider and a designated judge manage and account for the data in the affidavit submitted to the designated judge on the steps taken and the result of the steps by the Online Communication Service Provider in giving effect to the request made by a LEA or LEO.[3674]

Information stored shall be 'clearly indexed' in such a way that during retrieval, data is made available without unreasonable effort or delay.[3675]

An Online Communication Service Provider 'shall employ reasonable measures to ensure the availability' or retrieval of archived online communication.[3676]

Where an Online Communication Service Provider or storage provider is involved in the storage of real-time communication, an Online Communication Service Provider shall not give more information than is strictly necessary for the operational activities of the storage.[3677]

Finally, although there are some deficiencies in the provisions for storage and buffering, sorting, copying or duplicating and extraction or retrieving of data at the post-execution of an OCI under RICA and its Directives; the non-consideration of or non-referral to RICA Directives 2005 in the judgement of the court in *AmaBhugane*[3678] in this regard is a grievous error of judgement which prevents the court from expounding the jurisprudence on the conduct of an OCI in this study. However, this study corroborates the decision of the court in *AmaBhugane* on the gross inadequacy of the law in the areas of sealing, sorting and extraction or retrieving of data in the post-conduct of an OCI in the RSA.[3679]

[3674] Sections 7(5) and 8(4)(c) of RICA.
[3675] Paras 12.11, 13.1, 13.5, 16.7 and 16.11 of Schedule A and para 13.3 of Schedule B of RICA Directive 2005.
[3676] Para 15.8 of Schedule A of RICA Directive 2005.
[3677] Paras 12.9 (a) & (b) and 16.9 (a) & (b) of Schedule A of RICA Directive 2005.
[3678] *AmaBhungane v Minister of Justice* supra 98 and 108.
[3679] Schedules A -C of RICA Directive 2005; *AmaBhungane v Minister of Justice* supra 98 and 108.

7.5.5 Management of examination of data at the post-execution of online criminal investigation

The definition of the term 'intercept' includes the 'viewing, examination, or inspection of the contents of any indirect communication,[3680] while 'monitoring' includes 'listening to', all of which is carried out by different types of investigators in the conduct of an OCI.[3681]
To examine the data gathered in the post-execution of an OCI, the data must be stored in a format that is readable, intelligible and understandable.[3682]

Some provisions are made for the monitoring of access to the data gathered in the conduct of an OCI, which include the monitoring of the movement of a user when logging in and out of the Interception Centre devices by LEOs.[3683]

Nevertheless, RICA and its Directive do not make provision for the proper procedure for the examination of data that is gathered in the conduct of an OCI[3684] in terms of other issues mentioned or not mentioned in this study. One of such issues is, whether copying or duplicating of data for examination purposes include allowing a LEO have a hard copy transcript examined or the data can only be examined in a soft copy that is uncopiable in other non-official electronic devices (such as a mobile cellular telephone) to control access to the data?

Another issue is, whether every online device that is used in examining data should have an installed camera to monitor the use of the data by a LEO who may —for example— use a personal device to snap a screen-shot of data? In addition, as a corollary to the immediate foregoing enquiry, whether an examination of data can be carried out outside the Interception Centre environment to ensure unauthorised persons do not have access to online communication, given that online data is virtual?

Furthermore, another issue is what is the extent of the use of predictive software application to examine data or better still, what is the role of robotics and machine learning in examining data

[3680] See 'intercept' in section 1 of RICA.
[3681] Para 2.11 of Chapter 2 of this study.
[3682] Paras 10.8 and 13.5 of Schedule A of RICA Directive 2005.
[3683] Para 11.4 (l) (i) - (v) of Schedule A of RICA Directive 2005; Para 7.5.4 of this chapter.
[3684] *AmaBhungane v Minister of Justice* supra 98(8), 99 and 108.

or relevant data? Furthermore, how are third-parties and privileged communications protected in data examination?, amongst other measures.

Finally, it is submitted that although RICA defines the concept of examination of data gathered,[3685] however, the High Court rightly held in *AmaBhugane* that RICA fails to provide for the proper procedure for the examination of data.[3686]

7.5.6 Management of deletion of data in the post-execution of online criminal investigation

It is submitted that the deletion of data occurs where there is no legal basis for the authorities to further store, keep, duplicate, copy, buffer or do anything contrary to the right of a user of an online communication after gathering such data, otherwise, data is not deleted after the conduct of an OCI where the storage of data meets all the requirements for further storage or usage. Such requirements include whether the data gathered is relevant to the purpose of the conduct of an OCI[3687] *vis a vis* whether the data gathered does not constitute windfall evidence.[3688]

It is important to note that although RICA and its RICA Directive 2005 make provision for the deletion of data,[3689] however, it is inadequate in some respect, including but not limited to the deletion of irrelevant or surplus data that is gathered in the conduct of an OCI.[3690] In the deletion of an online data, it is required that the deletion tools are secure enough to ensure that data deleted is actually deleted and not retained elsewhere[3691] nor can be retrieved via the use of a software application.

The management of deletion of data in the post-execution of an OCI is as follows, amongst others.

[3685] See 'intercept' in section 1 of RICA.
[3686] *AmaBhungane v Minister of Justice* supra 98(8), 99 and 108.
[3687] Section 47(1) and (2) of RICA; *AmaBhungane v Minister of Justice* supra 105.
[3688] Para 7.8 of this chapter; *AmaBhungane v Minister of Justice* supra105.
[3689] Section 30(2)(a)(iii) and (8) of RICA; Para 10.5, 10.9 (b) and 13.6 (b) of Schedule A of RICA Directive 2005; *AmaBhungane v Minister of Justice* supra 105; Paras 7.3.4 and 7.5.6 of this chapter.
[3690] *AmaBhungane v Minister of Justice* supra 105.
[3691] Blumberg and Eckersley *Locational privacy* 324.

Technically, an Online Communication Service Provider must ensure that the online data available in its records[3692] is not deleted before the expiry of 90 days[3693] while the period that an Online Communication Service Provider stores a real-time online data is for at least 90 days,[3694] both of which do not have any determinable period. However, the United Nations regime requires that the destruction of online evidence gathered should take place as soon as practicable but not later than six months of expiry of the OCI direction,[3695] which confirms a terminal date for the deletion of data that is not relevant for the purpose for which it was gathered.

Administratively, RICA provides that all archived communication directions issued by a High Court, regional court and magistrates and copies of OCI applications must be physically kept by a designated judge for at least five years.[3696]

However, the provision for the storage of data before deletion takes place under RICA is inadequate in the following ways.

Firstly, there is no framework on the guideline on how the designated judge keeps the OCI application records entrusted in the custody of the designated judge,[3697] which corroborates part of the judgement of the court in *AmaBhungane* in this regard,[3698] thus creates an uncertainty in the protection of the right to offline and online communications. The lack of framework may be premised on the fact that the OCI application is made in an offline system[3699] and as such kept in the same manner as other offline documents are kept which may not be safe or secure.

This is unlike the guideline prescribed for the storage of online communication in an OCI,[3700] which though not adequate as examined below.[3701]

[3692] Paras 10.3 of Schedule A of RICA Directive 2005.
[3693] Para 10.5, 10.9 (b) and 13.6 (b) of Schedule A of RICA Directive 2005.
[3694] Paras 10.5, 10.9(b) of Schedule A of RICA Directive 2005.
[3695] Art 16 (13) of the UNODC 'Model legislative provisions against organised crime' 2012.
[3696] Section 19(8) of RICA.
[3697] Section 19(8) of RICA; JSCI Reports 2016 at 40.
[3698] *AmaBhungane v Minister of Justice* supra 98 and 108.
[3699] See para 5.10 of this study titled 'Techno-legal quadruple application', where offline OCI application is condemned.
[3700] See section 30(2)(a)(i)-(iii) of RICA.
[3701] See para 6.4.3 of this study titled 'Management of data in *post*-online criminal investigation'.

Aside from keeping all copies of OCI applications for at least five years by the designated judge,[3702] online data is kept by Online Communication Service Providers for a period between three to five years after the interception has been concluded.[3703] However, two categories of Online Communication Service Provider identified by RICA are also empowered to store real-time and archived data for a *cumulative* period of three years.[3704]

Secondly, although the minimum duration of keeping such records for five years might be seen to consider the principle of proportionality because the duration could be extended to ten years or more, the fact that the minimum period is five years negatives proportionality principle. This is because some records may not be required to be kept for up to five years at all in the following circumstances, amongst others:

a) Where proportionality principle is considered by the authorities in terms of the degree of seriousness of an offence, this, in turn, determines how long the copies of OCI applications must be kept by the designated authority, thus, a rigid five-year period will be disproportionate to keep the records of the outcome of the conduct of an OCI for a generally serious offence.[3705]

b) Drawing on the U.S. practice where there is a delivery of a post-OCI execution notice[3706] to an interception target who, within a reasonable period, subject to the extent of invasion of the right to the SOC, decides whether to consider pursuing legal action against the LEAs for the unjustifiable, irrational and unreasonable invasion of the right to the SOC. Therefore, the five-year period will not apply where the court holds otherwise on the justifiability and reasonableness of the invasion of the right to the SOC. In this instance, the time of the

[3702] See section 19(8) of RICA and para 6.4.1 of this study titled 'Management of data in *pre*-online criminal investigation application'.
[3703] Section 30(2)(a)(iii) of RICA.
[3704] RICA provides for three categories of Online Communication Service Provider which are fixed line operator ('FLO'), mobile cellular operators ('MCO') and Internet Service Providers ('ISP'), see para 1 of Schedules A - C of RICA Directive 2005. Amongst these three, FLO and MCO are empowered to store data, see para 13.2 and 17 of Schedules A and B of RICA respectively. Given the foregoing, it is obvious that ISPs are not required to have any storage capacity in this regard. In the U.S., small service providers lack capacity to store secure their systems, see Schedule C of RICA, see also Landau *Lawful electronic surveillance in the face of new technologies* 226.
[3705] Paras 6.3 - 6.6 and 7.3.5 of this study.
[3706] In the state of Maryland in the U.S., 60-day post notice is served on a person after the conclusion of an investigation, Cassilly *Geolocational Privacy and Surveillance Act* 269.

destruction of the data will be subject to the duration of the litigation for remedy by the target. However, there is no such provision on legal redress by a target in RICA.

c) Where after accessing the data gathered and LEAs discover that there is no need for prosecution,[3707] there will not be any need to keep a record of the copies of OCI applications for at least five years or any period whatsoever once the discovery is made.

d) Where there is provision for the role of a ghost or public advocate,[3708] the adverse interest of a target would be canvassed for by the advocate, which includes the application for the destruction of the copies of OCI applications before five years, subject to other factors, which include paragraphs (a) and (b) above, therefore, there will not be any need to keep data for five years or any other period;

e) Where data is gathered for purposes of tracing and tracking a person during the state of health disaster relating to the control of the spread of the coronavirus pandemic.[3709]

7.5.7 Double jeopardy in the management of data in the pre-and post-online criminal investigation

It is submitted that the general concept of double jeopardy states that a victim suffers twice or more in terms of the infringement of a right of the victim, the infringement of which should not have occurred in the first place.

In the management of data in the pre-and post-execution of an OCI and a ROCI, the occurrence of the concept of online conscription is the first and an automatic, indispensable or inevitable techno-legal infringement of the right to the SOC which commences the moment an online communication device is activated, and the infringement never ends, even after death. This is because some types of data —such as meta and traffic, which are indispensably recorded in every communication— are automatically, generally and perpetually recorded, stored and

[3707] Section 29(8)(b)(i) & (ii) of RICA.
[3708] Para 6.10.2 of Chapter 6 of this study.
[3709] Para 6.2.4 of Chapter 6 of this study.

tracked in the first instance[3710] before the second and occurrence of more infringements, which may or may not be permissible under the limitation clause of s 36 of the Constitution.

An infringement of the right to the SOC is one too many given the high levels of risk and protection of the right to the SOC,[3711] therefore, the second or subsequent infringements should be reasonably and justifiably conducted proportionately in every applicable area examined in this study.

7.5.8 Conclusion

The management of data between the pre-and post-execution of an OCI or ROCI lies in all authorities, entities, parties or persons that would have had one form of access to offline, and online data in the process of conducting or attempting to conduct an OCI or ROCI. Thus, in the performance of official duty; authorised persons, LEAs, LEOs, court, Online Communication Service Provider, Decryption Keyholders and employees of Online Communication Service Provider manage data between the pre and post-execution of an OCI. This is because there is a general prohibition of disclosure of data gathered in the process of conducting or attempting to conduct an OCI, given that an online communication perpetually remains a secret,[3712] save where required by law to disclose such secret data.[3713]

7.6 MANAGEMENT OF THE AFFAIRS AND ACTIVITIES OF THE AUTHORITIES OVERSEEING THE LAW ENFORCEMENT AGENCIES IN THE CONDUCT OF ONLINE CRIMINAL INVESTIGATION

7.6.1 Introduction

Given the sensitive nature and features of the right to the SOC and the conduct of an OCI, it is imperative and equitable that the authorities, bodies and entities —such as the JSCI and the OIGI— overseeing the affairs and activities of investigators and interception entities in the

[3710] Paras 2.3.3 and 2.6.2 of Chapter 2 of this study.
[3711] Chapter 3 of this study.
[3712] Sections 42(1), (2) & (3) and 43 of RICA.
[3713] Sections 29(1)(a), (2) (a), (b) &(c), (3)(b), (4)(a) &(b), (7) & (8)(b) of RICA. See also Schedules A-C of RICA Directive 2005.

conduct of an OCI should themselves be competent, transparent, independent and accountable[3714] in this regard.

The court held in *AmaBhungane* that the oversight regime on the conduct of an OCI in RICA is 'extremely light'.[3715] However, the oversight of interception affairs and activities is not absolutely lacking because the court held in the same case that the level of oversight is what is insufficient[3716] in the RSA, hence there is some level of oversight which is not sufficient to curb the continued infringement of the right to the SOC. Drawing on the practice by Barrack Obama (the former president of the U.S.) on OCI safeguards, he did not only block reform on the interception, but he took steps to 'expand unaccountable and unchecked surveillance power',[3717] the phenomenon of which is not too different in the RSA.

7.6.2 Role of non-governmental entities in the execution and post-execution of the conduct of online criminal investigation by law enforcement agencies

Aside from the statutory authorities that oversee the activities and affairs of the stakeholders in the conduct of an OCI, other entities that offer oversight functions on the interception affairs and activities[3718] are the non-governmental entities which include journalists, blogosphere,[3719] civil societies and pressure groups within and outside the RSA.

In executing its role in the oversight of the activities and affairs of the stakeholders in the conduct of an OCI, about forty society organisations —amongst these non-governmental entities— recently signed a petition that RICA should be amended in many ways[3720] while two civil society groups requested for a myriad of reliefs before the court praying for: a declaration that notice be given to targets after an OCI is completed; establishment of the appropriate procedure for copying, storing, sorting, examining, sharing, using, and destroying of

---

[3714] Right2Know 36 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).
[3715] *AmaBhungane v Minister of Justice* supra 106.
[3716] *AmaBhungane v Minister of Justice* supra 89(1) and (2) and 106; Rosenzweig *The sky isn't falling* 52.
[3717] *Greenwald Digital surveillance state: Vast, secret, and dangerous* 38-39 and 45; Rosenzweig P 'The sky isn't falling' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 49 (Rosenzweig *The sky isn't falling*).
[3718] Rosenzweig *The sky isn't falling* 50.
[3719] Rosenzweig *The sky isn't falling* 50.
[3720] Right2Know 34 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use:27 November 2018).

information obtained after conducting and OCI[3721] and a release of information by LEAs on how many applications were unlawfully brought before Magistrate Court.[3722]

It is argued that any non-governmental entity that intends to oversee the affairs and activities of the stakeholders in the conduct of an OCI must be competent, transparent, independent and accountable in these contexts which include objectivity, rationality and impartiality of the non-governmental entities. These qualities or characteristics are crucial so that the society at large is not misdirected or misled by domestic or foreign negative power or influence which is aimed at spying or destabilising the RSA. Also, the non-governmental agencies should not be engaged in some counter-productive or revolutionary, gender-based, inflammatory, provocative, malicious, outrageous, racist, retrogressive, unfair discriminatory, unjustifiable and unreasonable political and seditious claims and statements regarding the regulation or the conduct of an OCI in the RSA.

7.6.3 Role of the Office for Interception Centre in the execution and post-execution of the conduct of online criminal investigation by law enforcement agencies

7.6.3.1. Introduction

Although the OIC is the supervisory authority overseeing the activities and affairs of the Interception Centres in the RSA,[3723] however, it seems the acronym and the functions of this office are misconstrued by some writers and Parliament.[3724] This is because the Office for Interception Centre is different from the Interception Centre as generally examined in this study.

7.6.3.2 Human capital at the Office for Interception Centre

Although RICA provides that the Director, acting Director and officers of the Office for

[3721] Sole https://mg.co.za/article/2017-04-20-surveillance-silent-killer-of-journalism-and-democracy-1 (Date of use: 5 April 2018).

[3722] Lotz B 'How wide spread is state surveillance in SA? Right2Know is trying to find out' http://www.htxt.co.za/2017/05/25/how-wide-spread-is-state-surveillance-in-sa-right2know-is-trying-to-find-out/ (Date of use: 31 May 2017).

[3723] Para 7.3.6 of this chapter; *AmaBhungane v Minister of Justice* supra 34.

[3724] Swart 'Communication surveillance by the South African Intelligence Services' 2016 at 20 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use: 13 August 2016); JSCI Reports 2016 at 19.

Interception Centre are seconded to the OIC from other relevant departments,[3725] however, there is no law, regulation, policy or understanding on the requirements for the appointment of the incumbent. Essentially, there are no requirements for special knowledge, experience, training and skill in the employment, retention, deployment and execution of the functions of the office as a specialised group or unit[3726] in the techno-legal conduct of an OCI, which requires some relevant level of technocracy and professionalism.[3727]

7.6.3.3 Regulation of online criminal investigation procedure by the Director of Office for Interception

The OIC does not have any technical capability to conduct an OCI,[3728] but the Director of OIC has the administrative function of regulating and controlling the conduct of an OCI at the Interception Centre.[3729]

7.6.3.4 Competence and independence of the Office for Interception Centre

The competence and independence of the OIC are as follows.
Firstly, the OIC is not statutorily, technically and operationally expected to conduct an OCI as erroneously claimed by the court in *AmaBhungane* and a writer.[3730] It only engages in mere administrative responsibility in support of the functions of the stakeholders in conducting an OCI by the Interception Centres,[3731] thus the OIC is arguably incompetent and irrelevant in the technical aspects of the conduct of an OCI.

The fact that the relevance of the OIC is purely and merely administrative in the conduct of an OCI which can equally be carried out by a single and centralised Interception Centre —which is required to employ technical, operational and functional expertise— logically, reasonably

[3725] Section 34(1), (3), (4)(a)(i) - (iii) & (v) (b) and (5) of RICA.
[3726] Although s 195(5) of the Constitution stipulates that different or special legislation may be enacted to address the needs of 'different sectors, administration or institutions' however, this study posits that there is no specific law that addresses the issues raised herein.
[3727] Para 4.6 of Chapter 4 of this study.
[3728] JSCI Report 2016 para 4.7.2 at 19.
[3729] Sections 35(1) (a) -(h), more particularly paras (d), (e), (f), (g) & (h) and 36 (2) of RICA.
[3730] *AmaBhungane v Minister of Justice* supra 85; Swart 'Communication surveillance by the South African Intelligence Services' 2016 at 20-21 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use: 13 August 2016).
[3731] Para 7.3.6 of this chapter.

and substantially shows the technical, operational and functional incompetence and irrelevance of the OIC in the conduct of an OCI and management of the affairs and activities of the Interception Centres.

For example, the Director of OIC only oversees any defect discovered by the head of the Interception Centre in the telecommunication system or the operation of Interception Centre but the Director of OIC does not deal with the technical, operational or functional tasks of a telecommunication system,[3732] which is impliedly expected to be executed by the Interception Centre and independent of the OIC. Overtime and generally, oversight authorities in the RSA —such as the oversight authority by the erstwhile Minister of Police on IPID— have shown the tendency of frustrating the daily or routine running of the overseen entities.[3733] Therefore, it is submitted that the OIC is not competent nor relevant to oversee the affairs and activities of the Interception Centre in this regard.

Secondly, despite the consent and security clearance required from a seconded LEA[3734] and the constitutional principle of cooperative governance[3735] that enable secondment from other LEAs to the OIC in practice,[3736] the independence of the OIC is eroded by the provision for secondment only into the office of Director and officers of the OIC.[3737] One of the adverse implications is that it expressly or impliedly excludes anyone from outside the already existing agencies from being employed at the OIC. Although this provision may reluctantly be retained, it still does not prevent infiltration in these offices, if infiltration would inevitably occur.

Therefore, this provision should be amended to make the appointment into the OIC be open to the security cleared public to ensure availability or supply of competitive recruitment resources for the above positions.

[3732] Section 37(2)(a)(iii) of RICA.
[3733] Para 4.5.4 of Chapter 4 of this study.
[3734] Section 34(5) (b) &(c) of RICA.
[3735] Chapter 3 of the Constitution. Section 35(3) of RICA.
[3736] Section 34(1), (3), (4)(a) & (b), (5) of RICA.
[3737] Section 34(2) of RICA.

7.6.3.5 Oversight by and of the Office of the Interception Centre

The Director of OIC prescribes the type of data or information to be kept by the head of the Interception Centre relating to section 37 of RICA which includes the information about the application before the court, the direction of court relating to the specific Interception Centre and the outcome of the conduct of an OCI arising from the direction of the court.[3738] The Director of OIC also oversees the Interception Centre by prescribing the manner in and the duration within which data is kept.[3739]

Upon a request for a report on any activity of the Interception Centre or any activity in the Act relating to the powers of the Director of the OIC[3740] or a for an urgent report to the Director of OIC on any matter as determined by the Director of the OIC,[3741] the Director of the OIC oversees the written record or report submitted every quarter or as urgent or often as possible to it by the head of the Interception Centre.[3742] The Director of the OIC oversees the submission of records of any abuse relating to the execution of a direction which the head of Interception Centre is aware of.[3743]

These reports are submitted to the Minister of SSA and chairperson of the JSCI of Parliament, which the court criticises that is inadequate because it does not provide for judicial oversight in this regard.[3744] However, it is noted that limiting the responsibility of reporting only abuses that are known to the head of the Interception Centre is inadequate because, save there is a written proof of knowledge of abuse, all that the head of the Interception Centre needs to do is to feign ignorance of the abuse and that will be legally justified in RICA. However, it is recommended that an electronic register of complaints or petitions indicating abuse of execution of direction be established and maintained.

[3738] Section 35(1)(a)(f) of RICA.
[3739] Section 35(1)(a)(g) of RICA.
[3740] Section 37(2)(a) (iv)of RICA.
[3741] Section 37(2)(b) of RIICA.
[3742] Section 37(1), (2)(a)(i)-(iv) of RICA.
[3743] Section 37(2)(a)(ii) of RICA.
[3744] Section 37 (3) of RICA; *AmaBhungane v Minister of Justice* supra 106.

The affairs and activities of the OIC are overseen by the Minister of State Security because it is a unit under the State Security.[3745] However, the fact that the Director of the OIC[3746] is accountable to and under the control and direction of the Minister of State Security only[3747] proves that there is over-concentration of power in the executive arm of government. This may lead to abuse of power by or any of the duo and lack of oversight authority by Parliament and other independent overseers.

Should the above *status quo* prevail, one of the remedies to this defect is the invocation of the general powers of Parliament to ensure that the OIC is not dependent on the direction of the Minister of the State Security to control the OIC but on Parliament, as an arm of the government. This is because the fact that the Constitution empowers the Parliament to summon any authority or person -both public and private- to render account for their activity[3748] re-affirms the inherent broad powers of Parliament[3749] to oversee the affairs of the OIC.

However, the downside of the ad-hoc intervention by Parliament is that since there is no stipulated or mandatory period of appearance of the OIC in Parliament, it is more likely that OIC would only be invited to Parliament too late when various breaches of the law occur by which time serious challenges would have arisen in the operation of the OIC. Instead, in applying the checks and balances principle, RICA should be amended to ensure that the Director of OIC should be accountable to the Parliament.

Additionally, there is the need to emulate the ITU regime which creates the office of Independent Monitoring Authority —which is similar to the role of IPID—[3750] or the OIGI[3751] with the 'power to provide guidance and controls' in ensuring compliance with OCI requirements[3752] or an Independent Commissioner of Interception of Communication is appointed by Parliament to address OCI issues,[3753] the office of which is similar to the OIGI.[3754]

[3745] Section 34(2) of RICA; Swart 'Communication surveillance by the South African Intelligence Services' 2016 at 1 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use: 13 August 2016.
[3746] Section 35(1) (d), (f) & (g) and 37 (1) of RICA.
[3747] Section 35(1)(h) of RICA.
[3748] Section 56 of the Constitution.
[3749] Sections 42 (3), 44 (3), 55 (2) (a) & (b) (i) & (ii) and 56 (a) - (d) of RICA
[3750] Paras 4.3.4, 4.4.4 and 4.5.4 of Chapter 4 of this study.
[3751] Para 7.6.4 of this chapter.
[3752] Section 34 of ITU 'Interception Policy & Legislative Text' (2012).
[3753] Section 35 of ITU 'Interception Policy & Legislative Text' (2012).
[3754] Para 7.6.4 of this chapter.

The UN also recommends that LEAs should regularly report to Parliament on various issues concerning the conduct of an OCI which may be full, and partial reports,[3755] which include the provision of a copy of the interception order.[3756]

7.6.3.6 Conclusion

It does seem that the relevance of the operation of the OIC is not significant nor the competence of the OIC adequate in the conduct or administration of an OCI due to the lack of requirement of specialised skill in the techno-legal oversight of the affairs and activities of the Interception Centre. Therefore, the OIC should be abolished, while the administrative powers of the OIC should be transferred to a single and independent Interception Centre to statutorily administer and manage its activities and affairs. Furthermore, based on the principles of competence, transparency and independence, the Parliament and the OIGI should, in furtherance of these recommendations, oversee the activities and affairs of the single and independent Interception Centre accordingly.

7.6.4 Role of the Office of the Inspector-General of Intelligence in the execution and post-execution of the conduct of online criminal investigation by law enforcement agencies

7.6.4.1 Introduction

The OIGI[3757] is one of the authorities charged with the responsibility of overseeing the activities and affairs of the role players[3758] in the conduct of an OCI. These role players are the three LEAs established in the statute in this regard namely the SSA, CI-SAPS and CI-SANDF only.[3759] Thus, the regulation of the three LEAs only creates a lacuna regarding the authority

[3755] Art 16(12)(c), (14) and (15) of UNODC 'Model legislative provisions against organised crime 2012 at 64 and 83-84.
[3756] Art 16 (9) of the UNODC 'Model legislative provisions against organised crime 2012 at 64.
[3757] Para 4.5.5 of Chapter 4 of this study.
[3758] Section 210 of the Constitution.
[3759] See the definition of 'services' in s 1 of ISOA; PMG 'Nomination: Appointment of the Inspector General for Intelligence' https://pmg.org.za/call-for-comment/418/ (Date of use: 31 January 2018). It is also noted that applying s 2 of National Strategic Intelligence Act No 39 of 1994 ('NSIA') in *AmaBhungane v Minister of Justice* supra 149, the court referred to only the SSA, SANDF and CI-SAPS as the only LEAs that the SSA is empowered to 'train, and support users of electronic communication systems, products and related services' and provide security in this regard in addition to the developing, designing, procuring, inventing, installing or maintaining electronic communication systems.

that oversees other statutory LEAs in the conduct of an OCI which are the HAWKS, IPID and ID-NPA[3760] and the other types of investigators propounded in this study.[3761]

7.6.4.2 Human capital at the Office of the Inspector-General of Intelligence in the conduct of online criminal investigation by law enforcement agencies

The OIGI is constitutionally and statutorily established and the incumbent, who must be a South African citizen, is appointed by the President of the RSA based on the nomination by the JSCI and approved by two-third of the members of the National Assembly who have an option to nominate someone else amongst the nominees if they are dissatisfied with the main candidate.[3762]

The requirement that the IGI must be a fit and proper person[3763] and must have knowledge of intelligence services[3764] demonstrates to a large extent the fulfilment of the competence, independence and accountability of the IGI in overseeing the role players in the conduct of an OCI.[3765] To ensure the independence of the IGI, the incumbent appointed in 2017 went through some public interview and scrutiny processes.[3766] However, there is still no specific, published, and complementary legal framework —including advert placement decision or policy— that requires the head and members of the OIGI in the conduct of an OCI to be specialists or have some level of competency in the field of OCI as part of the requirements for the relevant positions.[3767]

The OIGI shall ensure compliance with the security requirements for the employees in the three LEAs herein and shall serve independently and impartially and perform the duty of the IGI in good faith and without bias, fear, favour or prejudice.[3768]

[3760] Para 4.2 of Chapter 4 of this study.
[3761] Paras 2.11.3 - 2.11.6 of Chapter 2 of this study.
[3762] Section 210(b) of the Constitution; Section 7(1) (a) &(b) and (2) of Intelligence Services Act 40 of 1994 (ISOA).
[3763] Paras 4.3.2, 4.3.4 and 4.37 of Chapter 4 of this study.
[3764] Section 7(2) of the ISOA; PMG 'Nomination: Appointment of the Inspector General for Intelligence' https://pmg.org.za/call-for-comment/418/ (Date of use: 31 January 2018) PMG https://pmg.org.za/call-for-comment/418/ (Date of use: 31 January 2018).
[3765] PMG https://pmg.org.za/call-for-comment/418/ (Date of use: 31 January 2018).
[3766] JSCI Report 2017 at 2017' 8-9.
[3767] Section 7(12) of the ISOA; PMG https://pmg.org.za/call-for-comment/418/ (Date of use: 31 January 2018).
[3768] Section 7(10) (a) & (b) of the ISOA.

Given the sensitive nature of the position of the IGI, the absolute power of the President of the RSA to remove the incumbent on grounds of withdrawal of security clearance,[3769] misconduct, incapacity, poor performance or incompetence[3770] is inadequate. Rather, the removal of the incumbent should be sanctioned by the National Assembly. However, it is reasonable to allow the President of the RSA to suspend the incumbent for the same grounds while an investigation is being carried out by the National Assembly[3771] to ensure the balance of interests and power, where it is necessary.

The statutory provision that the remuneration and condition of employment of the IGI is determined by the President and JSCI of Parliament and that the remuneration and condition of employment[3772] shall not be reduced goes a long way to ensure the competence, independence and accountability of the Inspector General of Intelligence in overseeing the role players in the conduct of an OCI.

7.6.4.3 Operation and funding of the Office of the Inspector-General of Intelligence in the conduct of online criminal investigation by law enforcement agencies

a) the OIGI monitors the level of compliance with the Constitution, other law and policy on intelligence and counterintelligence by the three LEAs which are overseen by the OIGI herein;[3773]

b) the OIGI reviews the intelligence and counter-intelligence activities of the three LEAs herein;[3774]

c) the OIGI executes the functions assigned to the IGI by the President of the RSA and the Minister of State Security,[3775] which are critiqued as being too broad. However, the provision that the Inspector General of Intelligence should report to the President and relevant minister on the assigned duty by the President and Minister[3776] is appropriate. This

[3769] PMG https://pmg.org.za/call-for-comment/418/ (Date of use: 31 January 2018).
[3770] Section 7 (4) of the ISOA.
[3771] Section 7(5) of the ISOA.
[3772] Section 7(3) of the ISOA; PMG https://pmg.org.za/call-for-comment/418/ (Date of use: 31 January 2018).
[3773] Section 7(7)(a) of the ISOA; *AmaBhungane v Minister of Justice* supra 99.
[3774] Section 7(7)(b) of the ISOA.
[3775] Section 7(7)(c) of the ISOA.
[3776] Section 7(7)(f) of the ISOA.

is because the President of the RSA and the relevant ministers are the respective chief security officers of the RSA and the political head of the relevant ministry who should be in the loop of the intelligence and security situation.

However, it is incongruous that the President and the Minister of State Security determine the scope of the function of the IGI because the power of the President and the relevant minister is statutorily undefined and uncertain in this regard. Therefore, the undefined and uncertain powers pose a danger to the administration of the conduct of an OCI because unconstitutional powers which impact on the conduct of an OCI might be wielded by the President or relevant minister in this regard;

d) the OIGI carries out investigation received from members of the public and the three LEAs herein concerning maladministration, abuse of office or power, breach of the constitution, other law or policy, commission of some serious offences, unlawful enrichment of a 'person through an act or omission of any member' of the three LEAs herein.[3777]

e) the OIGI shall have access to any intelligence, information or premises required, and shall demand from a LEA or its head or employees such necessary information, intelligence, report or explanation for the performance of the office.[3778]

However, arguably, there is no provision that refers to the online communication as part of information or intelligence in this regard, thus the OIGI will be acting ultra vires should a petition relating to the conduct of an OCI be submitted by a complainant. The High Court held in *AmaBhungane* that the express mention of a thing is to the exclusion of the others,[3779]

[3777] Section 7(7) (cA) of the ISOA. First, it is reported that the authorities only considered a petition submitted by two investigative journalists who were described as ATM bombers because a former Commissioner of Police who doubled as a current Minister of Police was mistakenly intercepted, otherwise the petition would not have been considered. Second, in another case, the petition submitted by an investigative journalist in 2015 has not been resolved (in May 2018) by the OIGI, while another investigative journalist decided to abandon an earlier petition submitted to the OIGI because of the expectation that no fruitful result will emerge as at May 2018 when the report was published. Third and finally, in a petition submitted by an investigative journalist, the I-GI objectively reported that the identity of the journalist, including the name of the media house, was disclosed to Judge Khumalo who ordered the OCI direction, for all these petitions, see Right2Know 'Spooked- Surveillance of Journalists in SA' at 6-7, 13-14 and 26 and 33 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018). (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).

[3778] Section 7(8)(a) of the ISOA.

[3779] *AmaBhungane v Minister of Justice* supra 163 and 164.

which arguably means that since the scope of the function of the OIGI does not cover online communication, a lacuna is created in this regard.

f) before the intention to physically access the premises of the relevant LEA, the OIGI dispatches a written notice to the head of the relevant LEA stating the date and nature of access to the premises.[3780] Information gathered must be considered accordingly after consultation with the President and the relevant minister responsible for the LEA without breaching national interests and restriction.[3781]

Although consent to access the premises is not required, but a notice is. However, the mere fact that notice is issued by the OIGI to the relevant LEAs before having physical access to the premises of a LEA defeats the essence of gathering more information in the investigation in this regard. The issuance of notice clearly indicates that this provision relates to an offline investigation only by OIGI because RICA does not allow the issuance of a notice to any target in the circumstances examined in this study.[3782] Essentially, the ISOA does not make provision for the empowerment of the OIGI to conduct an OCI against LEAs in which a complaint has been lodged.

g) The IGI shall, in the performance of the function of the office, subject to a warrant, have access to information, intelligence or premises which are not under the control of the three LEAs herein, provided the information is necessary for the performance of the duty of the OIGI.[3783] Information gathered must be considered accordingly after consultation with the person in possession of the information, President and the relevant minister responsible for the LEA without breaching national interests and restriction.[3784] However, the leakage of information by officials in the OIGI was recently reported.[3785]

h) the independence of the OIGI is guaranteed by the allocation of funds to the OIGI which is directly disbursed from the Appropriation Account approved by Parliament.[3786]

[3780] Section 7(7) (aA) of the ISOA.
[3781] Section 7(8)(b)(i)-(iii) of the ISOA.
[3782] Para 6.2 of Chapter 6 of this study.
[3783] Section 7(8)(c) of the ISOA.
[3784] Section 7(8)(d) (i) -(iv) of the ISOA.
[3785] JSCI Report 2016 at 15.
[3786] Section 7(13) of the ISOA.

7.6.4.4 Accountability and oversight by and of the Office of the Inspector-General of Intelligence in the conduct of online criminal investigation by law enforcement agencies

To ensure the accountability of LEAs and non-LEAs in the conduct of an OCI, no information is withheld from the OIGI in the performance of his or her duty.[3787] This gives the OIGI the opportunity of scrutinising the management of the activities and affairs of the LEAs and non-LEOs in the conduct of an OCI.

Each of the head of the three LEAs that the OIGI oversees[3788] is required to submit a report every year or at an earlier period to the relevant Minister, as may be determined by the relevant Minister heading the three LEAs herein on the activities and affairs of the three LEAs, a copy of which is submitted to the OIGI by the head of the LEA.[3789]

The IGI shall, as soon as practicable after receiving the report from each of the three LEAs, submit a certificate to the relevant minister indicating the level of satisfaction by the IGI on the report submitted by the LEAs. The certificate indicates, whether there was: any unlawful contravention of the direction issued by the relevant minister; an unlawful intelligence activity; any unreasonable or unnecessary exercise of power by the LEA; an important intelligence failure by the three LEAs herein and whether any remedy has been taken or intended to be taken by the three LEAs herein regarding the report.[3790] Thereafter, the relevant minister shall respectively submit the reports earlier received from the LEA and a certificate of satisfaction from the OIGI to the JSCI of Parliament.[3791]

The provision that the IGI submits reports on his or her overall activities and performances to the JSCI at least once a year[3792] is to the extent of submitting a report adequate to ensure that separation of powers and checks and balances prevail. However, given the sensitive nature of the intelligence services where there is a breach of the right to the SOC and the conduct of an OCI, a yearly submission of report by the IGI is inadequate. Therefore, it is recommended that

[3787] Section 7(9) of the ISOA.
[3788] Para 7.6.4.1 of this chapter.
[3789] Section 7(11)(a) of the ISOA.
[3790] Section 7(7)(d) and (11)(a)-(c)(i) & (ii) of the ISOA.
[3791] Section 7(11)(d) of the ISOA.
[3792] Section 7(6) and (7)(e) of the ISOA; PMG 'Nomination: Appointment of the Inspector General for Intelligence' https://pmg.org.za/call-for-comment/418/ (Date of use: 31 January 2018).

a clause that includes that the reporting schedule should be quarterly done or as and when required by the JSCI of Parliament will be adequate.

7.6.5 Role of the Joint Standing Committee on Intelligence of Parliament in the execution and post-execution of the conduct of online criminal investigation by law enforcement agencies

7.6.5.1 Introduction

The JSCI of Parliament, which is a creation of statute, oversees the activities of the three LEAs herein namely SSA, CI-SAPS and CI-SANDF on intelligence matters in the RSA.[3793] The JSCI has the power to consult with relevant ministers of the three LEAs herein whose functions relate to the performance of the duty of and oversight by the JSCI.[3794]

7.6.5.2 Human capital at the Joint Standing Committee on Intelligence in the conduct of online criminal investigation by law enforcement agencies

The JSCI comprises fifteen security cleared members of Parliament who are equitably appointed on proportional representative principle to serve in this committee.[3795]

It might be argued that the members of the JSCI merely perform oversight functions on the various stakeholders in the conduct of an OCI. However, there is no specific, published, and complementary legal framework —including advert placement decision or policy— that requires the chair and members of the JSCI to be specialists or have some level of competence in the field of OCI as part of the requirements for the relevant positions,[3796] given the complex and delicate nature and features of the protection of the right to the SOC and the conduct of an OCI.[3797]

To demonstrate one of the effects of the absence of the requirement for specialised skill in the conduct of an OCI for anyone or entity that is involved in the management, supervision or

[3793] Sections 2-6 of the ISOA.
[3794] Section 3(k) of the ISOA.
[3795] Section 2(2)(a)(i)-(iii) and (b) of the ISOA.
[3796] Para 4.3 of Chapter 4 of this study.
[3797] Chapters 2 and 3 of this study.

oversight of the conduct of an OCI, the JSCI, in its report, erroneously states that the OIC is involved in the operational conduct of an OCI, which in law contradicts the provisions of RICA, though the JSCI on the other hand rightly posits that the OIC carries out administrative and implementation functions in the conduct of an OCI.[3798]

7.6.5.3 Operation and funding of the Joint Standing Committee on Intelligence in the conduct of online criminal investigation by law enforcement agencies

The JSCI holds hearings, makes deliberations, subpoenas witnesses and makes recommendations on administrative and financial issues relating to intelligence and national security of the RSA.[3799]

In its operation, the JSCI reviews and makes recommendations on the interdepartmental working and cooperation, rationalisation and demarcation of functions among the three LEAs that the JSCI has control over.[3800]

The JSCI receives and refers to report from the appropriate Commission on issues concerning the promotion, protection and infringement of the Bill of Rights in the Constitution,[3801] thus asserts authority on LEAs for the breach of the Bill of Rights.

The JSCI invites explanation from the following office holders concerning any aspect of the report submitted by the A-G and the Secret Services Evaluation Committee: the heads of the three LEAs, the relevant ministers, the Inspector-General of Intelligence and the designated judge.[3802]

However, on the explanation of the report submitted by the designated judge, it is submitted that given the opinion in this study about the opposition to the appointment of a retired judge as a designated judge to adjudicate on the OCI application,[3803] the fact that Parliament can ask the designated judge questions whittles down the independence of the operation of the judge.

[3798] Sections 32 - 36 of RICA; JSCI Reports 2016 at 19.
[3799] Section 3(j) & (l) of the ISOA.
[3800] Section 3(e) of the ISOA.
[3801] Section 3(g) of the ISOA.
[3802] Section 3 (a), (b), (f), (h) and (i) of the ISOA.
[3803] Para 6.7 of Chapter 6 of this study.

The powers of a designated judge are only subject to judicial review by a higher court and not by Parliament in this instance. The practice of whittling down the powers of the interception judges in the RSA is not new in other instances and countries. After the 9-11 terrorist attacks, courts in the U.S. have now become 'extremely submissive to executive authority 'in the name of security',[3804] which compromises the independence of the operation of the judiciary.

Given that the JSCI is a committee of Parliament, it is funded from the budget allocated to Parliament by the Appropriation Account approved by Parliament itself.

Finally, in all the provisions examined above, none of the provisions specifically address the unique role of the JSCI on the nature and features of the right to the SOC and the conduct of an OCI thus creates some inadequacies in striking a balance between the duo, though one might rely on the implied role of the JSCI to address these inadequacies.

7.6.5.4 Accountability and oversight by and of the Joint Standing Committee on Intelligence in the conduct of online criminal investigation by law enforcement agencies

Where the JSCI receives a complaint lodged by the public which breaches the complainant's individual right to personhood or property, the JSCI orders and receives a report of a meritorious and *bona fide* investigation to be conducted by the concerned head of a LEA or the OIGI.[3805] Also, the JSCI oversees the three LEAs herein by considering and making a recommendation on the report and certificate submitted concerning the contravention of the law in the execution of intelligence services.[3806]

The JSCI oversees the administrative and financial activities of the three LEAs herein and reports same to Parliament.[3807] In doing this, the JSCI obtains financial statements, audit reports and other reports from the A-G to enable the former to do its job and report to Parliament.[3808] Two types of reports are submitted to Parliament, comprising the comprehensive report which

[3804] Greenwald *U.S. Filmmaker repeatedly detained at border* 185.
[3805] Section 3(f) of the ISOA.
[3806] Section 3(b) of the ISOA.
[3807] Section 2(1)(a) & (b) of the ISOA.
[3808] Section 3(a)(i) (aa)-(cc) of the ISOA.

is known to the oversight committee, while the general report which is submitted to Parliament shows the general statistics of the conduct of an OCI.[3809]

The JSCI oversees the three LEAs herein by initiating, considering, making a recommendation and reviewing legislation on intelligence activities and services, thus the JSCI makes the three LEAs accountable *ab initio* to it.[3810]

The JSCI requests from the Secret Services Evaluation Committee reports on the secret services as well as the proposed secret services which are evaluated and reviewed by the JSCI in conjunction with any comment or recommendation made at the discretion of the Secret Services Evaluation Committee.[3811] The JSCI also requests from the designated judge a report on the function performed by the judge in RICA including the appropriate comments, recommendations and statistics on the conduct of an OCI by LEAs but the report excludes the specific identification of an OCI application or direction.[3812]

In addition, the JSCI requests for a report on the budget of the three LEAs herein from the relevant ministers.[3813] It is noted that although no provision requires the JSCI to ask questions relating to the reports submitted by the designated judge and the relevant ministers of the three LEAs herein, it is submitted that the JSCI may ask questions in these regards subject to the criticism on querying a designated judge on the report submitted.[3814]

In addition to the oversight of the JSCI by Parliament, it remains to be seen that Parliament will not take decisions based on political affiliations on the protection of the right to the SOC and the conduct of an OCI, thus compromises the competence, objectivity, functions, operations and independence of the oversight function of Parliament.

Therefore, it is, in the interim, recommended that the chairperson of the JSCI be appointed or elected from the minority party as it is being practised in the SCOPA. A long-run recommendation, which is subject to the amendment of the Constitution on electioneering, is

[3809] JSCI Reports 2016 at 48-52.
[3810] Section 3(c) & (d) of the ISOA.
[3811] Section 3(a)(ii) of the ISOA.
[3812] Section 3(a)(iii) of the ISOA.
[3813] Section 3(a)(iv) of the ISOA.
[3814] Section 3 (i) of the ISOA; Para 7.6.5.3 of this chapter.

to provide that parties that contest for the presidential position cannot contest for parliamentary seats or a party that contests for a presidential position can only contest for not more than 49 % of the seats in Parliament even where a party wins more votes than 49 % of the votes cast.

It is presumed that where a party has more than 49 % of the votes or seats but cannot be allotted more than 49 % of the votes, the occupation of the presidential position would compensate for the unrecognised surplus votes in Parliament. This measure is meant to ensure that Parliament is largely accountable, independent, objective and transparent and does not compromise on several national issues based on party loyalty, including the subject matter in this study.

7.6.6 Role of the judiciary in overseeing the execution and post-execution of the conduct of online criminal investigation by law enforcement agencies

7.6.6.1 Introduction

The judiciary plays significant oversight,[3815] adjudicative,[3816] administrative and supervisory roles in the various oversight of the activities of the stake holders in the conduct of pre and post OCI.[3817]

7.6.6.2 Human capital at the judiciary in overseeing the conduct of online criminal investigation by law enforcement agencies

There is no specific, published, and complementary legal framework —including advert placement, decision or policy— that requires a designated judge, judge and magistrate in the conduct of an OCI to be a specialist or have some level of competence in the field of OCI as part of the requirements for the relevant positions. It is therefore not surprising that several erroneous pronouncements have been made by the courts denying the existence of one form of duty, right or liability in online communication integrity, safety and security and the conduct of an OCI.[3818] The existence of facts on the erroneous decisions by the court on this subject is exposed in the decision of the court in *AmaBhungane* that using retired judges as designated

[3815] *AmaBhungane v Minister of Justice* supra 27.
[3816] *AmaBhungane v Minister of Justice* supra 35.
[3817] For example, paras 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11, 6.12, 6.13, 6.14, 6.15, 6.16 and 7.4 of this study.
[3818] Paras 3.5.3, 3.5.5, 3.5.7 and 6.4.3 of this study.

judges enriches the pool of experienced jurists and enhance competence, decision making skill, impartiality, independence and legal knowledge.[3819]

7.6.6.3 Operation and funding of the judiciary in overseeing the conduct of online criminal investigation by law enforcement agencies

The determination of the competence and independence of the judiciary in carrying out oversight activities on the role players in the conduct of an OCI does not question the general competence and independence of the judiciary in terms of the general judicial function but examines the specific function of adjudication of the court in the conduct of an OCI.

It is submitted that the specific competency requirements in this regard are relatively and adequately provided in RICA in terms of the various provisions which regulate the adjudicative function of the authority charged with the responsibility of issuing a direction in the conduct of an OCI, including the functions of the adjudicating authority in some instances which do not require a direction but still comply with some post-execution of interception conditions to access an online communication.[3820]

However, the offline implementation of the pre-and post-conduct of an OCI by the judiciary in overseeing the activities of role players in the conduct of an OCI is fraught with administrative and bureaucratic bottlenecks and incompetence to the extent of defeating the purpose of conducting an OCI.[3821]

It is further submitted that the judiciary is generally independent in the RSA. However, the same may not be said of few judicial officers —including the designated judge— overseeing the activities of role players in the conduct of an OCI because of some of the inadequacies in RICA and negative reports on the role played by the court which issued some unreasonable and unjustifiable direction, the inadequacies of which are as follows.[3822]

[3819] *AmaBhungane v Minister of Justice* supra 57; Para 6.15.3 of Chapter 6 of this study.
[3820] Para 6.2 of Chapter 6 of this study.
[3821] Para 6.11 of Chapter 6 of this study.
[3822] Para 6.15.3 of Chapter 6 of this study.

Firstly, as examined earlier, the application of section 205 of the CPA by a magistrate in conducting an OCI is dependent on the CPA, a general law, which in this study, is incongruous because the provision does not comply with the independent and specialised requirements in RICA which address the issues in the conduct of an OCI.[3823]

Secondly, the judicial authority of an incumbent magistrate in adjudicating on the conduct of an OCI may not be questioned in terms of the continuous or ongoing legal status of a magistrate whose judicial authority is not discharged or terminated until retirement or disengagement regarding the administration of the conduct of an OCI. However, the judicial authority and independence of a designated judge, who has 'inherent (sic) contentious function',[3824] is fraught with some lacuna. One such lacuna is that the appointment procedure of a designated judge who is a discharged or retired judge[3825] is compromised where the Minister of Justice who, without going through the cumbersome JSC appointment process, exercises the power to appoint a designated judge for a renewable term.[3826]

Where a judge retires or is discharged from the initial substantive appointment as a judge by the JSC, it is submitted that the judicial authority of a discharged or retired judge ceases, does not exist again or is forever discharged or terminated at the end of the judicial service tenure. Consequently, the judicial authority of a designated judge is not absolute in the adjudication of OCI because the authority is subject to the provisions of RICA which do not have an unlimited jurisdiction. The legal status of a designated judge is opposed to a judge who is on secondment and whose judicial authority is not interrupted while on secondment such as the Deputy Chief Justice Raymond Zondo, the chair of the Commission of Enquiry on the State of Capture.

It is further submitted that where a person, without full judicial authority —such as a designated judge— occupies a judicial position which is erroneously presumed to be equivalent to the status of a high court or judge, it creates a lacuna in the appropriation of full judicial authority to the adjudicating office or the officer in the conduct of an OCI. Therefore, the office or authority and officer adjudicating on the conduct of an OCI will, *de facto* and *de jure*, be regarded as a quasi-judicial independent office or authority if the provisions for the designated

[3823] Para 6.12 of Chapter 6 of this study.
[3824] *AmaBhungane v Minister of Justice* supra 62 and 65; Para 6.7 of Chapter 6 of this study.
[3825] Para 6.7 of Chapter 6 of this study. *AmaBhungane v Minister of Justice* supra 61 - 62 and 68.
[3826] Para 6.7 of Chapter 6 of this study. *AmaBhungane v Minister of Justice* supra 61 - 62 and 68.

judge will still be retained in RICA, though the judicial authority in the RSA is better than that of general and senior administrative officers who issue OCI direction in Australia, Canada and U.K.[3827]

It is further recommended that a panel of designated judges —who should not be retired or discharged judges—[3828] be interviewed and processed by the JSC and appointed by the President of the RSA for the usual undetermined tenure of office as a judicial officer for the enforcement of various provisions of the RICA and general judicial authority. This suggestion is opposed to the decision of the court in *AmaBhungane* that the Chief Justice nominates, and the Minister of Justice appoints designated judges –who are retired or discharged judges-[3829] for a non-renewable term of two years.[3830]

It is noted that the appointment of a number of judges is subject to the proposition for *Popoola QOCI* protocol, in which it is recommended that not too many judges are required in the conduct or operation of a *Popoola QOCI* protocol.[3831] This is because the adjudication of OCI applications does not seem to be a full-time function that requires too many judges to perform, as opposed to other or general subject matters, though not undermining the expertise required to carry out this task.[3832]

Allowing the Chief Justice and the Minister of Justice —in their independent capacities and not in their collective membership of the JSC— to be involved in the appointment process impliedly invite the duo to descend to the arena of usurping the powers of the JSC and executive powers of the President of the RSA, the usurpation of which blurs the principle of separation of powers between the executive and judiciary and other authorities.[3833] Furthermore,

---

[3827] *AmaBhungane v Minister of Justice* supra 63.
[3828] Para 6.7 of Chapter 6 of this study.
[3829] *AmaBhungane v Minister of Justice* supra 69.
[3830] *AmaBhungane v Minister of Justice* supra 64 - 67 and 70 and 71.
[3831] Paras 6.7 and 6.11 of Chapter 6 of this study.
[3832] See para 4.6 of Chapter 4 of this study on the need for every office holder involved in the conduct and management of the conduct of an OCI to go through a professional training course in this subject matter in view of the various arguable erroneous administrative, judicial, management, operational, oversight and supervisory decisions or functions by the relevant stakeholders in this study.
[3833] It is noted that the exercise of the power of the Chief Justice in the appointment of the Deputy Chief Justice to the Commission of Enquiry on State Capture is not the same as the appointment of a judge under RICA provisions because the status of the former is quasi-judicial while the latter is purely judicial, as this study maintains that the status of the office of a RICA judge should not be made lesser than other judges in the judiciary**,** see Staff Reporter 'Deputy Chief Justice Raymond Zondo to head commission of inquiry into state capture' https://mg.co.za/article/2018-01-09-deputy-chief-justice-raymond-zondo-to-head-state-capture-commission-of-inquiry (Date of use: 13 July 2019).

appointing a designated judge for a non-renewable term of two years seems to suggest that any judge can be hired and fired in the adjudication of the complex and delicate OCI application, in which this study has proven that most stakeholders do not have a good understanding of the nature and features of the subject matters of this study.[3834]

In the funding of the designated judge in overseeing the activities and affairs of the authorities or entities in the conduct of an OCI, the office of the designated judge does not have its budget but draws its budget from the Higher and Record Management Directorate of the Department of Justice.[3835] In the case of the other personnel who participate in the adjudication of an OCI such as High Court judges, regional magistrates and magistrates,[3836] it does seem that their funding is drawn from the general funding of the judiciary from the Parliamentary appropriation.

7.6.6.4 Accountability and oversight by and of the judiciary in overseeing the conduct of online criminal investigation by law enforcement agencies

While the general role of the judiciary in its oversight function on the stakeholders is reasonably adequate, however, the competence and independence of the judiciary in overseeing the activities of stakeholders in the conduct of an OCI is inadequate.[3837] Although the court in *AmaBhungane* has great confidence in a 'specialist designated judges',[3838] which this study contests because of the erroneous orders made by the courts (including both designated and general judges),[3839] however, the court did not put absolute trust in any 'inexperienced and unfamiliar' judicial officer in carrying out an oversight function in RICA.[3840]

It is incongruous of the JSCI of Parliament to request the court to explain the report on the conduct of an OCI submitted to the former by the latter based on the earlier submission in this regard.[3841] However, it is a confirmation (and not contradictory on the other hand, given the

[3834] Paras 4.6 and 6.7 of this study.
[3835] JSCI Reports 2016 at 55.
[3836] See section 59 of RICA for the judicial officers empowered to adjudicate on the conduct of an OCI; *AmaBhungane v Minister of Justice* supra 55.
[3837] *AmaBhungane v Minister of Justice* supra 106.
[3838] *AmaBhungane v Minister of Justice* supra 106.
[3839] Paras 3.5.5, 3.5.7.2, 4.6, 6.7 and 6.15.3 of this study.
[3840] *AmaBhungane v Minister of Justice* supra 106.
[3841] Section 3(h) of the ISOA. Para 7.6.5.3 of this chapter.

earlier submission made in this regard) that the office and officer of the designated judge issuing an OCI direction are accountable to the JSCI, which is a committee of Parliament.

Furthermore, it is trite to say that the courts generally have unlimited powers. However, it is submitted that the same way that the court holds that the other arms of government —i.e., executive and parliament— do not have unlimited powers, the judiciary should hold itself to similar responsibility or principle by not unnecessarily extending their powers beyond the jurisprudence of reasonable and justifiable adjudication and interpretation of the law.

7.7. INSTITUTIONALISING ALTERNATIVE DISPUTE MANAGEMENT MECHANISM IN ONLINE CRIMINAL INVESTIGATION ABUSE AND CONFLICT

Although there is a constitutional provision[3842] for what is erroneously and generally called ACR or ADR mechanism, however, RICA does not make provision for an ACR or ADR mechanism that redresses the infringements, conflicts or disputes that arise between the protection of the right to the SOC and the conduct of an OCI.[3843]

The consideration of an ACR or ADR enables an aggrieved party —through the prosecuting authorities— to enter into a negotiated agreement with an erring party in both criminal and civil proceedings in a bid to manage the grievance. One such agreement is for an erring party to enter into a plea bargain with the prosecuting authorities —the practice of which is judicially noticed- given that RICA criminalises some breaches of its provisions,[3844] thus, an ACR mechanism is an appropriate mechanism to apply in avoiding a prolonged, new and unnecessary conflict or dispute in the provisions of RICA.

This study submits that, from the practical point or view, no infringement, conflict or dispute is ever resolved to a *tabular rasa* ('clean slate') level that no trace of caution, malice, discord,

[3842] Section 41(3) of the Constitution.

[3843] For example, an investigative journalist whose right to the SOC was infringed by a private entity is planning to take legal action against the latter as well as where an aggrieved party —such as an investigative journalist— feels that the SAPS will not conduct an investigation against their own (see Right2Know 2018 at 16 and 22 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018), it is submitted that an ACM or ADM mechanism may be adopted.

[3844] Right2Know at 22 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018); Para 3.10 of Chapter 3 of this study.

hostility, enmity, resentment is left behind or penalty meted out after an intervention in the conflict or dispute between parties, thus the appropriate description of the mechanism propounded here is an ACM or ADM.

This is because a conflict or dispute that has escalated from its latency to the peak in an imaginary graphical representation can only be managed or remedied by reducing the tension or crisis in a downward slope but not beyond the zero levels of its latency in a graphical representation because there is still an element of 'I forgive, but I won't forget' in the mind of an individual or entity in every conflict or dispute that arises. In any case, there is no absolute remedy to a conflict or dispute that does not leave a scar behind in the mind of an individual or entity, no matter how insignificant the conflict or dispute is, thus, it is fallacious to conclude that a conflict or dispute is ever resolved but managed.

The choice to embark on an ACM or ADM may occur before or after the consideration of the admissibility of evidence occurs in a trial court.

7.8 JURISPRUDENCE OF ADMISSIBILITY OF EVIDENCE OBTAINED IN ONLINE CONSCRIPTION AND ONLINE CRIMINAL INVESTIGATION

7.8.1 Introduction

The stage at which evidence is considered for admission occurs where an aggrieved party in a complaint against the breach of the right to the SOC or the conduct of an OCI is unable to manage the infringement via the process of an ACM or ADM,[3845] thus the path of prosecution follows, which ultimately and mainly requires the procedural admissibility of evidence at some point.

The jurisprudence of the admissibility of online evidence in a criminal proceeding is set out in section 35(5) of the Constitution which states that evidence that is unlawfully obtained in contravention of the Bill of Rights, including the emerging right to the SOC, is inadmissible 'if the admission of that evidence would', in the fundamentally competing interests 'render the

[3845] Para 7.7 of this chapter.

trial unfair or otherwise be detrimental to the administration of justice'.[3846] Essentially, the respect for the right to the SOC is 'instrumental to a fair trial.'[3847] From a foreign jurisdiction, Koops and Goodwin opine that where data is unlawfully obtained, the evidence does not outrightly have to be inadmissible, the main interest to consider is whether the evidence further infringes on the right of a victim and not that of a suspect.[3848]

In RICA, provision is only made for the use of online communication for civil and criminal proceedings without making provision for any specific rule on the admissibility of online evidence.[3849]

In the RSA, the interpretation of section 35(5) of the Constitutional provision has severally come before the lower courts with no clarity on the exact interpretation of section 35(5). However, the Constitutional Court has generally not made a pronouncement on this provision,[3850] let alone in the evidence obtained in online communication. The non-pronouncement by the Constitutional Court is not limited to the RSA but other jurisdictions. According to Koops and Goodwin, there is 'insufficient harmonisation of core' cybercrime issues relating to the admissibility of electronic evidence.[3851]

It is opined that the admissibility of online evidence is regulated by the same provision which regulates the admissibility of traditional evidence, thus no special rules of evidence govern electronic evidence.[3852] Some scholars and commentators believe that the South African law on the admissibility of electronic evidence is inadequate because of lack of guidelines on the procedure regulating the 'collection, storage and presentation of electronic evidence' required

[3846] Van der Merwe S E 'Exclusion of relevant evidence: Unconstitutionally obtained evidence' in Schwikkard P J and Van der Merwe S E *Principles of evidence* 4th ed. (2016) 198-199 and 201 -202 (Van der Merwe *Evidence*).
[3847] *AmaBhungane v Minister of Justice* supra 114.
[3848] Koops and Goodwin 75 www.tilburguniversity.edu/tilt (Date of use: 14 December 2016).
[3849] Sections 47 and 48 of RICA.
[3850] Van der Merwe *Evidence* 198-199.
[3851] Koops and Goodwin at 80 www.tilburguniversity.edu/tilt (Date of use: 14 December 2016).
[3852] Watney M 'Admissibility of electronic evidence in criminal proceedings: An Outline of the South African legal position' 2009 (1) *Journal of Information, Law & Technology* (*JILT*) 1 (Watney 2009 (1) *Journal of Information, Law & Technology* (*JILT*) 1).

for criminal proceedings,[3853] the guidelines of which are required for the admissibility of online evidence.[3854]

Nevertheless, there are two opposing schools of thought on the exclusion of unlawfully obtained evidence. The first school of thought believes that an unlawfully obtained evidence should not be excluded in the admissibility of evidence while the second school of thought says that an unlawfully obtained evidence should be excluded from the admissibility of evidence.

On the one hand, firstly, the exclusion rule regrettably enables the exclusion of a probative value of evidence. An exclusion rule prevents an enquiry, frustrates the effective work and excludes the volume and type of evidence obtained by an investigator in an era of increasing crime and sets the guilty free because the evidence was unlawfully obtained[3855] in the conduct of an OCI of serious offences. Therefore, any evidence unlawfully obtained should not be excluded under the admissibility of evidence principle.

Secondly, this school of thought also believes that should there be an infringement of a Bill of Right in an unlawfully obtained evidence from a perpetrator, suspect or accused person; other remedies are adequate to redress the infringement instead of excluding an unlawfully obtained evidence[3856] in the conduct of an OCI. Therefore, any evidence unlawfully obtained should not be excluded under the admissibility of evidence principle.

Thirdly, the fact that the services rendered by LEAs are social services, which are not meant for personal benefits, therefore, the society should, as a matter of necessity, tolerate the unlawful operation of LEAs in the public interests[3857] in the conduct of an OCI. This is because the criminal suspect did not refrain in causing harm, injury or damage in the commission of a crime against a victim,[3858] therefore, the court should not be reluctant to admit an unlawfully obtained evidence in the conduct of an OCI.

[3853] Watney 2009 (1) *Journal of Information, Law & Technology* (*JILT*) 1.
[3854] Section 63(3) (a)-(d) of the CCB of B-2015 emphasises on the manner and integrity of generation, storage and communication of data, manner of identification of the originator and receiver of data and other relevant factors.
[3855] Van der Merwe *Evidence* 202-203.
[3856] Van der Merwe *Evidence* 203.
[3857] Van der Merwe *Evidence* 203.
[3858] Van der Merwe *Evidence* 202-203.

Fourthly, an investigator may maliciously, and predictively, pre-emptorily or in advance determine what evidence would be admissible[3859] by intentionally and unlawfully frustrating the conduct of an OCI, so that such an unlawfully obtained evidence would regrettably be foreseeably and ultimately be excluded in the conduct of an OCI, which should not be encouraged.

Fifthly and arguably, should there be an exclusion of unlawfully obtained evidence in the conduct of an OCI, the court will impliedly and regrettably be condoning criminality because the evidence that should be admissible will be excluded.[3860]

Lastly, an exclusion rule does not allow the application of proportionality principle because the rule prohibits the court from considering the seriousness and nature of the commission of crime side by side the gravity and nature of the infringement[3861] in the conduct of an OCI.[3862]

Therefore, an unlawfully obtained evidence in the conduct of an OCI should not be excluded as follows.

On the other hand, firstly, an exclusion rule seeks to promote due process in the application of substantive and procedural law compliance[3863] in RICA and other law, thus, it matters how evidence is obtained to promote legality, judicial integrity as well as enable the court exercise judicial discretion on the admissibility of an unlawfully obtained evidence[3864] in the conduct of an OCI. Therefore, an unlawfully obtained evidence should be excluded in the admissibility of evidence.

Secondly, the exclusion rule favourably takes away the rigid law that the end result of an investigation justifies the means of obtaining evidence, which means that the court will not condone unlawful evidence obtained by LEAs[3865] in the conduct of an OCI.

[3859] Van der Merwe *Evidence* 203.
[3860] Van der Merwe *Evidence* 204.
[3861] Van der Merwe *Evidence* 204.
[3862] Para 7.8.3 of this chapter.
[3863] Van der Merwe *Evidence* 199.
[3864] Van der Merwe *Evidence* 200.
[3865] Van der Merwe *Evidence* 202-203.

Thirdly and finally, the examination of the concept of online conscription[3866] is 'to be balanced against the principle that people should not be compelled to condemn themselves out of their own mouths'[3867] in online communication, therefore, unlawfully obtained evidence in online communication is excluded in the admissibility of evidence obtained in the conduct of an OCI.

Any evidence considered for admissibility must not only meet the specific admissibility requirements of reasonableness and justifiability in section 35(5) of the Constitution[3868] but must comply with the general requirements in section 36(1) of the Constitution, both of which simultaneously operate to guide the discretion of the court in the limitation of the right[3869] to the SOC.

As authorities formulated flexible guidelines on the admissibility of unlawfully obtained evidence in the offline world,[3870] this rubric, aside from the specific permissible instances of online conscription,[3871] attempts to specifically consider the guidelines regulating the admissibility of unlawfully obtained online evidence in some instances in online conscription[3872] and online criminal investigation as voidable, void, and inadmissible pieces of evidence in the context of this study. These guidelines seek to reconcile the positions of the above two schools of thought on the application of section 35(5) of the Constitution in the unlawful conduct of an OCI in the RSA.

7.8.2 Admissibility of evidence in online conscription and online criminal investigation as an exception to the inadmissibility of unlawfully obtained online evidence

The core principle of section 35(5) of the Constitution in the offline world states that unlawfully obtained evidence is inadmissible despite its relevance and regardless of its otherwise likelihood of admissibility.[3873]

[3866] Para 2.3.3 of Chapter 2 of this study.
[3867] *Ferreira v Levin* supra 258.
[3868] *State v Miller* supra 65.
[3869] Van der Merwe *Evidence* 239.
[3870] Van der Merwe *Evidence* 200.
[3871] Para 2.3.3.7 of Chapter 2 of this study.
[3872] Para 2.3 of Chapter 2 of this study.
[3873] Section 35(5) of the Constitution; *Thint* supra 142 and 155; *Nel* supra 3; *State v Pillay* supra 430B-F,431G-432A, 445B-J and 446A-447B-J; *State v Naidoo* supra 483 G-H; Van der Merwe *Evidence* 199; Hubbard, Brauti and Fenton *Wiretapping* 10-26.10., 10-26.11 and 10-27 to 10-39.

However, it is submitted that should the core principle in section 35(5) be applied to the unlawful evidence obtained from online conscription, given that conscripted offline evidence is generally regarded as an unlawfully obtained evidence,[3874] it means that no evidence obtained in an online communication will ever be admissible. The inadmissibility of online evidence in this regard consequently grants an unlimited licence to the use of online communication devices for criminal purposes because evidence derived therefrom will be inadmissible.

Consequently, it is therefore submitted that the inadmissibility of online conscription in some instances will render a trial unfair or otherwise detrimental to the administration of justice in section 35(5) due to the inability of considering the merit of the evidence in each case,[3875] thus the admissibility principle is informed by the necessity to rely on the evidence obtained in online conscription in such reasonable and justifiable instances.[3876]

In some foreign jurisdictions, an unlawfully obtained evidence may or may not be reasonably and justifiably admissible. In Germany, it is reasonable and justifiable for evidence obtained in an undercover investigation to be admissible where other means of investigating serious criminal offences would offer no prospect of success or where such investigative method is much more difficult.[3877]

Furthermore, in Estonia, due to the time required to examine the large quantity of digital data, it is submitted that the storage of such data for future inspection may not be reasonable and justifiable[3878] without applying the proportionality principle on the duration of storage of data *vis-a-vis* the seriousness of an offence.[3879]

Nevertheless, in the U.S., it is unreasonable and unjustifiable where the facts used in determining the reasonable ground to conduct an OCI was *ab initio* obtained in online communication, whereas such information should have been obtained in the offline world as

[3874] Para 2.3, more particularly para 2.3.3.7 of Chapter 2 of this study.
[3875] *State v Pillay* supra 421 B-H422 A, 428 B-C & G-H, 430 B-D & H-431 B-J, 432 F-433 A-J, 434 G-H, 435 G-J, 436A and 445B-J, 446A-J - 447B-J; *State v Terrence Brown* supra 16, 17, 18 and 19; Section 15(3)(d) of the ECTA and section 63(3)(d) of the CCB B-2015; Section 51(7) of RICA; *State v Naidoo* supra 530B-D.
[3876] *State v Naidoo* supra 520H.
[3877] Section 110a (1)(4) of Criminal Code of Procedure of Germany.
[3878] Osula A *Remote search and seizure of extraterritorial data* 55.
[3879] Paras 6.3 and 6.4 of Chapter 6 of this study.

the basis to establish the relevant reasonable ground standard to conduct an OCI save where the commission of an offence occurred with the use of an online communication device which would have warranted the initial investigation commences in an online communication.[3880] Therefore, the evidence gathered would amount to 'the fruit of a poisonous tree', be unreasonable, unjustifiable and inadmissible.[3881]

At the international level, reasonable and justifiable instances[3882] mean that relevant online evidence lawfully obtained by an authorised person or entity —including an Online Communication Service Providers and the Interception Centre— in the conduct of an OCI through online conscription is admissible, in which a notice and copy of the recording must thereafter be given by LEA to the target.[3883]

7.8.3 Application of the proportionality principle in the admissibility of unlawfully obtained evidence in online conscription and online criminal investigation

One of the arguments by the school of thought against the exclusion of unlawfully obtained evidence is that an exclusion rule does not allow the application of the proportionality principle.[3884] This is because the exclusion of evidence prevents the court from having before it the consideration of two key factors which are the seriousness and nature of the offence, on the one hand, and the nature and gravity of the infringement[3885] of the right to the SOC in the conduct of an OCI, one the other hand, as a yardstick in the admissibility of unlawfully obtained evidence.

It is therefore submitted that given the consideration of these two factors, which relate to the two conflicting sides in this study,[3886] the admissibility of an unlawfully obtained online

[3880] Sloan *Law of privacy in a technological society* 58-59;
[3881] Sloan *Law of privacy in a technological society* 58-59; Paras 6.4.9 and 6.11 of Chapter 6 of this study.
[3882] *State v Naidoo* supra 520H.
[3883] Section 36 of ITU 'Interception policy & legislative text' (2012).
[3884] Van der Merwe *Evidence* 204.
[3885] Van der Merwe *Evidence* 204; Chapter 2 of this study, more particularly paras 2.3.3 and 2.8; Chapter 3 of this study, more particularly paras 3.4.4, 3.4.5, 3.5.7, 3.6 and 3.8; Chapter 5 of this study; Paras 6.3.3.1- 6.3.3.6, 6.5 and 6.6 of Chapter 6 of this study.
[3886] The conflicting sides are the protection of the right to the SOC and the conduct of an OCI; Chapter 2 of this study, more particularly paras 2.3.3 and 2.8; Chapter 3 of this study, more particularly paras 3.4.4, 3.4.5, 3.5.7, 3.6 and 3.8; Chapter 5 of this study; Paras 6.3.3.1- 6.3.3.6, 6.5 and 6.6 of Chapter 6 of this study.

evidence will proportionately[3887] consider the nature and seriousness of an offence factor under four criteria[3888] and the nature and level of infringement or intrusion into the sanctum of the SOC by virtue of online conscription and conduct of an OCI of content and non-content data.[3889]

For example, using the proportionality principle in the seriousness and nature of an offence, based on the fact that LEAs should not use an intrusive investigative method for a trivial offence or better still, 'one should not shoot a sparrow with a canon',[3890] it is submitted that where the effect of the commission of a serious offence is absolutely irreversible[3891] because such an offence is not a trivial offence, the court must consider the admissibility of an unlawfully obtained online evidence in online conscription and in an OCI.

Other proportionality criteria for the admissibility of evidence obtained from online conscription include the importance of the evidence gathered, the good or bad faith of the law enforcement agency or officer, inadvertent error, mere technical error, the degree of urgency to prevent the loss of evidence in the investigation, obtaining the evidence without a violation of a right and other circumstances relating to the admissibility of the unlawfully obtained evidence, amongst other reasonable and justifiable criteria, though with some exceptions.[3892]

7.8.4 Admissibility of voidable evidence

7.8.4.1 Introduction

Drawing on the principle of voidability in the law of contract, it is submitted that voidable online evidence is evidence that is unlawfully obtained under compelling, exceptional or exigent circumstances but yet still constitutes a lawfully obtained online evidence upon the fulfilment by LEAs of some conditions of admissibility of such evidence.

[3887] In addition to other forms of proportionality test identified in chapters 2-6, see mainly para 5.4 of Chapter 5 of this study.
[3888] Paragraphs 6.3.3.1- 6.3.3.6, 6.5 and 6.6 of Chapter 6 of this study.
[3889] Chapter 2 of this study, more particularly paras 2.3.3 and 2.8; Chapter 3 of this study, more particularly paras 3.4.4, 3.4.5, 3.5.7, 3.6 and 3.8; Chapter 5 of this study.
[3890] Van der Merwe *Evidence* 204; Sections 42- 43, 49-51 and 54 of RICA.
[3891] The four criteria for classifying serious offences are the bailability, penology, irreversibility and economic gain or harm criteria, see para 6.3.3 of Chapter 6 of this study. See para 6.3.3.4 of Chapter 6 of this study for the criterion on irreversibility of the effect of the commission of an offence. *State v Naidoo* supra 526D-E.
[3892] *State v Naidoo* supra 526D-E and 530 B-D.

It is submitted that where LEAs partially comply with the key requirements in RICA before unlawfully obtaining on online evidence, it is posited that the Inclusive-Exclusive Discretionary Rule under section 35(5) of the Constitution would apply in accordance with the proportionality principle between the seriousness of the offence and the level of an intrusion into online communication. The following, amongst others, illustrates the admissibility of voidable online evidence.

7.8.4.2 Evidence obtained in the technical maintenance of online communications and interception devices

Where there is an '*inadvertent*' or '*mere technical*' infringement of the right to the SOC through an OCI which has 'little consequence' or does not go to the root of the right to the SOC in the consideration of the fairness of a trial or administration of justice,[3893] it is advocated that the inclusionary principle is likely to be applied to the unlawfully obtained online evidence[3894] —provided it is not considered as windfall evidence— in accordance with the proportionality principle between the seriousness of an offence and the level of intrusion into online communication.

Conversely and impliedly, where there is an '*inadvertent*' or '*mere technical*' infringement of an OCI which has a significant consequence, it is submitted that such online evidence will be excluded. This is because such evidence will constitute a 'windfall evidence', which is generally not an acceptable means of obtaining online evidence, save where the evidence relates to the effect of the commission of an offence that is absolutely irreversible,[3895] in which case, such unlawfully obtained evidence would be equitably and proportionately admissible.
Finally, in any of the instances in this rubric, is it submitted that technical maintenance reason should not be used —whether fraudulently or maliciously— as a guise to conduct an OCI where the required reasonable ground standard is not met, otherwise, obtaining unlawful evidence under this rubric would constitute an offence in RICA.[3896]

[3893] Dissenting opinion of Scott JA in *State v Pillay* supra 448 D–F and *State v Naidoo* supra 483 D–E; Van der Merwe *Evidence* 269; Section 210 of the CPA; *Jwara v State* supra 13.
[3894] Van der Merwe *Evidence* 269; *Jwara v State* supra 13.
[3895] Para 6.3.3.4 of Chapter 6 of this study.
[3896] Section 51 of RICA.

7.8.4.3 Evidence obtained by special and emergency law enforcement officers

Given the risky and delicate nature of the role of Special and Emergency LEOs in the conduct of an OCI which is lawful as propounded in this study,[3897] it is submitted that though the evidence obtained by Special and Emergency LEOs are unlawful, the court will declare it voidable so that it is considered for admissibility upon compliance with some conditions. This is because the Special and Emergency LEOs are in a precarious situation that innocently and spontaneously requires the conduct of an OCI by LEOs without an OCI direction, therefore, the essence of conducting an OCI under this rubric will be useless should the evidence obtained be declared inadmissible after fulfilling some requirements stipulated by law.

7.8.4.4 Evidence obtained in robotic online criminal investigation

Because technological development is unstoppable and that 'computers can't do all the work by themselves, but they can expand the capabilities of humans exponentially'[3898] which constitute lawful acts, human beings (courts) are able to consider the evidence obtained in a ROCI system which is regarded as an unlawfully obtained evidence. This is because the automatic nature of the conduct of a ROCI does not enable human intervention —such as the issuance of a direction by a court— before the conduct of a ROCI. Therefore, the court is obliged to, at the end of the conduct of a ROCI favourably consider the admissibility of the unlawfully obtained online evidence upon fulfilling some conditions, one of which is the level of seriousness and complex nature of an offence that a ROCI picks up to investigate.[3899]

7.8.5 Admissibility of void evidence

7.8.5.1 Introduction

Drawing on the general understanding of the principle of voidness in the law of contract, it is submitted that —as opposed to the admissible and voidable evidence— a void online evidence is online evidence that is unlawfully obtained and consequently inadmissible at all times or almost impossible to admit such evidence. This is because the gathering of such online

[3897] Para 2.11.3 of Chapter 2 of this study.
[3898] Vlahos *Surveillance society: New high-tech cameras are watching you* 98.
[3899] Para 7.8.3 of this chapter.

evidence is automatically and basically a conscripted and self-incriminating evidence[3900] and fundamentally contravenes the basic rules of procedure in the conduct of an OCI in RICA and other law, the evidence of which is unequivocally appropriated as 'windfall evidence' or is regarded as a 'fruit from the poisonous tree' gathered by LEAs, either of which is inadmissible.[3901]

Void evidence is inadmissible also because a less restrictive means[3902] than the use of an OCI can be comparatively, greatly, routinely and substantially used to conduct an investigation, but it is not used, thus the evidence obtained becomes void. It consequently follows therefore that since no LEA or LEO is compelled at gun point or inevitably compelled to use an OCI, as the usage of an OCI is seemingly becoming easily or more fashionable for LEAs or LEOs to adopt its usage before even considering other methods of investigation, any unlawfully obtained evidence becomes void and inadmissible.

However, the only situation where there may be no alternative method of investigation is where there is a cybercrime commission in which the facts are required to be gathered *ab intio* at no other place than in the online communication, the evidence of which constitutes the relevant reasonable ground for the conduct of a further OCI.

It also follows therefore that a *fait accompli* principle[3903] does not apply to compel the admissibility of such unlawfully obtained online evidence simply because of the claim that the online evidence is already obtained, whereas the online evidence was unlawfully obtained which becomes void and inadmissible. Accordingly, it is incongruous for LEAs to believe that 'the end justifies the means' in terms of unlawfully obtaining online evidence in the complex, delicate and secretive nature of an online communication,[3904] the process of which cannot

[3900] Para 2.3.3 of Chapter 2 of this study; Van der Merwe *Evidence* 221 and 225.

[3901] In the offline world, 'the extent and flagrancy' of the breach of a statutory law by the SAPS remains a fundamental issue to be considered by the court in the exercise of its discretion, Van der Merwe *Evidence* 205-207 and 221, therefore, an intentional refusal –including obviously negligent conduct- to comply with the provisions of RICA will render such evidence inadmissible.

[3902] *AmaBhungane v Minister of Justice* supra 90.

[3903] *Fait accompli* principle is slightly similar to the principle of equity which states that equity regards as done what ought to be done. While there is no duty of care for the person executing a task or an offeror, who eventually seizes the opportunity that the offeree is too busy, decides to supply goods or render services to the offeree without the consent of the offeree, which at the end of the day, the offeree is compelled to pay for the goods or services. In the case of the principle of equity, there is a duty of care by the offeror to the offeree to carry out a function or task, Dawson R *Roger Dawson's secrets of power negotiating* (1995) 172 - 173.

[3904] Chapter 3 of this study, more particularly paras 3.4.4, 3.4.5, 3.5.7 and 3.8.

easily be by-passed or mistakenly conducted, condoned and be considered for admissibility. This is unlike the unlawfully obtained offline evidence which does not have the same cumbersome or rigid level of obtaining evidence unlawfully, thus susceptible to easy compromise of the process and the evidence and such offline evidence may be considered for admissibility.

An evidence can also be void where LEAs collect an information, which is, later used for entirely different purposes along the line.[3905] Evidence gathered which is not relevant to the purpose for which an OCI was conducted must be deleted immediately, otherwise the failure or refusal to delete it constitutes an offence, which arguably and impliedly means that such irrelevant evidence is inadmissible.[3906]

A distinction is made between offline and online windfall evidence. It is submitted that in the offline world, where windfall evidence[3907] is obtained, it may still be used in criminal proceedings even if obtained unlawfully.[3908] However, based on the various provisions of the domestic and international law in the online world, an OCI is specifically used for the investigation of serious offences only. In art 28(2)(b) of CoE CoCC, in which the RSA is a signatory to; access to data in the MLA Treaty cannot be used for other investigative purposes other than those stated in the request.[3909] Also, the United Nations prohibits the use of any evidence for prosecutorial purposes in cases other than serious offences.[3910] Therefore, any online windfall evidence obtained in this regard that constitutes a non-serious offence would be unlawfully obtained and as such, would fall away and be declared inadmissible.

In further making a distinction on the admissibility of void evidence between offline and online evidence, the imposition of criminal punishment in consequence of a breach of the right to the SOC by a LEA or a person and the general civil remedy in consequence of a breach of offline privacy makes a clear distinction. This distinction compels a conclusion on the greater seriousness of the unlawfulness of obtaining online evidence than the unlawfulness of

[3905] Vlahos *Surveillance society: New high-tech cameras are watching you* 100.
[3906] Section 23(1), (2) & (4) and 24 of ITU 'Interception policy & legislative text' (2012).
[3907] Van der Merwe *Evidence* at 205-207, 209-210 and 215 - 216.
[3908] Section 35 (5) of the Constitution.
[3909] Same applies in art 18(19) of TOCC. It is however unequitable for a requesting State Party to notify in advance or without delay the requested State party where a windfall evidence is exculpatory of an accused whereas, requesting State party does not follows this process where incriminating windfall evidence is found.
[3910] Art 16 (12)(a) of the UNODC 'Model legislative provisions against organised crime 2012.

obtaining offline evidence. Consequently, there is more likelihood of the inadmissibility of an unlawfully obtained online evidence than an unlawfully obtained offline evidence.[3911]

Jurisprudentially is it fallacious to criminalise acts of infringements in RICA by putting a LEO —who unlawfully obtains online evidence— in jail or by carrying out other criminal punishments and at the same time allow the LEAs enjoy the benefits from the fruit of the poisonous tree by admitting such unlawfully obtained online evidence in the interest of fair trial or the administration of justice[3912] in favour of the prosecuting authority or entity. Thus, the voidness or inadmissibility of an unlawfully obtained online evidence is more certain, effective, meaningful, implementable and practicable than an unlawfully obtained offline evidence.

This distinction, once again, raises the morality, reasonableness and justifiability of the application of the indemnity principle which the court applies in condoning the act of omission -negligence- or commission in RICA by a LEO or an entity in the exercise of a duty to conduct an OCI in which the court admits evidence where it was obvious that the LEO was not truthful in furnishing evidence.[3913]

Evidence can also be void in terms of compliance with the time of deletion or destruction and retention of data obtained. Given the fact that irrelevant information[3914] is required to be destroyed not later than 6 months of gathering information through an OCI in international law, and not later than 6 months of the expiry of an OCI warrant,[3915] the retention of an unlawfully obtained online evidence arguably questions the validity of the admissibility of such online windfall evidence after the stipulated duration. This impliedly means that the retention of irrelevant information will constitute an unlawfully obtained online evidence if it later becomes relevant in terms of the duration of preservation of the evidence, save where the evidence cannot be practicably destroyed as soon as possible.

[3911] Paras 7.8.5.2–7.8.5.7 of this chapter.
[3912] Van der Merwe *Evidence* 198-199 and 201 -202.
[3913] Section 51(7) of RICA; Section 204 of the CPA; Para 3.5.7.11 of Chapter 3 of this study; *State v Naidoo* supra 521 B-E.
[3914] Section 210 of the CPA.
[3915] Art 16(13) of UNODC 'Model legislative provisions against organised crime 2012.

Although the provisions of the Extradition Act support the application of windfall evidence,[3916] however, the Court has held that the principle of speciality be 'respected'[3917] which requires making windfall evidence inadmissible under the principle of speciality. Essentially, this means that an extradited individual cannot be prosecuted for an offence other than the one for which he was extradited,[3918] otherwise, the evidence obtained will be void. Arguably, this principle may generally be applied to an OCI such that any online evidence unlawfully obtained from an OCI —which is online windfall evidence— which is not related to the offence for which it was intercepted cannot be used for prosecution purposes because it is void evidence in the following circumstances, amongst others.

7.8.5.2 Evidence unlawfully obtained in an innocent online criminal investigation

In an unlawful OCI direction issued by a judge who received false information[3919] about two investigative journalists who were described as ATM bombers by LEOs, the CI-SAPS mistakenly included the mobile cellular telephone number of someone —who in different government administrations doubled as a National Commissioner of Police and Minister of Police— as part of the online communications in which an OCI was conducted in this regard.[3920] It is submitted that such online evidence is not admissible because, given the comprehensive or stringent procedural requirements of conducting an OCI, it is very unlikely that such an error could easily occur in the manner herein.

It is noted that one of the first compulsory steps taken in the conduct of an OCI is the invocation of section 39(3)(a)-(c) and (4) of RICA which empowers the LEAs to prepare, verify and access the identity of the owner of a subscriber number which would have formally revealed the true identity of the purported target even if the number was registered in a corporate name[3921] and prevented the conduct of an OCI on a wrong target.[3922]

[3916] Section 23(c) and 19 of the Extradition Act 67 of 1962.
[3917] *S v Stokes* 2008 (5) SA 644 (SCA) at para 10.
[3918] J Dugard et al 'Extradition'' 220.
[3919] *AmaBhungane v Minister of Justice* supra 20.
[3920] Right2Know 'Spooked- Surveillance of Journalists in SA' at 13-14 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018 (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018).
[3921] Section 39(1)(a) and (b) of RICA.
[3922] Section 39(3) (a) -(c) and (4) of RICA.

The conduct of an OCI is more stringent, unlike some offline investigations that are conducted spontaneously or in an unpredictable situation, which may not be possible or easy to obtain a warrant of search and seizure at that moment,[3923] for example, where the LEAs are present at the occurrence of the crime which does not require a warrant to conduct a search. Moreover, even where a warrant is required to be executed in a house, it is unlikely that a LEA would verify the identity of the ownership of a house which may or may not be owned by the target of the investigation. This is unlike the verification of the subscriber number which is personalised, though equity provision in RICA now recognises the right of an equitable user of a mobile cellular telephone.[3924]

7.8.5.3 Evidence obtained in contravention of some provisions of RICA

One of the instances where there is a contravention of the provisions of RICA is where LEAs or LEOs are required to seek and obtain an OCI direction before an interception but such LEAs or LEOs outrightly fail or refuse to apply for an OCI direction before conducting an OCI.[3925] It is submitted that the exclusionary rule applies[3926] in this instance, save in circumstances stipulated by RICA[3927] and in instances in an OCI conducted by Artificial and Special LEOs which or who do not require a prior OCI direction.[3928] However, the evidence obtained by Artificial and Special LEOs is admissible under section 35(5) of the Constitution in accordance with the proportionality principle between the seriousness of the offence and level of intrusion into online communication.

[3923] Chapter 2 of the CPA.
[3924] See the definition of family member in section 1 of RICA.
[3925] OCI does not generally operate as the offline investigation operates in section 22(b)(i) and (ii) of the CPA, therefore when applying section 22(b)(i) and (ii) of the CPA, its provision and that of section 22 of RICA cannot be used to contravene section 16 of RICA which regulates online communication as opposed to section 22(b)(i) and (ii) of CPA and section 22 of RICA both of which regulate offline communication.
[3926] Van der Merwe *Evidence* 269.
[3927] Para 6.2.2 - 6.2.6 of Chapter 6 of this study.
[3928] Paras 2.11.3, 2.11.4 and 6.4.9 of this study.

7.8.5.4 Evidence obtained by furnishing false statement in an application for an online criminal investigation

In the Supreme Court of Appeal case of *Jwara v State*[3929] where a LEO obtains an OCI direction *via* false information,[3930] the validity of such an OCI direction will not stand, therefore, it is submitted that the online evidence obtained therefrom is inadmissible as it was similarly held in *State v Pillay*.[3931] In a similar vein, it is further submitted that where CI-SAPS fabricated lies to the designated judge to obtain an OCI direction against two investigative journalists who were described as ATM bombers which resulted in the OCI direction that their real-time and archived mobile cellular telephone communications relating to phone call, SMS and metadata facilities be tapped,[3932] such online evidence obtained therefrom is inadmissible.[3933]

7.8.5.5 Evidence obtained while acting contrary to the authority of online criminal investigation direction

Where there is a failure on the part of LEAs or LEOs to comply with the direction of the court on a live monitoring order, the online evidence obtained is challenged as inadmissible evidence under the Canadian law;[3934] thus arguably applies in the RSA.

7.8.5.6 Evidence obtained by forging online criminal investigation direction

It is submitted that online evidence obtained by forging an OCI direction is inadmissible because there is no mandate whatsoever that is obtained from the adjudicating authority to conduct an OCI.

[3929] *Jwara v State* supra 13.
[3930] *AmaBhungane v Minister of Justice* supra 20.
[3931] *State v Pillay & others* 2004 (2) SACR 410 (SCA); *S v Hammers & ors* 1994 (2) SACR 496 (C); Van der Merwe *Evidence* 222.
[3932] *AmaBhungane v Minister of Justice* supra 20; Right2Know 'Spooked- Surveillance of Journalists in SA' at 12-13 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018) (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use:27 November 2018).
[3933] See also para 6.4.3 of Chapter 6 of this study where this study submits that the evidence falsely obtained in the principle of 'opportunistic online access and convertible intrusive standard of proof' is inadmissible.
[3934] See Hubbard, Brauti and Fenton *Wiretapping* at para 4.4.1 at page 4-43.

7.8.5.7 Evidence obtained after online criminal investigation direction is revoked

It is submitted that if an oral direction issued in terms of section 23(3) of RICA is cancelled in terms of section 25(2) of RICA, the online evidence obtained after the LEO fails to submit a further written application to the designated judge within forty-eight hours of granting an oral OCI direction will be inadmissible in criminal or civil proceedings. However, such evidence may be admissible where 'the court believes that the admission of such evidence would not render the trial unfair or otherwise be detrimental to the administration of justice.'[3935]

7.9 CONCLUSION

In conclusion, the following issues are addressed in this chapter.

Firstly, RICA does not, under the principle of *delegatus potest non delegare*, make provision for the regulation or adequate regulation of the delegation or further delegation of the powers of LEOs in the management of the conduct of an OCI because it is not expected that every Tom, Dick and Harry in the LEAs will be allowed to conduct an OCI in the delicate and complex right to the SOC.[3936]

Secondly, RICA makes provision for the role and management of the affairs and activities of executing authorities and entities in the conduct of an OCI including Online Communication Service Providers such as the Decryption Keyholder, the Cryptographer, the Authentications Service Provider, the Cyber Inspector, the Telecommunication Service Provider and the Interception Centre. However, the provisions are inadequate to strike a balance in the conflict between the protection of the right to the SOC and the conduct of an OCI in terms of the appointment of specialised staff, performance of functions, exercise of powers, conduct of operations and sources of funding and execution of oversight role of and by the stakeholders in the conduct of an OCI.[3937]

[3935] Section 13, 36 and 37 of ITU 'Interception Policy & Legislative Text' (2012).
[3936] Para 7.2 of this chapter.
[3937] Paras 7.3.1 - 7.3.3 and 7.3.5- 7.3.6 of this chapter.

Worse still, one of the executing authorities, the NCC, which operates under the control and management of the SSA, is not regulated by any law, yet conducts an unfettered domestic and international OCI without a direction, which is a grievous breach of the right to the SOC.[3938]

Thirdly, RICA makes provision that the LEAs submit reports to the designated judge in a proportionate manner, which is a fundamental principle in this study, however RICA does not regulate how the judge exercises this discretion in terms of the proportionality of the frequency of submission of report and the seriousness and occurrence of an offence.[3939]

Fourthly, RICA and RICA Directives 2005 make provision for the management of data in an OCI which cover several areas of data management. However, some provisions are reasonably inadequate such as the management of copying, duplicating, routing, provisioning, storage and deletion of data, while some provisions are grossly inadequate such as the management of sealing, sorting, retrieving and examination of data in the pre-and post-execution of an OCI.[3940]

Fifthly, amongst the authorities and entities —namely non-governmental entities, OIC, OIGI, JSCI of Parliament and judiciary— that oversee the LEAs and executing and interception entities in the conduct of an OCI; the JSCI and the judiciary are the most regulated authorities which are relatively institutionalised competent, independent and accountable, though some remarkable inadequacies are equally identified in this study.[3941]

Sixthly, although the Constitution makes provision for an ACR or ADR mechanism, however, RICA does not make provision for an ACR or ADR mechanism and as propounded in this study; an ACM or ADM mechanism to redress the conflict or dispute in the protection of the right to the SOC and the conduct of an OCI before the judicial process takes over.[3942]

The striking difference between an ACR or ADR and ACM or ADM is that there is no conflict or dispute that is ever resolved. Rather a conflict or dispute is only managed because there is still an element or iota —no matter how insignificant— of the effect of a conflict or dispute

[3938] Para 7.3.4 of this chapter.
[3939] Para 7.4 of this chapter.
[3940] Para 7.5 of this chapter.
[3941] Para 7.6 of this chapter.
[3942] Para 7.7 of this chapter.

left behind after negotiation has taken place between the aggrieved parties. Similarly, therefore, this study holds that a breach of the right to the SOC can never be resolved but managed because once a data is compromised by virtue of the unlawful conduct of an OCI, the data is unquantifiable and irreparable even where the LEAs or LEOs delete the data as recommended in this study.[3943]

Finally, although some pieces of evidence are unlawfully obtained through some sources such as the concept of online conscription,[3944] the conduct of an OCI and other forms of breaches of the right to the SOC; however, this study reveals that unlawfully obtained evidence can be considered under the admissibility principle as voidable and void pieces of evidence, wherein the former is admissible after complying with some conditions and the latter is very unlikely to be admissible subject to the provision of section 35(5) of the Constitution.[3945]

[3943] Paras 7.5.6 and 7.7 of this chapter.
[3944] Para 2.3.3 of Chapter 2 of this study.
[3945] Para 7.8 of this chapter.

The quick-silver technologically innovative and slippery race passes on the baton to the next generation to fight the unresolved wars of techno-legal complexities, sophistication and eagling with momentary and "miraging" solutions insight from many quarters.

CHAPTER 8: FINDINGS AND RECOMMENDATIONS

8.1 INTRODUCTION

This chapter does not only summarise the key findings in this study but proffers some key recommendations in pursuance of the findings made in chapters two to seven of this study. Expectedly, Chapter One, titled 'Introduction', which addresses various issues in any prologue, summarily identifies a myriad of techno-legal challenges in the protection of the right in online communication and the conduct of an OCI arising from the inadequate legal regime in these regards in the RSA.

8.2 CHAPTER 2: TECHNO-LEGAL ASPECTS OF THE NATURE AND FEATURES OF ONLINE COMMUNICATION AND CRIMINAL INVESTIGATION

This chapter lays the foundation for the techno-legal framework for the two concepts in this study, namely, online communication and online criminal investigation.[3946]

There are five channels of information communication which are broadcasting, human agent, postal service, offline electronic and online communications. An online communication channel, which is an on-demand online communication, is basically and cumulatively more exposed to unique, inherent and greater risks in the non-compartmentalised, non-passworded compartmentalised, interoperable and permanently conscriptive roaming and non-roaming

[3946] Chapter 2 of this study.

quick-silver online communication devices, technologies, networks, applications and services than the other channels of communication.[3947] Therefore, it is recommended that online communication deserves greater protection than the other channels of information communication.[3948]

The risks of exposure in online communication are exacerbated not only by the generally intrusive, worse still, piercing nature of the complex and delicate conduct of an OCI of online communication in the RSA but also by the globally condemned U.S. principle of 'no server, no law'.[3949] This principle requires the authorities in the RSA to usually request for consent from the U.S. authorities before conducting an OCI in an Internet-based platform relating to serious offences committed in the RSA and outside the RSA which fall under the international jurisdiction of the RSA like any country has same or similar duty to do so in the comity of nation.[3950]

It is therefore proposed that the conduct of an OCI should not only be protected in the Constitution as one of the ways to raise the standards in which an OCI is conducted but to protect the sovereignty of the RSA in terms of managing its affairs concerning the investigation of offences committed in the RSA through the conduct of an OCI in Internet-based platforms.[3951] Accordingly, this study conceptualises five techno-legal principles to refute the application of the U.S. principle of 'no server, no law' in the conduct of an OCI on the Internet in the RSA. These are the 'intellectual property right', 'global' or 'geographical location technology' (GLT), 'general business compliance', 'urgency and necessity' as well as 'constitutional law supremacy' principles.[3952]

Finally, given that RICA grants the power to conduct an OCI to only six LEAs, this study reveals that RICA denies other authorities and entities —such as the OPP, SARS, other Chapter Nine Institutions, and many more— the right to legally, independently, reasonably and satisfactorily execute their constitutional and statutory functions, which include the power to conduct an OCI of serious offences.[3953]

[3947] Paras 2.2 and 2.3 of Chapter 2 of this study.
[3948] Paras 2.2 - 2.3 and 2.10 of Chapter 2 of this study.
[3949] Chapter 2 of this study.
[3950] Chapter 2 of this study.
[3951] Paras 2.5 - 2.10 of Chapter 2 of this study.
[3952] Para 2.8 of Chapter 2 of this study.
[3953] Para 2.11.2 of Chapter 2 of this study.

In accordance with some grand rules,[3954] this study, in curing the defect herein, further recommends that the following general authorities and entities should be empowered to conduct an OCI, namely, constitutional online criminal law enforcement agencies; emergency online criminal law enforcement officers; foreign and international online criminal law enforcement agencies and professional and non-professional online criminal private investigators. Other authorities and entities include Special LEOs comprising pilots or captains and their crews who are trained and qualified to conduct an OCI in the air and on or in the sea respectively and Artificial LEOs (such as robots[3955] and drones[3956] which are configured to be triggered off[3957] in a manner akin to how a *Blackbox* is triggered off in an aircraft crash)[3958] to conduct an OCI in a robotically controlled environment.

8.3 CHAPTER 3: JURISPRUDENCE OF THE TECHNO-LEGAL PROTECTION OF THE RIGHT TO THE SECRECY OF ONLINE COMMUNICATION

In further substantiating the unimaginable risks in online communication and the need for greater protection of the right in online communication,[3959] this chapter reveals that section 14(d) of the Constitution, from which the jurisprudence of the right in online communication is derived and juxtaposed, does not expressly protect the right to the SOC, neither do the five pieces of legislation on privacy protection examined in this study adequately protect the right in online communication.[3960] Thus —as one of the findings from the foregoing— these

[3954] Para 2.11 of Chapter 2 of this study.

[3955] The idea of a robot, which is also called Bot, agent, spider or crawler was first introduced in 1921 by Karel Capek. It has been described as 'meaning a software agent which does the bidding of its master', Newton *Newtons' telecom dictionary* 782. Akwei I 'Nigerian Amina Mohammed interacts with Sophia the robot at the UN' http://www.africanews.com/2017/10/12/nigerian-amina-mohammed-interacts-with-sophia-the-robot-at-the-un-video// (Date of use: 18 October 2017) (Akwei http://www.africanews.com/2017/10/12/nigerian-amina-mohammed-interacts-with-sophia-the-robot-at-the-un-video// (Date of use: 18 October 2017); United Nations Radio 'Robots can and will "walk among us" robotics chief tells UN' http://www.unmultimedia.org/radio/english/2017/10/robots-can-and-will-walk-among-us-says-ceo-of-hanson-robotics/#.WhvkxlWWaUk (Date of use: 18 October 2017) (United Nations Radio http://www.unmultimedia.org/radio/english/2017/10/robots-can-and-will-walk-among-us-says-ceo-of-hanson-robotics/#.WhvkxlWWaUk (Date of use:18 October 2017).

[3956] Muller *Autonomous killer robots are probably good news* 70; De Greef *Delegation and responsibility: A human –Machine perspective* 139.

[3957] eNCA 'New gunshot detection system takes aim at Cape gangsterism' https://www.enca.com/new-gunshot-detection-system-takes-aim-cape-gangsterism (Date of use: 13 September 2017) (eNCA 'Gunshot detection system') (eNCA https://www.enca.com/new-gunshot-detection-system-takes-aim-cape-gangsterism (Date of use: 13 September, 2017**)**.

[3958] The colour of a Blackbox is actually a light orange device, which is used to record voice and data during an aircraft flight used by investigators to reconstruct the events before a plane crashes, Newton *Newtons' telecom dictionary* 161.

[3959] Para 8.2 of this chapter.

[3960] Para 3.5.6 of Chapter 3 of this study.

inadequacies arguably make it difficult for LEAs, LEO, investigators and unauthorised persons to respect and protect the right to the SOC in the RSA.[3961]

Accordingly, based on the general and the four special reasons and the thirteen criteria considered for the protection of online communication as opposed to the protection of information in other channels of information communication, this study cumulatively and unequivocally points to one direction.[3962] This direction necessitates the need to recognise and protect the independent or dependent right to the SOC, drawn on the recognition and protection of the right to the SOC in Europe and the U.S.A.[3963]

The right and sub-rights to the SOC are a befitting right that is proposed to be unequivocally protected in the Constitution either in section 14 privacy provision or under Chapter 11 of the Constitutional mandate of LEAs to maintain peace, law and order[3964] and in the various statutes of the RSA due to the greater factual and legal expectations of secrecy in online communication than in other channels of information communication.[3965]

As opposed to the existing three offline levels of the continuum of privacy,[3966] the recognition of the right in an online communication protects a higher, comprehensive and complex reasonable continuum of secrecy in online communication[3967] in the dynamic five levels of the reasonable continuum of secrecy of online communication. The five levels are the innermost, inner, middle and outer sancta and public domain levels of the continuum of online content and non-content communication secrecy which cater for the heterogeneous, complex and dynamic rights in the SOC.[3968]

Furthermore, the protection of the five levels is relatively, proportionately and reasonably adequate to conduct an OCI according to the severity and the types of serious offences on the

[3961] Para 3.5.6 of Chapter 3 of this study.
[3962] Paras 3.2 - 3.8 of Chapter 3 of this study.
[3963] Paras 3.2 - 3.8 of Chapter 3 of this study. In the U.S., it has been advised that the values, interests and right in online communication should not be treated as a physical property, Baker S A 'Privacy for the real world' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (2012) 145 (Baker *Privacy for the real world*); Ruiz *Privacy in telecommunications* 1-5, 15, 20-23, 45-46, 59-67, 70, 81-83, 86-87, 143, 151-159, 171-172, 175-177, 179-257, 313-318 and 322-323.
[3964] See para 8.8 of this chapter where the sub-rights of the SOC are highlighted.
[3965] Paras 3.5.6 and 3.6-3.8 of Chapter 3 of this study.
[3966] Para 3.7 of Chapter 3 of this study.
[3967] Paras 3.6 - 3.8 and 3.11 of Chapter 3 of this study.
[3968] Para 3.8 of Chapter 3 of this study.

one hand and the types of devices, technologies, networks, applications and services on the other hand.[3969] This study identifies this type of proportionality as the general 'proportionality of continuum of online secrecy' principle.[3970]

Given the adoption of a holistic approach to protect the right in online communication in this study, the second leg of this chapter reveals that the right to the SOC cannot be protected if the roles and liabilities of stakeholders in the protection of this right are not scrutinised and declared culpable if breached and consequently, sanctioned.[3971] Thus, the stakeholders in the protection of the right to the SOC must be held responsible in the management or otherwise of this right, otherwise, the justification for the protection of the right to the SOC will be an exercise in futility or another academic exercise.[3972]

Consequently, it is recommended that all stakeholders —including the regulatory and non-regulatory authorities, entities and users of online communication— owe a duty of care in the protection of the integrity and security of online communication, failing which criminal sanctions are imposed on or enforced against the stakeholders.[3973] In doing so, the various statutes need to be amended to incorporate proportionate responsibilities and sanctions against the various stakeholders, including regulatory authorities, LEOs, manufacturers of online communications and interception devices, Online Communication Service Providers, Interception Centre and users of online communication.[3974]

The foregoing measures will prevent the brazen, wilful, and unauthorised bulk and specific conduct of an OCI in the RSA by unauthorised persons.

[3969] Paras 2.2, 3.8, 5.3.4, 5.3.6, 5.4 and 6.3 of this study.
[3970] Para 5.4.2 of Chapter 5 of this study.
[3971] Paras 3.9 and 3.10 of Chapter 3 of this study.
[3972] Paras 3.9 and 3.10 of Chapter 3 of this study.
[3973] Paras 3.9 and 3.10 of this chapter.
[3974] Paras 3.9 and 3.10 of this chapter.

8.4 CHAPTER 4: MANAGEMENT OF THE AFFAIRS AND ACTIVITIES OF LAW ENFORCEMENT AGENCIES IN CONDUCTING ONLINE CRIMINAL INVESTIGATION

This study reveals that the general statutory, regulatory and policy frameworks for the management of the affairs and activities of LEAs and LEOs in the conduct of an OCI in the unique, complex and delicate online communication are inadequate.[3975] In particular:

a) There is the absence of constitutional provision and adequate statutory regime recognising, protecting and regulating the activity involved in the conduct of an OCI as a specialised and professional activity,[3976] which is distinct from the general investigative, security or intelligence services;

b) There is a dearth of regulation on the requirements of special knowledge, experience, training and skill in the employment, retention, deployment and execution[3977] of the functions of LEOs as a specialised unit in the conduct of an OCI;[3978]

[3975] Chapter 4 of this study.

[3976] Paras 4.3.8, 4.4 and 4.6 of this chapter. Although section 195(1)(a) and (2)(b) of the Constitution prescribes the promotion and maintenance of high ethical and professional standards of organs of state-including LEAs, no statutory principle or provision exists in RICA or other Acts to implement section 195(5) and (6) of the Constitution. Section 195(5) and (6) requires that a special consideration be given to the nature, functions and activities of different sectors, administrations or institutions in their regulation. However, there is absence of statutory provision recognising, protecting and regulating the activity involved in the conduct of an OCI, which is an inherently unrestrictive, intrusive and delicate form of investigation unlike the professional practice of medicine, law and accounting, amongst others. Whereas, there is a strong, formal and formidable call for the activity of mediators to be professionalised and accredited in the RSA as other noble professions are, see Marnewick C *Mediation practice in the Magistrates' Courts* (2015) 131, 136 and 148 (Marnewick *Mediation in the Magistrates' Courts*); Secretary General 'Report of the Secretary-General on UN United Nations Activities in Support of Mediation (2017) 19. If there is a call for the professionalism of the activity of mediators, it is submitted that the consideration for the professionalism of the activity involved in conducting an OCI is in recognition of the significance of the role of the activity of OCI in the criminal justice system in the twenty-first century era in the RSA. In sum, though the Constitution generally recognises the need to give special considerations to the nature, functions and activities of different sectors, administrations or institutions in their regulation, absenting an express mention of the activity of the conduct of an OCI seems to undermine the overarching significance of this method of investigation in contemporary society. Nevertheless, this submission does not in any way diminish the equal significance that should be attached to other methods of investigation, which can be addressed in another study, but does not form the scope of this study to embark on a broad study of that nature.

[3977] Mokgosi *The telecommunications regulators* 103 and 122-123. Reference can be made to the call for mediators to be trained theoretically and practically and comply with domestic and international ethical codes as professionals in the RSA as other professions do, Marnewick *Mediation in the Magistrates' Courts* 139-149.

[3978] Applicants Affidavit in *AmaBhungane v Minister of Justice* supra 175.3. In preparation for the implementation of cyber capacity to ensure the protection of critical information infrastructure for government in CCB B6-2017, judicial officers and prosecutors only are expressly mentioned to participate in the training in this regard. In other words, LEOs and other organs of state and entities involved in the conduct of OCI are

c) There is a lack of or inadequate regulation of the funding and techno-legal practical operation of an OCI as a specialised method, and unit in the investigative, security or intelligence services cluster;[3979]

d) There is a dearth of accountability[3980] and oversight of LEAs or LEOs as a specialised investigative, security or intelligence service in conducting an OCI.

Therefore, the current statutes should be amended to incorporate specific and principled provisions by adopting some due process, separation of powers as well as certain check and balance mechanisms in the appointment of specialised staff and conduct of specialised training for LEOs, operation and funding and accountability and the oversight of LEAs for purposes of conducting an effective and efficient OCI in the RSA.[3981]

In addition, in the same or similar ways that the medical, accounting and legal professions — amongst others— are regulated, this study recommends the need for statutory recognition, protection and regulation of the broad profession of electronic criminal investigators.[3982]
The profession will comprise both offline electronic and online communication investigators to ensure the regulation of proper and specialised appointment of staff and conduct specialised training, operation and accountability of LEOs in the conduct of an OCI.[3983]

excluded from the training in this regard. The inclusion of LEOs would have generally added to their knowledge and other relevant stakeholders in generally understanding online investigation, see para 86 of the Memorandum on the Objects of the Cybercrimes and Cybersecurity Bill 2017, which forms part of CCB B6-2017. In the U.S., specialised training is required of every investigator according to the field of specialisation, see CIA 'Training in investigative techniques' https://www.cia.gov/library/readingroom/docs/CIA-RDP57-00012A000200090081-3.pdf (Date of use: 11 September 2016).

[3979] The significance of independent funding for the effectiveness and efficiency of both LEAs and regulatory authorities in the telecoms industry cannot be over-emphasised, see Mokgosi *The telecommunications regulators* 103 and 121.

[3980] *Primemedia v Speaker, National Assembly* supra 72, 75 and 76; Mokgosi *The telecommunications regulators* 103, 119 and 121.

[3981] Chapter 4 of this study.

[3982] Para 4.6 of Chapter 4 of this study.

[3983] Para 4.6 of Chapter 4 of this study.

8.5 CHAPTER 5: LIMITATION OF THE RIGHT TO THE SECRECY OF ONLINE COMMUNICATION

Given that all rights are limited by section 36 of the Constitution of the RSA, statutory law — such as RICA— and common law,[3984] the right to the SOC is no exception to the application of section 36 principle where it is necessary to conduct an OCI of serious offences in the public criminal interest.[3985]

Based on the principle of constitutional democracy that the RSA subscribes to and enforces, this chapter further reveals that the five principles laid down in section 36 of the Constitution are adequate to limit the right to the SOC by way of conducting an OCI of serious offences.[3986] Specifically, chief amongst these principles that stand out in these five principles is the proportionality test principle,[3987] which though incorporates the other four principles in section 36 of the Constitution, is applicably constant, relevant and examined in chapters two to seven of this study under various rubrics. It is therefore recommended that the proportionality principle cannot be over-emphasised in an attempt to strike a balance between the protection of the right to the SOC and the conduct of an OCI in the RSA.

8.6 CHAPTER 6: APPLICATION FOR AND ISSUANCE OF ONLINE CRIMINAL INVESTIGATION DIRECTION

In this chapter, the following key findings and recommendations are made.

Firstly, this chapter reasonably reveals that there are court directed and non-court directed online interceptions.[3988] A court direction is required in an online criminal investigation which covers other circumstances which are not mentioned in the following.[3989] Non-court directed online interception occurs in a non-consensual party online intercept, consensual party online intercept, emergency online intercept, online criminal investigation under the CSA —though

[3984] Para 5.2 of Chapter 5 of this study.
[3985] Para 5.3 of Chapter 5 of this study.
[3986] Para 5.3 of Chapter 5 of this study.
[3987] Paras 5.3.4, 5.3.6 and 5. 4 of Chapter 5 of this study; *AmaBhungane v Minister of Justice* supra 167.
[3988] Paras 6.2 of Chapter 6 of this study.
[3989] Para 6.2 of this chapter.

it is argued that a direction is unrequired here— and technical maintenance and monitoring online intercept.[3990]

Secondly, this study reveals that despite the pronouncement by the Constitutional Court on the need to have the earlier offline investigation of some serious offences, no law or regime — which is in defiance of the proportionality principle— classifies serious offences, its timing or its stage of investigation nor provides for a specific standard of proof to investigate the serious offences identified by the Constitutional Court in the offline or online worlds.[3991]

The reality in the conduct of an OCI is that LEAs are the representatives of the executive authority whose applications before the court must be reasonable, rational and justifiable in the offences that constitute 'severe' risks —for example— to proportionately conduct an OCI at the first class and stage of crime commission, which is Herculean to prove and almost comparable to the task of attempting to take a camel through the eye of a needle.[3992]

In pursuance of the prominence or indispensability of the application of the proportionality principle in chapters two to seven, this study makes the following recommendations.

The first recommendation identifies six categories of serious offences in each of the four criteria for a specific classification of serious offences in an OCI application before the court which are: a) the bail condition criterion against a perpetrator; b) the penology of an offence criterion against a perpetrator; c) the criterion of the irreversibility of the effect of the commission of an offence on a victim; d) the criterion of economic harm or loss to the victim.[3993] Practically, it is recommended that two criteria must be considered by the court in an OCI application with at least one criterion from paragraphs (a) and (b) and one criterion from paragraphs (c) and (d) in order to attempt to strike a balance in the conflict of interest of justice between the perpetrator and the victim of the crime.[3994]

[3990] Para 6.2 of this chapter.
[3991] Para 6.3 of this chapter.
[3992] Paras 5.3.4, 5.3.6, 5.4 and 6.3 of this study.
[3993] Para 6.3 of Chapter 6 of this study.
[3994] *Investigating Directorate v Hyundai and Smit No* supra 54.

In further practical pursuance of the above classification, this study proposes some 'proportionality of seriousness and class or stage of crime commission' measures,[3995] in which the court is expected to consider at least two out of the four classifications of serious offences criteria in simultaneously determining the degree of serious offences and the appropriate timing of the conduct of an OCI in such categorised offences.[3996] For example, 'severe national risk' offences will be investigated at the earliest stages of crime commission than 'high and medium risk' offences.[3997] Given the Herculean task of conducting an OCI at the earliest or first stage of crime commission, this study justifies the need to create, retain and maintain this stage of crime commission to prevent and control crime in the RSA.[3998]

Secondly, in attempting to influence the current legal position of legal reasoning, rationale and robust discourse[3999] on the standards of proof, with a commitment to demonstrate the use of numerous quantitative reasoning methods, the demonstration of which is not meant to make LEAs, lawyers, judges or other stakeholders become mathematicians,[4000] this study creates an imaginary mathematical assumption in the minds of LEOs on the standard of proof in conducting an OCI in the RSA.[4001] In this regard, the proposed Popoola mathematical formulae provide a panacea of good knowledge and insight for the likely confused or indeterminable state of minds of some stakeholders to accurately gather facts or access facts gathered in the offline and online worlds in the first instance.[4002] These formulae also enable the court to discern facts presented before it[4003] to specifically establish the relevant standards of proof in the conduct of an OCI of relevant serious offences.

Therefore, the second recommendation in this chapter proposes that the proportionality principle is applied in the legislatively proposed Popoola mathematical and non-mathematical substantive and adjectival standards of proof required in an OCI application to correspondingly investigate the proposed classified six classes and stages of crime commission in the RSA.[4004]

[3995] Para 5.4 of Chapter 5 of this study.
[3996] Para 6.3 of Chapter 6 of this study.
[3997] Para 6.4 of Chapter 6 of this study.
[3998] Para 6.3 of Chapter 6 of this study.
[3999] Finkelstein and Levin *Statistics for Lawyers* xi.
[4000] Finkelstein and Levin *Statistics for Lawyers* viii, ix and x; Hutchinson *Doctrinal research* 8.
[4001] Para 6.4.4 of Chapter 6 of this study.
[4002] Finkelstein and Levin *Statistics for Lawyers* x- xi.
[4003] Finkelstein and Levin *Statistics for Lawyers* x- xi.
[4004] Paras 6.4 - 6.6 of Chapter 6 of this study.

In addition, the mathematical formulae lay the foundation for consideration by programmers of the configuration of an artificially intelligent LEO or a ROCITOR —with machine learning capability— to accurately determine the various standards of proof to conduct an OCI.[4005] The application of AI has already taken over the general or basic human operations in contemporary society, therefore, the field of cyberlaw, more particularly the conduct of an OCI, should not be an exception.[4006]

Therefore, this study lays the foundation for the guidance on the proper configuration and deployment of an AI in the conduct of an OCI in the unforeseen nearest future.[4007] According to cyber law jurists, there is a marital symbiotic relationship between human and artificial intelligent entities, which ultimately create a powerful and more effective interdependent synergy that goes beyond the independent limit of each entity, otherwise, each entity is unable to solve complex problems individually.[4008]

Thirdly, aside from the provision for oral and written ex-parte covert conduct of an OCI before a magistrate, regional magistrate, judge or designated judge,[4009] no law makes provision for an application for motion on notice to a ghost or public advocate and an intervening application by a vigilant target, therefore it is recommended that a proportionately competent LEO[4010] or an investigator conducts an OCI in the latter manners herein.

Fourthly, in resolving the problems associated with offline application and hearing processes in an OCI, this study proposes *Popoola QOCI* protocol solution on the basis that in contemporary society, there is a very strong possibility of using audio-visual devices for online filing and hearing of an OCI application.[4011] For example, although the 'WhatsApp' audio-visual software application is not currently reliable in terms of undisrupted, uninterrupted and clear audio and visual connectivity, however, 'WhatsApp' is easily available in the RSA for the general public in their routine communications.[4012]

[4005] Paras 6.3- 6.6 of this chapter. See generally the 'high level of technological readiness' of robust performance of autonomous artificial intelligence in the use of drones, which are tested outside the laboratory, Muller *Autonomous killer robots are probably good news* 70.
[4006] Paras 2.11.4 and 6.4.9 of this study.
[4007] Paras 2.11.4, 6.4.9 and 6.11 of this study.
[4008] De Greef *Delegation and responsibility: A human –Machine perspective* 139.
[4009] Paras 6.7 - 6.10 of this chapter.
[4010] Para 6.8 of chapter 6 of this study.
[4011] Para 6.11 of Chapter 6 of this study.
[4012] Para 6.11 of Chapter 6 of this study.

Given this technological development, it is a confirmation that a specific piece of legislation that allows a technically secure, undisrupted, uninterrupted and clear audio-visual hearing application ensures the efficiency and effectiveness of the conduct of an OCI in the RSA by preventing the brazen, wilful, and unauthorised bulk and specific conduct of an OCI in the RSA by unauthorised persons.[4013]

The fifth recommendation is that section 205 of the CPA, which has been validly sanctioned by the Constitutional Court is incongruous in the conduct of an OCI because it does not comply with the object and provisions of RICA as the main legislation in the conduct of an OCI. Therefore, section 205 should be amended to incorporate the provisions of RICA, be expunged from RICA if it cannot be amended to align with the provisions of RICA or be applicable to offline investigation only.[4014]

In the sixth recommendation, it is reiterated that the High Court in *AmaBhungane* vehemently opposes the implementation of mass OCI[4015] because of the absence of regulation of mass OCI in RICA or any other law, the conduct of which is generally anathemic in the conduct of an investigation. Instead of having an outright ban on mass conduct of an OCI, this study proposes a proportionately regulated mass OCI that should be conducted according to the degree of serious offences, irreversibility of the effect of the commission of a serious offence and other special circumstances in an application brought before three judges with adequate knowledge in the conduct of an OCI.[4016]

In the seventh recommendation, this study reveals that the right of an innocent or third party in online communication is not protected when conducting an OCI.[4017] However, this study proposes a techno-legal remedy that enables the technical sifting of the online communication of an innocent or third party and a declaration in an OCI application that LEOs and investigators will not embark on conducting an OCI on an innocent or third party.[4018]

[4013] Para 6.11 of Chapter 6 of this study.
[4014] Para 6.12 of this chapter.
[4015] *AmaBhungane v Minister of Justice* supra 143 -165.
[4016] Paras 6.3.3 and 6.13 of Chapter 6 of this chapter.
[4017] Para 6.14 of Chapter 6 of this study.
[4018] Para 6.14 of Chapter 6 of this study.

The eighth recommendation is that this chapter further reveals that privileged online communications between an attorney and a client, investigative journalists and an informer or whistle-blower and other similar relationships exist and such relationships are not protected in RICA or any other law in the RSA.[4019] However, in the case of *AmaBhungane*, the court, in emphasising on some conditions, reinstates the protection of privilege online communication between an attorney and a client and an investigating journalist and an informer, the principle of which does not exonerate these professionals where they have personal criminal liability to answer to.[4020]

It is further recommended that before journalists or investigative journalists enjoy this privilege, they must —like the legal professionals are— be regulated and registered by statute, but such journalists cannot be regulated in terms of censorship law such as PSIB (or 'Secrecy Bill') that seeks to shutout the voice of journalists in revealing the necessary State secret.[4021]

In the ninth recommendation, it is revealed that the indemnity from prosecution of a LEO or an investigator for the unlawful conduct of an OCI in RICA does not proportionately consider the level of intention or type of breach of RICA provisions by a LEO or investigator in the conduct of an OCI and the nature and seriousness of an offence for which evidence is unlawfully obtained in RICA *vis-a-vis* the admissibility of such intentionally and unlawfully obtained evidence in the investigation of a serious offence.[4022]

Accordingly, it is recommended that the proportionality principle be applied when considering whether to grant an indemnity to a LEO or an investigator who has unlawfully conducted an OCI.

Lastly, in summarising the foregoing recommendations, the overall befitting recommendation to make concerning the conduct of an OCI is to incorporate this mandate in the Constitution of the RSA as the most appropriate, rational and reasonable decision in contemporary society.

[4019] Para 6.15 of this study.
[4020] Para 6.15 of Chapter 6 of this study.
[4021] Right2Know at 6 https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November, 2018; Ferreira E New secrecy bill recalls the failings of the old https://www.iol.co.za/news/politics/new-secrecy-bill-recalls-the-failings-of-the-old-17106869 (Date of use 25 September 2018); Para 6.15 of this study.
[4022] Para 6.16 of Chapter 6 of this study.

8.7 CHAPTER 7: EXECUTION AND POST-EXECUTION OF ONLINE CRIMINAL INVESTIGATION DIRECTION

In this chapter, the following findings and recommendations are made.

Firstly, RICA does not, under the principle of *delegatus potest non delegare*, make provision for the regulation or adequate regulation of the delegation or further delegation of power originally granted to LEOs to conduct an OCI because it is not expected that every Tom, Dick and Harry in the LEAs will be allowed to conduct an OCI in the delicate and complex right to the SOC.[4023] Consequently, it is recommended that a relevant provision be made in RICA and other law in this regard.

Secondly, RICA makes provision for the role and management of the affairs and activities of executing authorities and entities —including Online Communication Service Providers such as Decryption Keyholder, Cryptographer, Authentication Service Provider, Cyber Inspector, Telecommunication Service Provider and Interception Centre— in the conduct of an OCI. Nonetheless, the provisions are inadequate to strike a balance in the conflict between the protection of the right to the SOC and the conduct of an OCI in terms of the appointment of specialised staff, functions, powers, operations and oversight by and of the stakeholders in the conduct of an OCI.[4024]

Worse still, one of the executing authorities, the NCC, which operates under the control and management of the SSA, is not regulated by any law, yet conducts an unfettered domestic and international OCI without a direction which is a grievous infringement of the right to the SOC.[4025]

Accordingly, it is recommended that comprehensive and adequate provision be made on the management of the affairs and activities of the executing authorities and entities in the conduct of an OCI in terms of the appointment of specialised staff, functions, powers, operations, funding and oversight by and of the stakeholders in the conduct of an OCI.[4026]

[4023] Para 7.2 of Chapter 7 of this study.
[4024] Paras 7.3.1- 7.3.3 and 7.3.5- 7.3.6 of Chapter 7 of this study.
[4025] Para 7.3.4 of Chapter 7 of this study.
[4026] Paras 7.3 and 7.6 of Chapter 7 of this study.

Thirdly, RICA makes provision that the LEAs submit reports to the designated judge in a proportionate manner, which is a fundamental principle in this study. However, RICA does not regulate how the judge exercises this discretion in terms of the frequency of submission of a report according to the seriousness of an offence.[4027] Therefore, it is proposed that a comprehensive judges' rule on the conduct of an OCI should be established for proper guidance in this regard.[4028]

Fourthly, RICA and RICA Directives 2005 make provision for the management of data in an OCI which cover several areas of data management. However, some provisions are reasonably inadequate such as the management of copying, duplicating, routing, provisioning, storage and deletion of data, while some provisions are grossly inadequate such as the management of sealing, sorting, retrieving and examination of data in the pre and post-execution of an OCI.[4029] It is therefore not surprising that the court in *AmaBhungane* held that there cannot be a 'pass-mark approach' for the adequacy of the provisions of RICA.[4030]

Because of this, the role of stakeholders in the various aspects of the pre and post-execution management of data should be clearly set out in RICA as ordered by the court that guiding rules should be incorporated in the primary source of law, which is RICA and not secondary sources of law such as RICA Directives 2005.[4031] The additional approach to be adopted in this recommendation is for the drafters of the law to adequately identify and make provision for every techno-legal activity and affair involved in the 'what', 'when', 'who', 'how' and 'why' of the pre and post-execution management of data in the conduct of an OCI.

Fifthly, amongst the governmental authorities and entities —namely the OIC, OIGI, JSCI of Parliament and judiciary who are the direct stakeholders in this regard— and the non-governmental entities —who are the indirect stakeholders in this regard— that oversee the activities and affairs of LEAs and interception entities in the conduct of an OCI, the JSCI and the judiciary are the most institutionalised and regulated authorities.[4032] These latter authorities

[4027] Para 7.4 of Chapter 7 of this study.
[4028] Section 58 of RICA.
[4029] Para 7.5 of Chapter 7 of this study.
[4030] *AmaBhungane v Minister of Justice* supra 104.
[4031] *AmaBhungane v Minister of Justice* supra 89(2), 101 and 107.
[4032] Para 7.6 of Chapter 7 of this study.

are relatively competent, independent and accountable in overseeing the activities and affairs of the LEAs and interception entities in the conduct of an OCI.[4033]

Nonetheless, some remarkable inadequacies are identified in the performance of the role of the direct stakeholders who oversee the activities and affairs of LEAs and interception entities in the conduct of an OCI.[4034] This is more particularly pronounced, amongst others, in the absence of or inadequate operational or practical requirements in the area of knowledge, skill and experience acquisition of the direct stakeholders, given the complex, complicated and technical nature and features of the right to the SOC and the conduct of an OCI.[4035]

Sequel to the abovementioned points, it is recommended that the direct stakeholders who oversee the activities and affairs of the LEAs and interception entities in the conduct of an OCI be compelled to attend and be formally certified in the professional training meant for electronic criminal investigators,[4036] amongst other requirements. This is to improve the competence, independence and accountability of the direct stakeholders in overseeing the activities and affairs of the LEAs and interception entities.[4037]

Sixthly, the Constitution makes provision for an ACR or ADR mechanism. However, RICA does not make provision for an alternative conflict or dispute resolution or management ACM or ADM mechanism to redress the disputes or conflicts that arise in the protection of the right to the SOC and the conduct of an OCI.[4038] It therefore follows that an ombudsman be established, operational and funded under RICA or in a comprehensive law to address the grievances of aggrieved parties in the conflict between the right to the SOC and the conduct of an OCI before such grievances are escalated to the Office of the Inspector-General of Intelligence.[4039]

Finally, even though some pieces of evidence are unlawfully obtained through the concept of online conscription,[4040] the conduct of an OCI and other necessitating methods of investigations

[4033] Para 7.6 of Chapter 7 of this study.
[4034] Paras 7.3 and 7.6 of Chapter 6 of this study.
[4035] Para 7.6 of Chapter 7 of this study.
[4036] Para 4.6 of Chapter 4 of this study.
[4037] Para 7.3 and 7.6 of Chapter 7 of this study.
[4038] Para 7.7 of Chapter 7 of this study.
[4039] Paras 7.6.4 and 7.7 of Chapter 7 of this study.
[4040] Para 2.3.3 of Chapter 2 of this study.

in RICA, however, this study reveals that unlawfully obtained evidence can ultimately be considered voidable and voided pieces of online evidence.[4041]

It is therefore recommended that the rule of admissibility to be adopted in the online evidence that is lawfully or unlawfully obtained through an OCI should primarily and mainly be determined by the following factors: the nature and features of the particular type of online communication data that is being obtained; the nature and irreversibility of the effect of the commission of a serious offence that is being investigated; the type of an OCI that is conducted and the state of lawlessness in the RSA that may warrant the inevitability of unlawfully obtaining online evidence, amongst other criteria.[4042]

8.8 OVERALL FINDINGS AND RECOMMENDATIONS

Although the Constitution broadly protects the right to privacy, nonetheless, it does not expressly recognise the right to the SOC in section 14(4). Furthermore, although five main statutes expressly protect the complex and complicated nature and features of the right in online communication and the conduct of an OCI,[4043] however, these statutes do not adequately protect both the right to the SOC as an independent and dependent right and the conduct of an OCI.[4044] These inadequacies created in the regime regulating the two sides of the coin above are not only problematic in the obvious contemporary quick-silver technological era due to the irresponsiveness of the law but exacerbate the natural conflict between the two sides of the coin.[4045]

Nonetheless, if section 36 constitutional limitation clause is properly interpreted in line with the peculiar risky nature of online communication protection, it is adequate to strike a balance in the conflict between the right to the SOC and the conduct of an OCI of serious offences to protect the public criminal interests.[4046]

[4041] Para 7.8 of Chapter 7 of this study.
[4042] Paras 2.2, 2.3, 2.5 - 2.10 of Chapter 2 and 6.3.3 of this study; Van der Merwe S E 'Exclusion of Relevant Evidence: Unconstitutionally obtained evidence' in Schwikkard P J and Van der Merwe S E *Principles of evidence* 4th ed. (2016) 227-228.
[4043] Paras 2.3, 3.5, 8.2 and 8.3 of this study.
[4044] Para 3.5.6 and *AmaBhungane v Minister of Justice* supra 167.
[4045] Para 3.5.6 of Chapter 3 of this study.
[4046] Chapters 2, 3, 5, 6 and 7 of this study.

The inadequacies identified in this study are exacerbated by the LEAs, LEOs and other types of investigators whose management of affairs and activities in determining the risk levels of crime commission to determine the conduct of an OCI is inadequate to strike a balance between the two sides of the coin.[4047]

The inadequacies above are further exacerbated by the deficiencies in the application for and issuance of an OCI direction, mainly the non-classification of serious offences for purposes of proportionately conducting an OCI in which no specific, and accurate, better still, mathematical and non-mathematical substantive and procedural standards of proof in an OCI and a ROCI are pronounced by the courts.[4048]

Worse still, the conduct of an OCI, which is substantially or even absolutely supposed to be an online investigation, including the administrative processes of conducting an OCI, is ironically still administratively, infringingly and substantially conducted in an offline method in terms of the compelling offline filing and hearing of an OCI application and offline issuance of an OCI direction by the court to the LEAs.[4049] This offline process is opposed to the *Popoola QOCI* protocol and direction propounded in this study, which addresses the conflicting issues raised in this regard in the study.[4050]

Further inadequacies identified in this study include: the incongruity of section 205 of the CPA which enables the LEAs, LEOs and other investigators conduct an OCI without complying with the crucial provisions of RICA[4051] and the unregulated conduct of bulk or mass conduct of an OCI by the NCC.[4052] Other inadequacies include: the unprotected right in a privileged online communication between a client and a statutorily registered attorney and an investigative journalist —who is not required to be statutorily registered in the RSA— and informer respectively in a general online communication when conducting an OCI[4053] and inadequate provision for the management of data in the pre and post-execution conduct of an OCI including lack of institutionalised ADR mechanism.[4054] In addition, other inadequacies

[4047] Chapter 4 and para of 8.4 of this study.
[4048] Chapter 5 (more particularly paras 5.3.4 and 6.3.6) and paras 6.3 - 6.5 and 8.5 of this study.
[4049] Para 6.11 of Chapter 6 of this study.
[4050] Paras 6.11 and 8.6 of this study.
[4051] Paras 6.12 and 8.6 of this study.
[4052] Paras 6.13 and 8.6 of this study.
[4053] Paras 6.14, 6.15 and 8.6 of this study.
[4054] Paras 7.3 -7.5, 7.7 and 8.7 of this study.

are as follows: inadequate provision for the competence, transparency, independence and accountability of the key oversight authorities in overseeing the activities and affairs of LEOs and interception entities in the conduct of an OCI[4055] and save for the appropriate application of the adequate provision of section 35(5) of the Constitution on the admissibility of unlawfully obtained evidence, the deficient provision in RICA on the regulation of the admissibility of an unlawfully obtained online evidence in the conduct of an OCI cannot be over-emphasised.[4056]

It is therefore recommended that the Constitution should recognise, promote and protect the right and sub-rights in online communication, not only as a right to privacy which lays the foundation for general information protection but as respective independent and dependent rights to secrecy, as well as the fact that the Constitution should recognise the mandate and sub-mandates to conduct an OCI in the Constitution in pursuance of the limitation clause in section 36 of the Constitution.[4057] It is important to note that should these rights and sub-rights and the mandates and sub-mandates be inserted in section 36 of the Constitution, it would take away the objectivity, simplicity and uniformity of the principles in section 36 which broadly limit every right in the Constitution.[4058]

The sub-rights or mandates, some of which may be included in section 14 constitutional privacy provision or under Chapter 11 of the Constitutional mandate of the LEAs to maintain peace, law and order; arguably include the right to: relative compartmentalisation and passworded compartmentalisation of an online communication;[4059] protection of interoperable online communication[4060] and a controlled online communication conscription.[4061] Other sub-rights are the right to: enjoy the 'no server, but law' principle;[4062] personhood, human dignity and autonomy in an online communication;[4063] intimacy in an online communication;[4064] be left alone in an online communication;[4065] limit access to the self in an online communication[4066]

[4055] Paras 7.6 and 8.7 of this study.
[4056] Paras 7.8 and 8.7 of this study.
[4057] Chapters 2 and 3 of this study, particularly paras 2.4 and 3.11 respectively.
[4058] Chapters 3 and 5 of this study.
[4059] Para 2.3.1 of Chapter 2 of this study.
[4060] Para 2.3.2 of Chapter 2 of this study.
[4061] Paras 2.2.2, 2.3.1 - 2.3.3 and 3.4.5.4 of this study.
[4062] Para 2.8 of Chapter 2 of this study.
[4063] Para 3.4.4.2 of Chapter 3 of this study.
[4064] Para 3.4.4.3 of Chapter 3 of this study.
[4065] Para 3.4.4.4 of Chapter 3 of this study.
[4066] Para 3.4.4.5 of Chapter 3 of this study.

and control information and communication in an online communication.[4067] In addition, the sub-rights include the right to: access to an online communication;[4068] control and protect intangible, intellectual and invaluable property in an online communication;[4069] integrity and security of basic online communication;[4070] decent and orderly manner of investigation in online communication;[4071] confirmation of identity of an OCI target before conducting an OCI;[4072] timeously receive a post-conduct notice of OCI;[4073] protect an innocent or third party in an OCI;[4074] privileged online communication[4075] and remedy in an unlawful conduct of an OCI.[4076]

In addition, adequate converse provisions in the inadequacies examined in this study should be made not in disjointed and disharmonious statutes but a single, comprehensive, coordinated and self-explanatory statute regulating the management of the activities and affairs of the LEAs in the conduct of an OCI and the principles, practices and procedures in the pre and post-execution of an OCI of serious offences in the broad areas examined in this study.[4077] This recommendation corroborates the judgment in *AmaBhungane* where the court observed that the Deputy Minister of Justice should not be pessimistic about amending RICA within two years, given the assurance by a senior state law adviser in charge of the amendment of RICA that a new version of RICA in totality will be finalised soon.[4078]

Finally, the conflict between the protection of the right to the SOC and the conduct of an OCI is a natural tension, which cannot be resolved[4079] but managed as examined in this study, given the fact that no conflict is ever resolved but managed.[4080]

[4067] Para 3.4.4.6 of Chapter 3 of this study.
[4068] Para 3.4.5.2 of Chapter 3 of this study.
[4069] Para 3.4.5.3 of Chapter 3 of this study.
[4070] Para 3.4.5.5 of Chapter 3 of this study.
[4071] Para 3.5.7.9 of Chapter 3 of this study.
[4072] Para 7.8.5.2 and 7.8.5.4 of Chapter 7 of this study.
[4073] Para 6.10 of Chapter 6 of this study.
[4074] Para 6.14 of Chapter 6 of this study.
[4075] Para 6.15 of Chapter 6 of this study.
[4076] Para 7.7 of Chapter 7 of this study.
[4077] Chapter 4 of this study.
[4078] *AmaBhungane v Minister of Justice* supra *8.*
[4079] *AmaBhungane v Minister of Justice* supra 27.
[4080] Para 7.7 of Chapter 7 of this study.

BOOKS

Adem D T *Legislative drafting: Mathematics & other devices* (LexisNexis Johannesburg 2013) (Adem *Legislative drafting:Mathematics & other devices*)

Agwu F A *Armed drones and globalisation in asymmetric war on terror- challenges for the law of armed conflict and global political economy* (Routledge New York 2018) (Agwu *armed drones and globalisation in asymmetric war on terror*)

Ahern J P 'Laptop searches and other violations of privacy faced by Americans returning from overseas travel' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Ahern *Laptop searches and overseas travel*)

Alberti A A *Wiretaps: A complete guide for the law and criminal justice professional* (Austin & Winfield USA 1999) (Alberti *Wiretaps*)

Alheit K *Issues of civil liability arising from the use of expert systems* (LL.D thesis Unisa 1997) (Alheit *Issues of civil liability arising from the use of expert systems*)

Allen A L *Uneasy access: privacy for women in a free society* (1988) (N.J. Rowman and Littlefield Totowa 1988) (Allen *Uneasy access*)

Angwin J 'How much should people worry about the loss of online privacy?' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Angwin *Loss of online privacy*)

Badejogbin O A *Sentencing reforms in a postcolonial society- Call for the rationalisation of sentencing discretion in Nigeria, drawing on South Africa and England* (PhD thesis UCT 2015) (Badejogbin *Sentencing reforms*)

Badenhorst C *Criminal capacity of children* (PhD thesis Unisa 2006) (Badenhorst *Criminal capacity of children*)

Baker S A 'Privacy for the real world' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Baker *Privacy for the real world*)

Bailey F L and Rothblatt H B *Investigation and preparation of criminal cases* 2 ed. (The Lawyers Co-operative Publishing Company New York 1985) (Bailey and Rothblatt *Investigation*)

Bailey F L and Rothblatt H B *Investigation and preparation of criminal cases- federal and state* (The Lawyers Co-operative Publishing Company USA 1970) (Bailey and Rothblatt *Investigation of criminal cases- federal and state*)

Bainbridge D *Intellectual property* 5th ed. (Pearson Education Limited England 2002) (Bainbridge *Intellectual property*)

Barefoot J K *Undercover investigation* 2 ed. (Butterworth London 1983) (Barefoot *Undercover investigation*)

Barnes B *Archbold magistrates' courts criminal practice* 4 ed. (Sweet & Maxwell London 2008) (Barnes *Archbold magistrates' courts criminal practice*)

Basdeo V *A constitutional perspective of police powers of search and seizure in the criminal justice system* (LLM dissertation Unisa 2009) (Basdeo *A constitutional search and seizure*)

Bathia K L and Srivastava S C *Legal method, reasoning and research methodology* (Regal Publications New Delhi 2014) (Bathia and Srivastava *Legal method, reasoning and research methodology*)

Bawa N 'Regulation of the Interception of Communications and Provisions of Communication Related Information Act' in Thorton L et. al. (eds.) *Telecommunication law in South Africa* (STE Publishers South Africa 2006) (Bawa *ROICA*)

Bayuk J *Cyberforensics- Understanding information security investigations* (Springer USA 2010) (Bayuk *Cyberforensics*)

Bennett W W and Hess K M *Management and supervision in law enforcement* (West/Wadsworth Belmont CA 2004) (Bennett and Hess *Management and supervision in law enforcement*)

Bekker P M *Criminal procedure handbook* 9 ed. (Juta South Africa 2009)

Berlatsky N (ed.) *Whistleblowers* (Greenhaven Press New York 2012) (Berlatsky *Whistleblowers*)

Bevan V and Lidstone K *The Investigation of crime- A guide to police powers* (Butterworts London 1991) (Bevan and Lidstone *Investigation-police powers*)

Blackman C and Srivastava L (eds.) *Telecommunication regulation handbook* – Tenth Anniversary Ed. (World Bank and the International Telecommunication Union Washington DC 2011) (Blackman and Srivastava *Telecommunication*)

Block C, Dabdoub M and Fregly S *Crime analysis through computer mapping* (Police Executive Research Forum Washington DC 1995) (Block, Dabdoub and Fregly *Crime analysis through computer mapping*)

Blumberg A J and Eckersley P 'On locational privacy, and how to avoid losing it forever' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Blumberg and Eckersley *Locational privacy*)

Blume P 'Data protection and privacy- Basic concepts in a changing world' in Wahlgren P (ed.) *Information and communication technology* –Scandinavian Studies in Law Vol. 56 at 153 (The Stockholm University Law Faculty Stockholm 2010) (Blume *Data protection and privacy*)

Bonnici J P M *Self-regulation in cyberspace information technology & law series 16* (T.T.C Press The Hague 2008) (Bonnici *Self-regulation in cyberspace*)

Botha S 'Intelligence and democracy in South Africa' issues in Hutton L *To spy or not to spy: Intelligence and democracy in South Africa* Monograph 157 (Institute of Security Studies South Africa 2009) (Botha *Intelligence and democracy in South Africa*)

Botha H and Woolman S 'Limitations' in Chaskalson M et. al. *Constitutional law of South Africa* 2ed. (Juta South Africa 2002) Chapter 36 34.17 - 34.18 (Botha and Woolman 'Limitation')

Braham P *Crimes against the state and crimes against persons - Detective fiction in Cuba and Mexico* (University of Minnesota Press London 2004) (Braham *Crimes against the state and crimes against persons*)

Brierley M 'Telecommunications Technologies' in Thorton L et al (eds) *Telecommunication law in South Africa* (STE Publishers South Africa 2006) (Brierley *Telecommunications technologies*)

Brin D 'The transparent society' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Brin *The transparent society*)

Brown M F *Criminal investigation: Paw and practice* (Butterworth-Heinemann Boston 1998) (Brown *Criminal investigation*)

Brown C V et al. *Managing information technology* 7 ed. (Pearson Boston 2012) (Brown et al. *Managing information technology*)

Brunty J and Helenek K *Social media investigation for law enforcement* (Elsevier: Amsterdam, 2013) (Brunty and Helenek *Social media investigation for law enforcement*)

Burton M 'Doing empirical research – Exploring the decision making of magistrates and juries' in Watkins D and Burton M (eds.) *Research methods in law* (Routledge London 2018) (Burton *Doing empirical research – Exploring the decision making of magistrates and juries*)

Calaca D F *Use of polygraph tests and related evidentiary aspects in labour disputes* (LLM dissertation) (University of Pretoria South Africa 2010) (Calaca *Use of polygraph tests*)

Campbell E, Poh-York L and Tooher J *Legal research materials and methods* (4th ed.) (LBC Information Services Syndey 1996) (Campbell, Poh-York and Tooher *Legal Research Materials and Methods*)

Cape E D *Defending suspects at police stations –The practitioners guide to advice and representation* 5ed. (Legal Action Group London 2006) (Cape *Defending suspects at police stations*)

Caproni V 'Going dark: Lawful electronic surveillance in the face of new technologies' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Caproni *Lawful electronic surveillance*)

Cardwell K et al *The best damn cybercrime and digital forensics book period* (Syngress Publishing Inc. USA 2007) (Cardwell et al *Cybercrime and digital forensics*)

Carr J G *The law of electronic surveillance* 2 ed. (Clark Boardman Company New York 1987) **(**Carr *Electronic surveillance***)**

Carr N 'Tracking is an assault on liberty, with real dangers' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Carr *Tracking is an assault on liberty*)

Casey E *Digital evidence and computer crime – Forensic science, computers and the Internet* 3 ed. (Academic Press USA 2011) (Casey *Digital evidence and computer crime*)

Cassese A *International law* (Oxford University Press Oxford 2005) (Cassese *International law*)

Cassilly J I 'Geolocational Privacy and Surveillance Act' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Cassilly *Geolocational Privacy and Surveillance Act*)

Cassim F *The right to meaningful and informed participation in the criminal process* (LL. D thesis Unisa South Africa 2003) (Cassim *Right to informed participation in the criminal process*)

Cate F H *Privacy in perspective* (AEI Press Washington DC 2001) (Cate *Privacy in perspective*)

Cate F H *Privacy in the information age* **(**Brookings Institution Press Washington DC 1997) (Cate F H *Privacy in the information age*)

McConville M and Chui W H (eds.) 'Introduction and overview' in *Research methods for law* (Edinburg University Press Edinburg 2014) (McConville and Chui (eds.) *Introduction and Overview*)

Chui W H 'Quantitative legal research' in McConville M and Chui W H (eds.) *Research methods for law* (Edinburg University Press Edinburg 2014) (Chui *Quantitative Legal Research*)

Clark F and Diliberto K *Investigating computer crime* (CRC Press USA 1996) (Clark and Diliberto *Investigating computer crime*)

Clermont K M *Standards of decision in Law- Psychological and logical Bases for the standard of proof, here and abroad* (Carolina Academic Press North Carolina 2013)

Clinch P and Beaumont J *Legal research –A practitioners handbook* (2nd ed) (Wildy, Simmonds and Hill Publishing London 2013) (Clinch and Beaumont Legal Research)

Clough J *Principles of cybercrime* (Cambridge University Press Cambridge 2010) (Clough *Principles of cybercrime*)

Cohen S A *Invasion of privacy –police and electronic surveillance in Canada* (The Careswell Company Limited Toronto 1983) (Cohen *Police and electronic surveillance in Canada*)

Collier D W 'Electronic evidence and related matters' in Schwikkard P and Van der Merwe S (eds). *Principles of evidence* 3ed. (Juta South Africa 2008) (Collier *Electronic evidence and related matters*)

Conklin J E *Criminology* 2nd ed. (McMillan U.S.A 1986)

Cook J G *Constitutional rights of the accused pretrial rights* (The Lawyers Co-operative Publishing Company New York 1972) (Cook *Pretrial rights*)

Cook J A *Inside investigative criminal procedure: What matters and why* (Walters Kluwer USA 2012) (Cook *Investigative criminal procedure*)

Cooley T M *Law of torts* 2ed. (Callagan Chicago 1888)

Crawford J *Brownlie Principle of Public International Law* 8th ed. (J Crawford *International Law*) (Oxford University Press Oxford 2012) (Crawford *Public international law*)

Creamer J S *The law of arrest, search and seizure* 3 ed. (Rinehart and Winston USA Holt 1980) (Creamer *Law of arrest, search and seizure*)

Crump C 'On the Geolocational Privacy and Surveillance Act' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Crump *Geolocational Privacy and Surveillance Act*)

Cupido C 'Electronic communications regulations' in Papadopoulos S and Snail S (eds.) *Cyberlaw @ SA 111 – The law of the Internet in South Africa* (Van Schaik Publishers Pretoria 2012) (Cupido *Electronic communications regulations*)

Currie I and De Waal J *The bill of rights handbook* 6 ed. (Juta South Africa 2014) (Currie and De Waal *Rights*)

Daniel L and Daniel L *Digital forensics for legal professionals* (Syngress Boston 2011) (Daniel and Daniel *Digital forensics for legal professionals*)

Dantzker M L *Understanding today's police* (Prentice Hall Education, Career & Technology New Jersey 1995) (Dantzker *Understanding today's police*)

Davis D M "Criminal justice and direction on research in South Africa" in Olmesdahl M C J and Steytler N C *Criminal justice in South Africa* (Juta Cape Town 1983) (Davis *Criminal justice and direction on research*)

Dawson R *Roger Dawson's secrets of power negotiating* (Career Press U.S.A 1995)

Dean T *Network+ guide to networks* (Cambridge Thomson Learning 2000) (Dean *Network + guide to networks*)

De Greef T 'Delegation and responsibility: A human –machine perspective' in Di Nucci E and De Sio F S (eds) *Drones and responsibility- Legal, philosophical and socio-technical perspectives on remotely controlled weapons* (Routledge London 2016)(De Greef *Delegation and Responsibility: A Human –Machine Perspective*)

De Jager J 'Electronic evidence' in Schwikkard P J et al *Principles of evidence* **(**Juta Cape Town 2016**)** (De Jager *Electronic evidence*)

De Klerk K L *The role of the victim in the criminal justice system: A specific focus on victim offender mediation and victim impact statement* (LLM dissertation University of Pretoria 2012) (De Klerk *Role of the victim*)

De Koker L *South African money laundering and terror financing law* (2014) Com7-5 to Com 7-58 (LexisNexis South Africa 2014) (de Koker *Money laundering & terror financing*)

De Sola Pool I and Baeza M L *Safeguarding the first amendment in the telecommunications era technologies of freedom* (Belknap Press of Harvard University Press Cambridge I983) (De Sola Pool and Baeza *Telecommunications era technologies of freedom*)

Devenish G E *A contemporary analysis of South African bill of rights* (Butterworth Durban 1999) (Devenish *Rights*)

De Villiers M *The Roman and Roman-Dutch law of injuries* (Abe Books U.K 1899) (De Villiers *Law of injuries*)

De Villeirs F 'Confidentiality and Journalism' in Oosthuizen G C et al (eds.) *Professional Secrecy in South Africa* (Oxford University Press South Africa 1983) 64 (De Villeirs *Confidentiality and Journalism*)

De Vos P (Ed) *South African constitutional law in context* (Oxford University Press Oxford 2014) (De Vos (Ed) *Constitutional law*)

Dick R C *Legal drafting in plain English* (3rd ed.) (Carswell Thomson Professional Publishing Canada 1995)

Di Nucci E and De Sio F S (eds.) *Drones and responsibility- Legal, philosophical and socio-technical perspectives on remotely controlled weapons* (Routledge London 2016) (Di Nucci and De Sio (eds.) *Drones and responsibility- Remotely controlled weapons*)

Dobinson I and Johns F 'Qualitative legal research' in McConville M and Chui W H (eds) *Research methods for law* (Edinburg University Press Edinburg 2014) (Dobinson and Johns *Qualitative legal research*)

Doherty E P *Digital forensics for handled devices* (CRC Press USA 2013) (Doherty E P *Digital forensics for handled devices*)

Donnelly-Lasarov B *A Philosophy of criminal attempts-The substantive approach* (Cambrdge University Press 2015)

Downing D A, Covington M A and Covington M M *Dictionary of computer and Internet terms* (Barron's Educational Series New York 2000) 243 (Downing, Covington and Covington *Dictionary of computer and Internet terms*)

Dugard J *International Law: A South African perspective* 4th ed. (Juta South Africa 2013) (Dugard *International law: SA*)

Du Plessis M 'International criminal courts, the International Criminal Court, and South Africa's implementation of the Rome statute' in John Dugard *International Law: A South African perspective* 4th ed. (Juta South Africa 2013) (Du Plessis *International Criminal Courts*)

Du Plessis L and De Ville J 'Personal Rights' in Van Wyk D et.al (eds.) *Rights and constitutionalism: The New South African legal order* (Clarendon Oxford 1994) 242 (Du Plessis and De Ville 'Personal Rights')

Du Preez G 'Criminal investigation*'* in J Van der Westhuizen (ed.) *Forensic criminalistics* 2ed. (Heineman Johannesburg 1996) (Du Preez *Criminal Investigation*)

Du Toit D, Van der Waldt G and Stroh E C *Public management - The Grassroot* (Juta Kenwyn Juta 1997) **(**Du Toit, Van der Waldt and Stroh *Public management***)**

Du Toit E et. al. *Commentary on the Criminal Procedure Act revision service 49 2012* (Juta Cape Town 2012) (Du Toit et. al. *Criminal Procedure Act revision*)

Eastman J 'Surveillance of our enemies during wartime? I'm shocked 'in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Eastman *Surveillance of our enemies during wartime*)

Edwards L and Howells G 'Anonymity, consumers and the Internet: where everyone knows you're a dog' in C Nicoll et al. (eds.) *Digital anonymity and the law: tensions and dimensions* (TMC Asser Press The Hague 2003) (Edwards and Howells *Anonymity, consumers and the Internet: where everyone knows you're a dog*)

Ellison N B et al 'Privacy and SNS: An overview' in Trepte S and Reinecke L (eds) *Privacy online- Perspectives on privacy and self-disclosure in the social web* (Springer-Verlag Berlin Heidelberg 2011) 22 (Ellison et al *Privacy and SNS*)

Eiselen S ‘E-Commerce’ in Van der Merwe D et. al. *Information and communication technology law* (Lexis Nexis Durban 2008) (Eiselen *E-Commerce*)

Ernst M L and Schwartz A U *Privacy-The right to be let alone* (MacMillan Company U K 1968) (Ernst and Schwartz *Privacy-The right to be let alone*)

Finkelstein M O and Levin B *Statistics for Lawyers* 2nd ed. (Springer New York 2000) (Finkelstein and Levin *Statistics for lawyers*)

Fowler H W and Fowler F G *The Concise Oxford Dictionary of Current English* (Oxford University Press 1995) 1249

Gabela M *Evaluation of the questions used in polygraph test* (M. Tech dissertation Unisa 2013) (Gabela *Polygraph test*)

Gellman R and Dixon P *Online privacy* (ABC Clio U.S. A 2011)

Govender D *The Nature and extent of problems experienced by detectives in the collection, processing and utilisation of crime information at the Rustenburg detective service* (M Tech. dissertation Unisa 2008) at 1 (Govender *Nature and extent of problems experienced by detectives* 2008)

Greenwald G ‘The digital surveillance state: Vast, secret, and dangerous’ in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Greenwald *Digital surveillance state: vast, secret, and dangerous*)

Greenwald G ‘The surveillance state thrives on fear’ in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Greenwald *The surveillance state thrives on fear*)

Greenwald G ‘U.S. Filmmaker repeatedly detained at border’ in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Greenwald *‘U.S. filmmaker repeatedly detained at border’*)

Fazel I 'Who shall guard the Guards? Civilian operational oversight and the inspector-general of intelligence' in Hutton L (ed.) To spy or not to spy? 157 Monograph (Institute of Security Studies South Africa 2009) (Fazel *Who shall guard the Guards?*)

Federal Bureau of Investigations *Handbook of forensic science* (US Department of Justice US 1994) (Federal Bureau of Investigations *Handbook of forensic science*)

Fitzgerald D G *Informants and undercover investigations- A practical guide to law, policy and procedure* (Taylor and Francis Group USA 2007) (Fitzgerald *Informants and undercover investigations*)

Flaherty D H *Protecting privacy in surveillance societies* (1989) at 8 (University of North Carolina Press U.S.A 1989) (Flaherty *Protecting privacy in surveillance societies*)

Gaines L K and Kappeler V E *Policing in America* (Anderson Pub. Newark 2011) (Gaines L K and Kappeler V E *Policing in America*)

Geldenhuys T and J J Joubert J J (eds.) *Criminal procedure handbook* 2 ed. (Juta South Africa 1996) (Geldenhuys and Joubert (eds.) *Criminal procedure*)

Geomans C and J Dumortier J 'Enforcement issues-Mandatory retention of traffic data in the EU: Possible impact on privacy and online anonymity' in Nicoll C et. al. (eds.) *Digital anonymity and the law: tensions and dimensions* (TMC Asser Press The Hague 2003) (Geomans and Dumortier *Mandatory retention of traffic data in the EU*)

Gereda S L 'Electronic Communications and Transactions Act' in 'Thorton L et al (eds) *Telecommunication Law in South Africa* (STE Publishers South Africa 2006) (Gereda *Electronic Communications and Transactions Act*).

Gilbert J N *Criminal investigation* (Pretice Hall USA 2001) (Gilbert *Criminal investigation I*)

Gilbert J N *Criminal investigation* (Charles E Merrill Publishing Co Columbus 1980) (Gilbert *Criminal investigation 11*)

Gilder B 'Are our intelligence services really that bad?' in Hutton L *To spy or not to spy: Intelligence and democracy in south Africa* (2009) Monograph 157 (Institute of Security Studies South Africa 2009) (Gilder *Are our intelligence services really that bad?*)

Goetz K *An introduction to Internet-based financial investigations –structuring and resourcing the search for hidden assets and information* (Gower UK 2011) (Goetz *Internet-based financial investigations*)

Goodman M *Future crimes: A journey to the dark side of technology - and how to survive it* (Bamtam Press UK 2015) (Goodman *Future crimes: Dark side of technology*)

Gratton E *Internet and wireless privacy- A legal guide to global business practices* (2003) at 299 – 305 (CCH Ltd Canada 2003) (Gratton *Wireless privacy - Guide to global business practices*)

Greenwald G 'The digital surveillance state: Vast, secret, and dangerous' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (*Greenwald Digital surveillance state: Vast, secret, and dangerous*)

Gringras C *The Laws of the Internet* (London Butterworths 1997)

Guiora A N *Constitutional limits on coercive interrogation* (Oxford University Press Oxford 2008) (Guiora *Constitutional limits on coercive interrogation*)

Hamilton C *The Presumption of innocence and Irish criminal law- "Whittling the golden thread"* (Irish Academic Press Dublin 2007) (Hamilton *Presumption of innocence*)

Hance O *Business and Law on the Internet* (New York McGraw-Hill 1996)

Harper J 'It's modern trade: Web users get as much as they give' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Harper *It's modern trade: Web users get as much as they give*)

Heaton-Armstrong A, E Shepherd E and Wolchover D *Analysing witness testimony-A guide for legal practitioners & other professionals* (Blackstone Press Limited London 1999) **(**Heaton-Armstrong, Shepherd and Wolchover *Analysing witness testimony***)**

Hess K M and Wrobleski H M - *Police operations: Theory and practice* 4ed. (Wadsworth/Thomson Learning: Belmont CA 2006) (Hess and Wrobleski *Police operations*)

Hiatt V E *Eavesdropping in Roman comedy* (PhD thesis University of Chicago 1946) **(**Hiatt *Eavesdropping*)

Hiselius P 'ICT/Internet and the right to privacy' in P Wahlgren (ed.) *Information and communication technology- Legal issues Scandinavian studies in law* Vol. *56* (The Stockholm University Law Faculty Stockholm 2010) (Hiselius *ICT/Internet and the right to privacy*)

Hoffman M and Rumsey M *International and foreign legal research: A Course book* (Martinus Nijhoff Publihsers Netherlands 2008) (Hoffman and Rumsey *International and Foreign Legal Research*)

Hofmann L L H *The South African law of evidence* 4 ed. (Butterworths South Africa 1988) (Hofmann *Evidence*)

Hofstee E *Constructing a good dissertation – A practical guide to finishing a masters, mba or phd on schedule* (EPE South Africa 2006) (Hofstee *Constructing a good dissertation*)

Hogarth J *Sentencing as a human process* (University of Toronto Canada 1971)

Stockdale E and Devlin K *Sentencing* (Waterlow Publishers London 1987)

Home Office *Police and Criminal Evidence Act 1984 (s 66) –Codes of practice* (Crown Copyright London 1986) (Home Office *Police and Criminal Evidence Act 1984*)

Horswell J *The practice of crime scene investigation* (CRC Washington D.C. 2004) (Horswell *Crime scene investigation*)

Hubbard R W, Brauti P M and Fenton S K *Wiretapping and other electronic surveillance: Law and procedure* – Vol. 1 (Canada Law Book Toronto 2013) (Hubbard, Brauti and Fenton *Wiretapping*)

Hufnagel S *Police cooperation across borders- Comparative perspectives on law enforcement within the EU and Australia* (Ashgate Publishing USA 2013) (Hufnagel *Police cooperation across borders*)

Hutchinson T 'Doctrinal research' in Watkins D and Burton M (eds.) *Research methods in law* (Routledge United Kingdom 2018) 8 (Hutchinson *Doctrinal research*).

Hutton L (ed.) 'Secrets, spies and security: An overview of the issues' in Hutton L *To spy or not to spy: Intelligence and democracy in South Africa* Monograph 157 (Institute of Security Studies South Africa 2009) (Hutton (ed.) *Secrets, spies and security*)

Ibidapo-Obe A and Nwankwo C *The bail process and human rights in Nigeria* (Constitutional Rights Project Nigeria 1992) (Ibidapo-Obe and Nwankwo *The bail process in Nigeria*)

Jackson J D and Summers S J *The Internationalization of criminal evidence- Beyond the common law and civil law traditions* (Cambridge University Press Cambridge 2012) (Jackson and Summers *The internationalization of criminal evidence*)

Jaiswal J *Human rights of accused and juveniles –Delinquent in conflict with law* (Kalpaz Publications Delhi 2005) (Jaiswal *Human rights of accused and juveniles*)

Jarrett M H and Bailie M W *Prosecuting computer crimes* (Office of Legal Education Executive Office for United States Attorneys USA 2007) (Jarrett and Bailie *Prosecuting computer crimes*)

Jimenez A (ed.) A *Privacy- An overview of federal law governing wiretapping and electronic eavesdropping* (Nova Science Publishers Inc. New York 2010) ('Jimenez (ed.) *Wiretapping'*)

Joubert J J (ed.) *Criminal procedure handbook* 3 ed. (South Africa Juta 1998) (Joubert (ed.) *Criminal procedure*)

Joubert W A *Grondslae van die Personoonlikheidsreg* (LL.D thesis Univesrity of Stellebosh 1953)15 (Joubert *Personoonlikheidsreg*)

Kapoor H L *Police investigation and procedure* (Ess Ess Publications New Delhi 1989) (Kapoor *Police investigation and procedure*)

kasrils R 'To spy or not to spy? Intelligence and democracy in South Africa issues' in Hutton L *To spy or not to spy: Intelligence and democracy in South Africa* Monograph 157 (Institute of Security Studies South Africa 2009) (kasrils *To spy or not to spy*)

Keeton W P et al. *Prosser and Keeton on the Law of torts* 5 ed. (West Group U.S.A. 1984) 866 - 7 (Keeton et al. *Law of Torts*)

Kisoon C 'PAIA and public participation in Hutton L *To spy or not to spy: Intelligence and democracy in South Africa* Monograph 157 (Institute of Security Studies South Africa 2009) (Kisoon *PAIA and public participation*)

Kemp G et. al. *Criminal law in South Africa* 2nd ed. (2015) (G Kemp et al. *Criminal Law* (Oxford University Press South Africa 2015) (Kemp et. al. *Criminal law*)

Kemp G P, Terblanche S S and Watney M M *Criminal procedure casebook* (Juta Claremont 2010) (Kemp, Terblanche and Watney *Criminal procedure*)

Khera F Y 'Laptop searches and other violations of privacy faced by Americans returning from overseas travel' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Khera *Laptop searches and overseas travel*)

Kipper G *Wireless crime and forensic investigation* (Taylor & Francis Group New York 2007) (Kipper *Wireless crime and forensic investigation*)

Klamberg M 'FRA and the European convention on human Rights - A Paradigm shift in Swedish electronic surveillance law' in D W Schartaum (ed.) in *Overvåking i en rettstat* in the series Nordisk årbok i rettsinformatikk (Nordic Yearbook of Law and Information Technology Stockholm 2010) (Klamberg *Swedish electronic surveillance law*)

Koops B J and Brenner S W (eds.) *Cybercrime and jurisdiction- a Global survey* (T.M.C Asser Press Hague 2006) (Koops and Brenner (eds.) *Cybercrime and jurisdiction*)

Kosseff J *Cybersecurity law* (John Wiley U.S.A 2017) (Kosseff *Cybersecurity Law*)

Kruger A *Organised crime and proceeds of crime Law in South Africa* (A Kruger *Organised Crime*) (LexisNexis South Africa 2008) (Kruger *Organised crime and proceeds of crime*)

LaFave W R *Search and seizure- A Treatise on the Fourth Amendment Vol. 5*(St Paul Minn-West Publishing Co USA 1996) (LaFave *Search and seizure*)

Landever A R *Electronic Surveillance and the American constitutional system* (PhD thesis New York University New York 1969) (Landever A R *Electronic Surveillance and the American Constitutional System*)

Landau S 'Going dark: Lawful electronic surveillance in the face of new technologies' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Landau *Lawful electronic surveillance in the face of new technologies*)

Larsson C "Telecom operator's incident investigations" in P Wahlgren (ed.) *Information and communication technology- Legal issues Scandinavian studies in law Vol.56* (The Stockholm University Law Faculty Stockholm 2010) (Larsson *Telecom operator's incident investigations*)

Lee LC and Davidson JS *Intellectual property for the Internet* (New York Wiley Law Publications 1997) (Lee and Davidson *Intellectual property for the Internet*)

Lehman BA "Intellectual property and the national information infrastructure: Report of the working group on intellectual property rights" in Perrit Jr H *Law and the Information Superhighway: Privacy, access, intellectual property, commerce and liability* (New York Wiley Law Publications 1996) (Lehman *Intellectual property and the national and global information infrastructure*)

Levi M *Regulating fraud –White-collar crime and the criminal process* (Tavistock Publications London 1987) (Levi *Regulating fraud –White-collar crime and the criminal process*)

Lindberg A and Svensson D 'IT law from a practitioner's perspective' in Wahlgren P (ed.) *Information and communication technology- Legal issues* Vol. 56 (Stockholm Institute for Law Sweden 2010) 12- 23 (Lindberg and Svensson *IT law from a practitioner's perspective*)

Lim Y F *Cyberspace law- Commentaries and materials* 2 ed. (Oxford University Press Oxford 2007) (Lim *Cyberspace law*)

Lippman M *Criminal procedure* 2ed. (SAGE Publications U.S.A 2014) (Lippman *Criminal procedure*)

Lo A H *Excluding evidence obtained through illegal electronic surveillance: A comparison between the U.S. and Canada* (LL.M thesis University of Toronto 2005) (Lo *Excluding evidence obtained through illegal electronic surveillance: A comparison between the U.S. and Canada*)

Lomio J P and Span-Hanssen H S *Legal research methods in the U.S. & Europe* 2nd ed. (DJOF Publishing Denmark 2009) (Lomio and Span-Hanssen Legal Research Methods in the U.S. & Europe)

Lomio J P, Span-Hanssen H S and Wilson G D *Legal research methods in a modern world: A course book* (DJOF Publishing Denmark 2011) (Lomio, Span-Hanssen and Wilson *Legal research methods in a modern world*)

Loubser M *et. al*. *The law of delict in South Africa* 2nd ed. (Oxford University Press South Africa 2012) (Loubser *et. al*. *Delict*)

Madrigal A 'I'm being followed: How Google-and 104 other companies- Are tracking me on the web' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Madrigal *I'm being followed: How Google-and 104 other companies- Are tracking me on the web*)

Marcella A Jr. and D Menendez D *Cyber forensics –A field of manual for collecting, examining and preserving evidence of computer crimes* (2ed.) (Auerbach Publications USA 2008) (Marcella Jr. and Menendez *Cyber forensics – Collecting, examining and preserving evidence of computer crimes*)

Marnewick C *Mediation practice in the Magistrates' Courts* (LexisNexis South Africa 2015) (Marnewick *Mediation in the Magistrates' Courts*)

Meehan E and Currie J H *The law of criminal attempt* 2 ed. (Carswell Toronto 2000)

Mokgosi L 'The telecommunications regulators' in Thorton L et. al. (eds.) *Telecommunication law in South Africa* (STE Publishers South Africa 2006) (Mokgosi *The Telecommunications Regulators*)

Mokgosi L 'The telecommunications regulators' in Thorton L et. al. (eds.) *Telecommunication law in South Africa* (STE Publishers South Africa 2006) (Mokgosi *The telecommunications regulators*)

Mathews S A 'State Secrecy' in G C Oosthuizen et al (eds.) *Professional secrecy in South Africa* (Oxford University Press South Africa 1983) (Mathews *State secrecy*)

McAuliffe J *Criminal investigations: A scenario-based text for police recruits and officers* (Prentice Hall New Jersey 2002) (McAuliffe *Criminal investigations*)

Moodley D *The perceptions of Crime Intelligence manager's on the organizational structure of the Crime Intelligence Division of the South African Police Service* (MBA dissertation UKZN 2006)

Moster D *Utilisation of the Financial Intelligence Centre as a crime intelligence source* (M. Tech. dissertation Unisa 2012)

Pendleton M 'Non-empirical discovery in legal scholasrhsip- Choosing, researching and writing a traditional scholarly article' in McConville M and Chui W H (eds) *Research methods for law* (Edinburg University Press Edinburg 2014) (Pendleton *Non-empirical discovery in legal scholasrhsip- Choosing, researching and writing a traditional scholarly article*)

McCullagh D 'FBI: we need wiretap-ready websites- Now' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (McCullagh *FBI: we need wiretap-ready websites- Now*)

Mokgosi L 'The telecommunications regulators' in Thorton L et. al. (eds.) *Telecommunication law in South Africa* (STE Publishers South Africa 2006) (Mokgosi *The telecommunications regulators*)

McQuoid-Mason D 'Privacy' in Woolman et.al. *Constitutional law of South Africa* 2nd ed. *Revision service 5* (Juta South Africa 2013) (McQuoid-Mason 'Privacy II')

McQuoid-Mason D J *The law of privacy in South Africa* (Juta & Company Ltd South Africa 1978) (McQuoid-Mason *Privacy I*')

Meintjes-van der Walt L 'Electronic evidence' in Papadopoulos S & Snail S (eds.) *Cyberlaw @ SA 111 – The law of the Internet in South Africa* (Van Schaik Publishers Pretoria 2012) (Meintjes-van der Walt *Electronic evidence*)

Miettinen S *Criminal law and policy in the European Union* (Routledge London 2013)

Milne S and Tucker K *A practical guide to legal research* (2nd ed.) (Thomas Reuters (Professional) Australia Limited Australia 2010) (Milne and Tucker *A practical guide to legal research*)

Minnaar A 'The difficulties of implementing cybersecurity measures as a foundational preventive cyberterrorism measure' in Plywaczewki E (ed.) *Current problems of the penal law and criminology* 6th ed. (Bialystok Poland 2014)

Mokwena R J *The value of photography in the investigation of crime scenes* at ii, 2, 47 and 72 -73 (M.Tech dissertation Unisa 2012) (Mokwena *Value of photography in the investigation of crime scenes*)

Montesh M *A Critical analysis of crime investigative system within the South African criminal justice system: A comparative study* (PhD thesis Unisa 2007) (Montesh *Crime investigative system*)

Moodley D *The perceptions of crime intelligence manager's on the organisational structure of the Crime Intelligence Division of the South African Police Service* (MBA dissertation University of Kwazulu-Natal 2006) (Moodley *Perceptions of crime intelligence manager's on the organisational structure of the Crime Intelligence Division*)

Moore M 'Critique of the protection of information bill' in Hutton L *To spy or not to spy: Intelligence and democracy in South Africa* Monograph 157 (Institute of Security Studies South Africa 2009) (Moore 'Critique of the protection of information bill'')

More H W and Miller L S *Effective police supervision* 6th ed. (Anderson publishing USA 2011) (More and Miller *Effective police supervision*)

Morgan D and Stephenson G (eds.) *Suspicion and silence- The right to silence in criminal investigations* (Blackstone Press Limited Britain 1994) (Morgan and Stephenson (eds.) *Suspicion and silence*)

Mostert H and Badenhorst P J 'Property and the Bill of Rights' in Butterworth's *Bill of Rights Compendium* (Issue 18) (2006) 3FB3 (LexisNexis South Africa 2006)

Msimang M 'Universal service and universal access' in 'Thorton L et al (eds.) *Telecommunication law in South Africa* (STE Publishers South Africa 2006) (Msimang *Universal service and universal access*)

Mudaly L *Search and seizure of documents in the investigation of tax-related cases* (M. Tech dissertation Unisa 2011)

Muir J A and Van Oorschot P C 'Internet geo-location and evasion (Ottawa School of Computer Science Carleton University 2006)

Muller V C 'Autonomous killer robots are probably good news' in Di Nucci E and De Sio F S (eds) *Drones and responsibility- Legal, philosophical and socio-technical perspectives on remotely controlled weapons* (Routledge London 2016) (Muller *Autonomous killer robots are probably good news*)

Murphy P *A practical approach to evidence* (Blackstone Press Limited UK 1980) (Murphy *Practical approach to evidence*)

Nagel S S *Microcomputers as decision aids in law practice* (Quorum Books New York 1987) **(**Nagel *Microcomputers as decision aids in law practice***)**

Nagy R L *Through the public/private lens: Reconciliation, responsibility and democratization in South Africa* at 132 – 178 (PhD thesis University of Toronto 2003) (Nagy *Through the public/private lens: Reconciliation, responsibility and democratization in South Africa*)

Neethling J *Die Reg op Privaatheid* (Unisa Pretoria 1976) 23 (Neethling *Privaatheid*)

Neethling J 'Legal Protection of Personal Data' in *Neethling's Law of Personality* 267-269 (NexisLexis South Africa 2005) (Neethling 'Legal Protection of Personal Data')

Neethling J, Potgieter J M and Visser P J *Neethling's law of personality* (Butterworths Durban 1996) (Neethling, Potgieter and Visser *Neethling's Law of personality*)

Neethling J, Potgieter J M and Visser P J *Law of delict* (Butterworths Durban 1995) (Neethling, Potgieter and Visser *Delict*)

Neethling J J, Potgieter J M and Visser P J 2nd ed. *Law of delict* (Butterworths Durban 1994) (Neethling J J, Potgieter J M and Visser *Delict*)

Neethling J, Potgieter J and Visser P J *Neethling's law of personality* 2nd ed. (2005) (LexisNexis Durban 2005) (Neethling, Potgieter and Visser *Neethling's law of personality*)

Nel S 'Freedom of expression, anonymity and the Internet' in Papadopoulos S & Snail S *Cyberlaw @ SA 111- The law of the Internet in South Africa* (2012) at 255 (Van Schaik Pretoria 2012) (Nel *Internet*)

Newton H *Newtons' Telecom Dictionary* 22nd ed. (CMP United States 2006)

Ngomane A R *The use of electronic evidence in forensic investigation* (M. Tech thesis Unisa 2010) (Ngomane *Electronic evidence in forensic investigation*)

Nielsen S R *Electronic surveillance: Law enforcements need for a state wiretap statute in California* (Msters thesis California State University 1985) (Nielsen *Electronic surveillance in California*)

Onions C T (ed) *The shorter of Oxford English dictionary* (Clarendon Press Oxford 1933) 1586

Online Investigation Working Group *Online investigative principles for federal law enforcement agencies* (United States Government US 1999) (*Online investigative principles*)

O'Day A (ed.) *Cyberterrorism* (Ashgate USA 2004) **(**O'Day (ed.) *Cyberterrorism***)**

O' Hara C E and O' Hara G L *Fundamentals of criminal investigation* 7ed. (Charles C Thomas Publishers Ltd USA 2003) (O' Hara and O' Hara *Criminal investigation*)

Ortmeier P J *Policing the community: A guide for patrol operations* (Prentice Hall Upper Saddle River N.J. 2002) (Ortmeier *Policing the community: Patrol operations*)

Oosthuizen G C et al (eds.) *Professional secrecy in South Africa* (Oxford University Press South Africa 1983)

Osula A *Remote search and seizure of extraterritorial data* (PhD thesis University of Tartu 2017) (Osula *Remote search and seizure of extraterritorial data*)

Palmiotto M J *Criminal investigations* (Austin & Winfield San Francisco Calif. 1998) (Palmiotto *Criminal investigations*)

Pandya N D *Illegally obtained evidence* (Unisa South Africa 1986**) (**Pandya *Illegally obtained evidence***)**

Papadopoulos S 'An introduction to Cyberlaw' in Papadopoulos S & Snail S (eds.) *Cyberlaw @ SA 111 – The law of the Internet in South Africa* (Van Schaik Publishers Pretoria 2012) (Papadopoulos *Cyberlaw*)

Papadopoulos S and Snail S 'Privacy and data protection' in Papadopoulos S and Snail S (eds.) *Cyberlaw @ SA 111 – The law of the Internet in South Africa* (Van Schaik Publishers Pretoria 2012) (Papadopoulos and Snail *Privacy and data protection*)

Pakendorf H 'The journalist and his sources' in Oosthuizen G C et al (eds.) *Professional secrecy in South Africa* (Oxford University Press South Africa 1983) 71 (Pakendorf '*The journalist and his sources*')

Pistorius T "Copyright law and IT" in Van der Merwe D et al *Information and communications technology law* (LexisNexis South Africa 2008)

Plaatjies M F *A model for implementation of restorative justice in the South African correctional system* at 106-137 (PhD thesis Unisa 2008) (Plaatjies *Restorative justice*)

Police Executive Research Forum 'Cameras' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Police Executive Research Forum 'Cameras')

Pollock D A *Aspects of electronic audio surveillance* (PhD thesis University of California 1972) (Pollock *Electronic audio surveillance*)

Popoola O O *Statutory limitation of the liability of Internet service providers in decentralized peer to peer file sharing* (LL.M thesis Unisa 2012) (Popoola *Liability of ISPs*)

Posner R A *The Economics of justice* (Harvard University Press Cambridge 1981)

Posner R A *Economic analysis of law* 5 ed. (Aspen Law and Business USA 1998)

Price M E and Verhulst S G *Self-regulation and the Internet* (Kluwer Law International The Hague 2005) (Price and Verhulst *Self-regulation and the Internet*)

Radcliffe J and Bailey E *The New International Webster's Pocket Dictionary of the English language* (new rev ed.) (Trident Press International U.S.A1998)

Rapp D 'Privacy vs. security" Are you prepared for the thorny issues surrounding student surveillance?' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Rapp *Privacy vs. security - student surveillance*)

Rautenbach I M 'Introduction to the bill of rights' in LexisNexis *Bill of rights compendium* (LexisNexis South Africa 2008) (Rautenbach *Introduction to the Bill of Rights*)

Reed C *Making laws for cyberspace* (Oxford University Press Oxford 2012) (Reed *Cyberspace*)

Reed C *Internet law: Text and materials* 2nd ed. (2004) 106 (Cambridge University Press London 2004) ((Reed *Internet law: Text and materials*)

Reiman J H Privacy, intimacy and personhood in Schoeman F D (ed.) *Philosophical dimensions of privacy* (1984) 300 and 314 (J H Reimah 'Privacy, intimacy and personhood') (Cambridge University Press U.K 1984) (Reiman *Privacy, intimacy and personhood*)

Ringel W E *Searches and seizure-arrest and confessions* (Clark Boardman Company New York 1974) (Ringel *Searches and seizure-arrest and confessions*)

Robertson C, Das D K and J K Singer J K (eds.) *Police without borders- The fading distinction between local and global* (CRC Press USA 2010) (Robertson, Das and Singer (eds.) *Police without borders*)

Rogers C et al *Police work: Principles and practice* **(**Routledge New York 2011) (Rogers et. al. *Police work: Principles and practice*)

Rogers C and Lewis R (eds.) *An introduction to police work* (Willan Cullompton 2007) (Rogers and Lewis eds. *Introduction to police work*)

Roos A 'Data protection' in D Van der Merwe et al *Information and communications technology law* (Lexis Nexis Durban 2008) (Roos *Data protection*)

Rooyen HJN *Investigate corruption* (HJN Training South Africa 2013) (Rooyen *Investigate corruption*)

Rosenzweig P 'The sky isn't falling' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Rosenzweig *The sky isn't falling*)

Roux T 'Property' in Woolman *et al* (eds.) *Constitutional Law of South Africa* 2nd ed. *Revision Service 5* (Juta South Africa 2013) 46.3(b))

Ruan K *Cybercrime and cloud forensics: Applications for investigation processes* (IGI Global USA 2013) (Ruan *Cybercrime and cloud forensics: Applications for investigation processes*)

Rudestine D *The day the presses stopped: A history of the Pentagon papers case* – (University of California Press California 1996) (Rudestine *The day the presses stopped*)

Ruiz B R *Privacy in telecommunications –A European and an American approach* (1997) at 64 - 66 (Kluwer Law International Hague 1997**) (**Ruiz *Privacy in telecommunications***)**

Ryngaert C *Jurisdiction in international law* (2nd ed.) (Oxford University Press Oxford 2015)

Sales N A 'Laptop searches and other violations of privacy faced by Americans returning from overseas travel' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Sales *Laptop searches and overseas travel*)

Samar C J *The right to privacy –Gays, lesbians and the constitution* at (1991) 18 (Temple University Press Philadelphia 1991) (Samar *Right to privacy –Gays, lesbians*)

Sammons J and Rajewski J *The basics of digital forensics: The primer for getting started in digital forensics* (Elsevier/Syngress Waltham MA 2012) (Sammons and Rajewski *Digital forensics*)

Sangha B, K Roach K and Moles R *Forensic investigations and miscarriage of justice- The rhetoric meets the reality* (Irwin Law Inc. Toronto 2010) at 191 (Sangha, Roach and Moles *Forensic investigations*)

Savona E (ed.) *Crime and technology –New frontiers for regulation, law enforcement and research* (Springer Netherlands 2004) (Savona (ed.) *Crime and technology*)

Schmitt M N (ed.), *Tallinn manual on the international law applicable to cyber Warfare* (Cambridge University Press 2013) 16

Schuster J F *Electronic eavesdropping and the fourth amendment* (PhD thesis) (Pennsylvania State University US 1965) (Schuster *Electronic eavesdropping*)

Schmalleger F *Criminal justice today: an introductory text for the 21st century* 3rd ed. (Englewood Cliffs U.S.A 1995)

Schmitt M N (ed.), *Tallinn manual on the international law applicable to cyber warfare* (Campbridge University Press Cambrideg 2013)

Schwikkard P J 'Arrested, detained and accused persons' in Currie I and De Waal J *The bill of rights handbook* (Juta Cape South Africa Town 2014) (Schwikkard 'Arrested, detained and accused persons')

Schwikkard P J *Presumption of innocence* (Juta and Co South Africa 1999) (Schwikkard *Presumption of innocence*)

Schwikkard P J 'Private privilege' in Schwikkard P J and Van Der Merwe *Principles of evidence* (Juta South Africz 2016)

Schwikkard P J and Van der Merwe S E 'The standard and burden of proof of evidential duties in criminal trials' in Schwikkard P J and van der Merwe S E *Principles of evidence* 4th ed. (Juta South Africa 2016) (Schwikkard and van der Merwe *Standard and burden of proof*)

Scoglio S *Transforming Privacy - A transpersonal philosophy of rights* (Praeger Publishers U.S.A 1998) 1

Scott J D *Investigative methods* (Reston Publishing Company Inc. USA 1978) (Scott *investigative methods*)

Sefanyetso J T *Personal description: An investigation technique to identify suspects* (M Tech thesis Unisa 2009) (Sefanyetso *An investigation technique to identify suspects*)

Sennewald C A and Tsukayama J K *Process of investigation: Concepts and strategies for investigators in the private sector.* 3ed. (Butterworth-Heinemann Oxford UK 2006) (Sennewald and Tsukayama *Concepts and strategies for investigators in the private sector*)

Shapiro B J *Beyond reasonable doubt and probable cause: Historical perspectives on the Anglo-American law of evidence* (University of California Press USA 1991) (Shapiro *Beyond reasonable doubt and probable cause*)

Shaw M N *International law* 6th ed. 646 (Cambrideg University Press Cambridge 2008) (Shaw *International law*)

Shur E M *Crimes without victims: deviant behaviour and public policy* 169 (1965)

Smith G J H *Internet law and regulation* (Sweet & Maxwell London 2002) (Smith *Internet law*)

Snail S and Papadopoulos S 'Privacy and data protection' in Van der Merwe D et al *Information communications and technology law* (Lexis Nexis Durban 2008) (Snail and Papadoulos *Privacy and data protection*)

Sloan I J *Law of Privacy in a technological society* (Oceana Publications U.S.A.1986) 61 (Sloan *Privacy in a technological society*)

Sole S 'To spy or not to spy? Intelligence in a democratic South Africa in Hutton L *To spy or not to spy: Intelligence and democracy in South Africa* Monograph 157 (Institute of Security Studies South Africa 2009) (Sole *To spy or not to spy? Intelligence in a democratic South Africa*)

Solove D J *Understanding privacy* (Harvard University Press Cambridge 2008) 102 (Solove *'Privacy'*)

Starmer k and Christou T A *Human rights manual and sourcebook for Africa* (British Institute of International and Comparative Law London 2005) (Starmer and Christou *Human rights*)

Stephenson P *Investigating computer-related crime* (CRC Press USA 2000) (Stephenson *Investigating computer-related crime*)

Stevens G and C Doyle *Privacy: wiretapping and electronic eavesdropping* (Novinka Books New York 2002) (Stevens and Doyle *Privacy: wiretapping and electronic eavesdropping*)

Stone R *The law of entry, search and seizure* 4 ed. (Oxford University Press Oxford 2005) (Stone *The law of entry, search and seizure*)

Strauss S A ‘Legal professional privilege’ in Oosthuizen G C et al (eds.) *Professional secrecy in South Africa* (Oxford University Press South Africa 1983) 26 (Strauss *Legal professional privilege*)

Strijdom H G ‘Factors influencing a victim’s a decision to report an offence ‘in Olmesdahl M C J and Steytler N C *Criminal justice in South Africa* (Juta 1983 Cape Town) (Strijdom *Factors influencing a victim’s a decision to report an offence*)

Stumer A *The presumption of innocence- Evidential and human rights perspectives* (Harp Publishing Oxford 2010) (Stumer *The presumption of innocence*)

Suping U et. al. ‘Convergence’ in Thornton L et. al. (eds.) *Telecommunications law in South Africa* (2006) (STE Publishers Johannesburg 2006) (Suping et. al. *Convergence*)

Swanson C R *Criminal investigation* (McGraw-Hill USA 1996) (Swanson *Criminal investigation*)

Swanson C R, Chamelin N C and Territo L *Criminal investigation* 8ed. (McCraw-Hill Boston 2003) (Swanson, Chamelin and Territo *Criminal investigation*)

Swanson C R *Investigators, the investigative process, and the crime scene- Chapter overview* 8ed. (2002) (McGraw USA 2002) (Swanson *Investigators, the investigative process, and the crime scene*)

Swire P P and Ahmad K (eds.) ‘Introduction’ in Swire P P and Ahmad K *Privacy and surveillance with new technologies* (International Debate Education Association New York 2012) (Swire and Ahmad (eds.) *Introduction*)

Swire P P and Ahmad K (eds.) ‘Part 4: Backdoor surveillance’ in Swire P P and Ahmad K *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) (Swire and Ahmad (eds.) *Part 4: Backdoor surveillance*)

Swire P P and Ahmad K (eds.) 'Part 5: Locational Tracking' in *Privacy and surveillance with new technologies* (International Debate Education Association New York 2012) (Swire and Ahmad (eds.) *Part 5: Locational Tracking*)

Swire P P and Ahmad K (eds.) 'Part 6: Online Privacy' in Swire P P and Ahmad K *Privacy and surveillance with new technologies* (International Debate Education Association U.S. 2012) 329-330 (Swire and Ahmad (eds.) *Part 6: Online Privacy*)

Swire P and Ahmad K (eds.) '''Going dark'' versus a ''Golden age for surveillance''' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association New York 2012) (Swire and Ahmad *Going dark v Golden age for surveillance*)

The Economist 'Economist debates: online privacy' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association New York 2012) (The Economist *Online privacy*)

The Economist 'Learning to live with big brother' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association New York 2012) (The Economist *Learning to live with big brother*)

Thompson R M II '*United States v Jones*: GPS monitoring, property, and privacy' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association New York 2012) (Thompson *GPS monitoring*)

Taslitz A E and M L Paris *Constitutional criminal procedure* 2 ed. (Foundation Press New York 2003) (Taslitz and Paris *Constitutional criminal procedure*)

Thaman S C *Comparative criminal procedure: A casebook approach* (Academic Press Carolina 2002) (Thaman *Comparative criminal procedure: A casebook approach*)

Thorton L et. al. (eds.) *Telecommunication law in South Africa* (STE Publishers Johannesburg 2006) (Thorton et. al. (eds.) *Telecommunication law*)

Thorton L 'Telecommunication law –An Overview' in Thorton L et al (eds) *Telecommunication law in South Africa* (STE Publishers South Africa 2006) (Thorton *Telecommunication Law*)

United Nations Office on Drugs and Crime *Handbook on police accountability, oversight and integrity* (United Nations Publications New York 2011) (United Nations Office on Drugs and Crime *Handbook on police accountability, oversight and integrity*)

U.S. Department of Justice *Electronic crime scene investigation – A Guide for first responders* (U.S Department of Justice Washinton 2001)

Vadackumchery J *Crime law and police science* (Concept Publishing Company New Delhi 2003) (Vadackumchery *Crime law and police science*)

Vagias M *The territorial jurisdiction of the International Criminal Court* (2014) (Oxford University Press Oxford 2014)

Van der Berg E and Van der Merwe S E 'Opinion evidence' in Schwikkard P J and Van der Merwe S E *Principles of evidence* 3rd ed. (Juta South Africa 2009)

Van der Merwe D 'Criminal law' in Van der Merwe D, A Roos and T Pistorius (eds.) *Information communications and technology law* (2008) (Lexis Nexis Durban 2008) (Van der Merwe 'Criminal law')

Van der Merwe D 'Introduction' in van der Merwe D, A Roos and T Pistorius (eds.) *Information communications and technology law* (2008) at 1(Lexis Nexis Durban 2008) (Van der Merwe 'Introduction')

Van der Merwe D 'Telecommunication law' in Van der Merwe D, A Roos and T Pistorius (eds.) *Information communications and technology law* (2008) (Lexis Nexis Durban 2008) (Van der Merwe 'Telecommunication law')

Van der Merwe D 'The law of ICT evidence' in Van der Merwe D, A Roos and T Pistorius (eds.) *Information communications and technology law* (2008) at 1(Lexis Nexis Durban 2008) (Van der Merwe 'The law of ICT evidence')

Van der Merwe S E 'Unconstitutionally obtained evidence' in Schwikkard P J and Van der Merwe S E *Principles of evidence* 4th ed. (Van der Merwe S E 'Unconstitutionally obtained evidence' (Juta South Africa 2016) (Van der Merwe *Unconstitutionally obtained evidence*)

Van der Vyver J D 'State secrecy' in G C Oosthuizen et al (eds.) *Professional secrecy in South Africa* (Oxford University Press South Africa 1983)

Van der Westhuizen J, *Forensic criminalistic.* 2nd ed. (Heinemann Johannesburg 1996) (Van der Westhuizen *Forensic criminalistic*)

Van der Walt J C & Midgley J R *Delict- Principles and Cases: Volume 1: Principles* 2nd ed. (Butterworths Durban 1997) 32(Van der Walt & Midgley *Delict- Vol 1: Principles*)

Van der Walt A J *The Constitutional Property Clause:* A comparative analysis of Section 25 of the South Africa constitution of 1996 (Juta Kenwyn 1997)

Van der Wusthuizen J *An introduction to criminological research: study manual series No 7* (Unisa South Africa 1996) (Van der Wusthuizen *Introduction to criminological research*)

Van Eeden E *Consumer protection law in South Africa* (Lexis Nexis South Africa 2013) (Van Eeden *Consumer protection law*)

Van Gerven D 'Professional secrecy in Europe' in the bar of the Brussels *Professional Secrecy of Lawyers in Europe* (Cambridge University Press U K 2013)

Van Heerden T J *Introduction to police science* (Unisa South Africa 1986) (Van Heerden *Police science*)

Van Jaarsveld S R 'Agency' in Nagel C J (ed.) Commercial law 3ed (Lexis Nexis Butterworths South Africa 2006) (Van Jaarsveld *Agency*)

Van Niekerk A *The analysis of a cell phone record as a source of intelligence in the investigation of copper cable* (M Tech dissertation Unisa 2015) (Van Niekerk *The analysis of a cell phone record as a source of intelligence*)

Van Rooyen H J N *The A-Z of investigation: A practical guide for private and corporate investigators* (Crime Solve Pretoria 2004) (Van Rooyen *The A-Z of investigation*)

Van Rooyen H J N *Crime scene investigation* (HJN Training South Africa 2007) (Van Rooyen *Crime scene investigation*)

Vlahos J 'Surveillance society: New high-tech cameras are watching you' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association New York 2012) (Vlahos *Surveillance society: New high-tech cameras are watching you*)

Von Solms S H and Eloff J H P *Information security* (University of Johannesburg and University of Pretoria South Africa 2004)

Waggoner K and Suchma K H (eds.) *Handbook of forensic services* (FBI Laboratory Publication Virginia 2007) (Waggoner and Suchma (eds.) *Forensic services*)

Walsh A and C Hemmens C (eds) *Introduction to criminology: A Text /Reader* (Thousand Oaks U.S. A 2008)

Watkins D and Burton M (eds) *Research methods in law* (2nd ed) (Routledge London 2018) (Watkins and Burton (eds) *Research methods in law*)

Watney M 'Cybercrime and the investigation of crime' in Papadopoulos S and Snail S (eds.) *Cyberlaw @ SA 111- The law of the Internet in South Africa* (Van Schaik Pretoria 2012) (Watney *Cybercrime and investigation*)

Weber R H and Weber R *Internet of things –Legal perspectives* (2010) (Springer London 2010) (Weber and Weber *Internet of things –Legal perspectives*)

Westerman P C ‘Open or Autonomous? The Debate on Legal Methodology as a Reflection of the Debate on Law’ in Van Hoecke M *Methodologies of legal research- What kind of methods for what kind of discipline?* (Hart Publishing Oxford 2013) (Westerman *Open or autonomous? The debate on legal methodology as a reflection of the debate on law*)

Weir G and Mason S ‘The sources of digital evidence’ in Mason S (ed.) *Electronic evidence* 3 ed. (Harvard U.S. 2012) (Weir and Mason *The sources of digital evidence*)

Walden I *Computer crimes and digital investigations* (Oxford University Press Oxford 2007) (Walden *Computer crimes and digital investigations*)

Watt D *Law of Electronic surveillance in Canada first supplement* (The Carswell Company Limited Toronto 1983) (Watt *Law of electronic surveillance in Canada*)

Westin A *Privacy and freedom* (1967) 487 (Atheneum New York 1967) (Westin *Privacy and freedom*)

Wennerstrom E O and Sandberg C ‘Combating cybercrime – Developments in the European union’ in Wahlgren P (ed) *Information and Communication Technology- Legal Issues Scandinavian Studies in Law* Volume 56 (The Stockholm University Law Faculty Stockholm 2010) (Wennerstrom and Sandberg ‘Combating cybercrime – Developments in the European union’)

Wenzel W *Law enforcement's electronic surveillance requirements in an evolving telecommunications environment* (Masters dissertation Saint Mary's University of Minnesota 1997) (Wenzel *Law enforcement's electronic surveillance*)

Whelan D P *Practice law in the cloud* (Canada Law Book, Canada, 2013) Williams V *Surveillance and intelligence law handbook* (Oxford Oxford University Press 2006) (Whelan *Practice law in the cloud*)

Wiese T Alternative dispute resolution in South Africa- Negotiation, mediation, arbitration and ombudsmen (Juta South Africa 2016) (Wiese *ADR in SA*)

Wong T (ed.) *Regulation of interception of communications in selected judgment* (Research and Library Services Division HongKong 2005) (Wong (ed.) *Regulation of interception of communications in selected judgment*)

Wood G 'Prison without walls' in Swire P P and Ahmad K (eds.) *Privacy and surveillance with new technologies* (International Debate Education Association New York 2012) (Wood *Prison without walls*)

Woolman S and M Bishop *Constitutional Law of South Africa:* 2nd ed. *Revision Service 5* Vol 3 (Juta South Africa 2013) (Woolman and Bishop *Constitutional Law*)

Yacoob S and Pillay K 'Licensing' in L Thornton et. al. (eds.) *Telecommunications law in South Africa* (2006) (S Yacoob and K Pillay 'Licensing') (STE Publishers Johannesburg 2006) (Yacoob and Pillay *Licensing*)

Young L *Life among the giants: A Childs' eye-view of the grown-up world* (1966) at 193 and 245 (McGraw-Hill Book Company New York 1966) (Young *Life among the giants: A childs' eye-view of the grown-up world*)

Young M R et al. *Accounting irregularities and financial fraud: A corporate governance guide* (Aspen Law & Business New York 2002) (Young et al. *Accounting irregularities and financial fraud*)

JOURNAL ARTICLES

Ackermann L W 'Constitutional comparativism in South Africa' (2006) Vol 123 Issue 3 *SALJ* (Ackermann 2006 Vol 123 Issue 3 *SALJ*)

AnKathuria A and Porporino F J 'Implementing information technology for corrections in Africa: A Case example of the Namibian Correctional Service automated offender management information system' 2015 *Acta Criminologica: Southern African Journal of Criminology Special Edition No 2/2015* (AnKathuria and Porporino 2015 *Acta Criminologica: Southern African Journal of Criminology Special Edition No 2/2015*)

Barnes H 'F v Minister of Safety and Security-Vicarious liability and State accountability for the criminal acts of police officers' 2014 47 *SACQ* 29 (Barnes 2014 47 *SACQ* 29)

Berning J and Montesh M 'Countering corruption in South Africa-The rise and fall of the Scorpions and Hawks' 2012 39 *SACQ* 3 at 5-8 (Berning and Montesh 2012 39 *SACQ* 3)

Barrie G N 'International law and economic coercion- A legal assessment' 1985-1986 11 *SAYIL* 40 (Barrie 1985-1986 11 *SAYIL* 40)

Basdeo V 'The constitutional validity of search and seizure powers in South African criminal procedure' 2009 *PER* (12)4 316/360 - 319/360 and 326/360 - 328/360 (Basdeo 2009 *PER* (12)4 316/360 - 319/360 and 326/360 - 328/360)

Basdeo V 'The legal challenges of search and seizure of electronic evidence in South African criminal procedure: A comparative analysis' 2012 2 *SACJ* 198 at 205 (Basdeo 2012 2 *SACJ* 198)

Berkowitz R 'Packet Sniffers and Privacy: Why the no-suspicion-required standard in the USA Patriot Act is constitutional' 2002 7 *Computer Law Review and Technology Journal* (Berkowitz 2002 7 *Computer Law Review and Technology Journal* 2)

Brennan T J and Macaulay M K 'Remote sensing satellites and privacy: a framework for policy assessment' 1995 Vol.4, No 3 *Law, Computer & Artificial Intelligence* 1995 at 233-249 (Brennan and Macaulay 1995 Vol. 4 No 3 *Law, Computer & Artificial Intelligence*)

Bruce D 'Measuring output, neglecting outcomes-The auditor-general's role in SAPS performance assessment' 2011 38 *SACQ* 3 (Bruce 2011 38 *SACQ* 3)

Bruce D 'New blood-implications of e*n-masse* recruitment for the South African Police Service' 2013 43 *SACQ* 17 (Bruce 2013 43 *SACQ* 17)

Burger J 'To protect and server-restoring public confidence in the SAPS' 2011 36 *SACQ* 13 at 13-19 (Burger 2011 36 *SACQ* 13)

Calland R and Masuku T 'Tough on crime and strong on human rights: The challenge for us all' 2009 *Sabinet Law, Democracy and Development* 131(Calland and Masuku 2009 *Sabinet Law, Democracy and Development* 131)

Cameron E 'Sexual orientation and constitution: A test case for human rights' 1993 110 *SALJ* (Cameron 1993 110 *SALJ* 450)

Cameron S D Brown 'Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice' 2015 *International Journal of Cyber Criminology* Vol. 9 Issue 1 January – June (Cameron 2015 *International Journal of Cyber Criminology* Vol. 9 Issue 1 January – June)

Cassim F 'Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?' 2015 *PER/PELJ* 2015(18) 2 at 77 (Cassim 2015 *PER/PELJ* 2015(18) 2 at 77)

Currie I 'The concept of privacy in the South African constitution: Reprise' 2008 *TSAR* 3 553-554 (Currie 2008 *TSAR* 3 553-554)

De Quintal M T 'Sovereignty disputes in the Antarctic' 1984 *SAYIL* 10 161 (De Quintal 1984 SAYIL10 161)

Du Plessis M and Penfold G 'Bill of rights jurisprudence: Operational provisions of the bills of rights 2008 *Juta's Annual Survey of South African Law* 50 (Du Plessis and Penfold 2008 *Juta's Annual Survey of South African Law* 50)

Ebersohn G 'A common law perspective on computer-related crimes' 2004 *THRHR* 22 (Ebersohn 2004 *THRHR* 22)

Faull A 'On the record-interview with Francois Beukman, executive director Independent Complaint Directorate' 2011 36 *SACQ* 37 (Faull 2011 36 *SACQ* 37)

Faull A 'Oversight agencies in South Africa and the challenge of police corruption' 2011 *ISS* 227 (Faull 2011 *ISS* Paper 227)

Faull A 'When I see them I feel like beating them-Corruption and the South African Police Service' 2010 34 *SACQ* 33 (Faull 2010 34 *SACQ* 33)

Faull A and Mtsolongo T 'From stings to wings-integrity management and the Directorate for Priority Crime Investigations' 2009 29 *SACQ* 17 at 17 -22 (Faull and Mtsolongo 2009 29 *SACQ* 17)

Fergusson-Brown K 'The legality of economic sanctions against South Africa in contemporary international law' 1988-9 14 *SAYIL* 59 (Fergusson-Brown 1988-9 14 *SAYIL* 59)

Gevers C '*Southern Africa Litigation Centre &another v National Director of Public Prosecutions & others*' 2013 130 *SALJ* at 293 (Gevers 2013 130 *SALJ* 293)

Georgieva I 'Privacy under fire-foreign surveillance under NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' 2015 31 (80) *Utrecht Journal of International and European Law* 104 (Georgieva 2015 31 (80) *Utrecht Journal of International and European Law* 104)

Gould C 'On the record-Sindiswa Chikunga, Chairperson of the Parliamentary Portfolio Committee on Police' 2012 40 *SACQ* 39 at 41 (Gould 2012 40 *SACQ* 39)

Godkin E L *Libel and Its Legal Remedy* 1880 12 *J Soc SCI* 69 (Godkin 1880 12 *J Soc SCI* 69)

Goldsmith J L 'Against cyberanarchy' 1998 *University of Chicago law Review* 65 1199 (Goldsmith 1998 *University of Chicago law Review* 65 1199)

Goldsmith J L 'The Internet and the abiding significance of territorial sovereignty' 1998 *Indiana Journal of Global Legal Studies* 5 49 (Goldsmith 1998 *Indiana Journal of Global Legal Studies* 5 49)

Grimmelman J 'Saving facebook' 2009 94 *Iowa LR* 1144 (Grimmelman 2009 94 *Iowa LR* 1144)

Harfield C The organisation of organised crime policing and its international context 2008 8 (4) *Criminology and Criminal Justice* 483 (Harfield 2008 8 (4) *Criminology and Criminal Justice* 483)

Holmes O W Jnr 'The path of law' 1897 *Harvard Law Review* 10 457(Holmes 1897 *Harvard Law Review* 10)

Johnson D R and Post D G 'Law and borders-The rise of law in cyberspace' 1996 48 *Stanford Law Review* 1367 (Johnson and Post 1996 48 *Stanford Law Review* 1367)

Jourard S M 'Some psychological aspects of privacy' 1966 31 *Law & Contemp. Prob.* 307 (Jourard 1966 31 *Law & Contemp. Prob.* 307)

JSTOR 'United States Comprehensive Anti-Apartheid Act of 1986' 1987 26 *ILM* 111 (JSTOR 1987 26 *ILM* 111)

Karst K L 'The files': Legal controls over the accuracy and accessibility of stored personal data 1996 31 *Law & Contempt Probs* 342 (Karst 1996 31 *Law & Contempt Probs* 342)

Koops B 'Cybercrime legislation in the Netherlands' 2010 Vol.14.3 *Electronic Journal of Comparative Law* (Koops 2010 Vol.14.3 *Electronic Journal of Comparative Law*)

Koops B-J and Goodwin M 'Cyberspace, the cloud, and cross-border criminal investigation' 2014 83 *Tilburg Law School Research Paper* 5/2016 (Koops and Goodwin 2014 83 *Tilburg Law School Research Paper* 5/2016)

Kinnes I and Newham G 'Freeing the Hawks-Why an anti-corruption agency should not be in SAPS' 2012 39 *SACQ* 33 (Kinnes and Newham 2012 39 *SACQ* 33)

Kleve P, De Mulder R V & Van Der Wees J G L 'Re-engineering dispute in an EDI-environment' Law' 1995 Vol. 4 No 1 *Computers & Artificial Intelligence* at 25- 32 (Kleve, De Mulder and Van Der Wees 1995 Vol. 4 No 1 *Computers & Artificial Intelligence* 25)

Kohn L 'The burgeoning constitutional requirement rationality and separation of powers: Has rationality review gone too far' 2013 130 *SALJ* 813 (Kohn 2013 130 *SALJ* 813)

Lewis M and Stenning P 'Considering the Glenister judgment –Independence requirements for anti-corruptions institutions' 2012 39 *SACQ* 11 (Lewis and Stenning 2012 39 *SACQ* 11)

Lindberg A and Svensson D 'IT law from a practitioner's perspective' in Wahlgren P (ed.) 2010 Vol. 56 *Information and communication technology-Legal Issues* (2010) 12 (Lindberg and Svensson 2010 Vol. 56 *Information and communication technology-Legal Issues* 12)

Luck R 'POPI- is South Africa keeping up with international trend' May 2014 *De Rebus* at 44 (Luck May 2014 *De Rebus* 44)

Mashele P 'Will the Scorpion still sting?-The future of the Directorate of Special Operations' 2006 17 *SACQ* 24 at 24-29 (Mashele 2006 17 *SACQ* 24)

McQuoid-Mason D 'Invasion of privacy: Common law v Constitutional delict-Does it make a difference?' 2000 *Acta Juridica* 248 (McQuoid-Mason 2000 *Acta Juridica* 248)

Minnaar A 'Organised crime and the 'New more sophisticated' criminals within the cybercrime environment: How 'organised' are they in the traditional sense' 2016 *Acta Criminologica*:

Southern African Journal of Criminology 29(2) (Minnaar 2016 *Acta Criminologica*: *Southern African Journal of Criminology* 29(2))

Minnaar A 'Crackers', cyberattacks and cybersecurity vulnerabilities: The difficulties in combating the 'new' cybercriminals' 2/2014 *Acta Criminlogica: Southern African Journal of Criminology, Special Edition 2/2014: Research and practice in Criminology and Criminal Justice*: 129 – 144 (Minnaar 2/2014 *Acta Criminlogica: Southern African Journal of Criminology, Special Edition 2/2014: Research and practice in Criminology and Criminal Justice*: 129)

Moseneke D 'Striking a balance between the will of the people and the supremacy of the constitution' 2012 12 *SALJ* at 17 (Moseneke 2012 12 *SALJ* 17)

Muthaphuli P 'Different route, same destination? Assessing the (r)evolution of offender reform in South Africa twenty years into democracy' *Acta Criminologica: Southern African Journal of Criminology* Special Edition No 1/2015 at 132, 136 and 137 (Muthaphuli 2015 *Acta Criminologica: Southern African Journal of Criminology* Special Edition No 1/2015 132)

Nathan L 'Lighting up the intelligence community: An agenda for intelligence reform in South African' March 2009 18.1 *African Security Review* 91

Ncube C B 'Watching the watcher: Recent developments in privacy regulation and cyber-surveillance in South Africa' 2006 13 *SCRIPT-ed* 349 (Ncube 'Watching the Watcher: cyber-surveillance' 2006 13 *SCRIPT-ed* 349)

Neethling J 'Outeursreg en Persoonlikheidregte: 'n teoretiese analise met verwysing na outeursregbevoegdhede in die SA Reg' 1975 *THRHR* 333 (Neethling 1975 *THRHR* 333)

Neethling J 'The concept of privacy in South African law' (2005) 122 *SALJ* 20 (Neethling 2005 122 *SALJ* 20)

Neethling J 'The protection of the right to privacy against fixation of private facts' (2004) 121 *SALJ* 519 **(**Neethling 2004 121 *SALJ* 519)

Nieman A 'Cyberforensics: Bridging the law/technology divide' 2009(1) *Journal of Information, Law & Technology* 2013 *JILT* 13 (Nieman 2013 *JILT* 13)

Osula A 'Remote search and seizure in domestic criminal procedure: Estonian case study' Winter 2016 Volume 24, Issue 4 *Int J Law Info Tech* 343 (Osula Winter 2016 Volume 24, Issue 4 *Int J Law Info Tech* 343)

Paust J and Blaustein A P 'The Arab-oil weapon-A threat to international peace' 1974 68 *AJIL* 410 (Paust and Blaustein 1974 68 *AJIL* 410)

Pistorius T "Formation of Internet contracts: An analysis of the contractual and security issues" 1999 11 *SA Merc. LJ* 282 (Pistorius 1999 11 *SA Merc. LJ* 282)

Rautenbach I M 'The conduct and interests protected by the right to privacy in section 14 of the constitution' 2001 Vol *TSAR* 116 (Rautenbach 2001 *TSAR* 116)

Rautenbach I M 'Privacy taxonomy' 2009 3 *TSAR* 550 and 554 (Rautenbach 2009 3 *TSAR* 550)

Reeves C 'After Glenister - The case for a new dedicated agency' 2012 39 *SACQ* 23 (Reeves 2012 39 *SACQ* 23)

Roos A 'Privacy in the facebook era: A South African legal perspective' 2012 129 *SALJ* 394 (Roos 2012 129 *SALJ* 394)

Roos A 'Data protection: Explaining the international backdrop and evaluating the South African position' 2007 124 *SALJ* 400 (Roos 2007 124 *SALJ* 400)

Schönteich M 'A story of trials and tribulations -The National Prosecuting Authority, 1998 – 2014' *SA Crime Quarterly* No. 50 at 7 (Schönteich 1998 – 2014 *SA Crime Quarterly* No. 50 7)

Seitz N 'Trans-border search: A new perspective in law enforcement' 2004 7 *Yale JL & Tech* 28 (Seitz 2004 7 *Yale JL & Tech* 28)

Shils E ‘Privacy: Its constitution and vicissitudes’ 1966 31 *Law & Contemp. Probs*. 305 (Shils 1966 31 *Law & Contemp. Probs*. 305)

Silard J ‘A constitutional forecast: Demise of the State action- Limit on the equal protection guarantee’ 1966 66 *Col L Rev* 855 (Silard 1966 66 *Col L Rev* 855)

Schiffres J ‘invasion of privacy-Use of plaintiff’s name or likeness for non-advertising purposes’ (1970) 30 *ALR* 3d 203, 212 (Schiffres 1970 30 *ALR* 3d)

Shnider S P ‘The “design to conceal” Requirement and the elusive culprits of money-laundering’ Spring 2012 48 *Criminal Law Bulletin* 2 (Shnider 2012 48 *Criminal Law Bulletin* 2)

Solove D J ‘Conceptualising privacy’ 2002 Vol. 90 *California Law Review* 1088 (Solove 2002 Vol. 90 *California Law Review* 1088)

Spencer A B ‘Jurisdiction and the Internet: Returning to traditional principles to analyse networked-mediated contacts’ 2006 No 1 *University of Illinois Law Review* 79 (Spencer 2006 No 1 *University fo Illinois Law Review* 79)

Stuntz W J ‘Privacy’s problem and the law of criminal procedure’, 1995 93 *Mich. L. Rev.* 1016 (Stuntz 1995 93 *Mich. L. Rev.* 1016)

Sutherland E ‘Governance of cybersecurity - The case of South Africa’ 2017 Issue 20 *AJIC* 85(Sutherland 2017 Issue 20 *AJIC* 85)

Svanatesson D J B ‘How does the accuracy of geo-location technologies affect the world’ 2007 *Masaryk University Journal of Law and Technology* 2 (Svanatesson 2007 *Masaryk University Journal of Law and Technology* 2)

Tang T ‘A systemic theory of the security environment’ 2004 Vol. 27 *The Journal of Strategic Studies* (Tang 2004 Vol. 27 *The Journal of Strategic Studies*)

Vladeck D C ‘Machines without principals: Liability rules and artificial intelligence’ 2014 Vol. 89 *Washington Law Review* 117 (Vladeck 2014 Vol. 89 *Washington Law Review* 117)

Volonino L ‘Electronic evidence and computer forensics’ 2003 12 *Communications of the Association for Information Systems* 459 (Volonino 2003 12 *Communications of the Association for Information Systems* 459)

Von Heinegg W H ‘Territorial sovereignty and neutrality in cyberspace’ 2003 89 *Int’l L. Stud.* 123 (Von Heinegg 2003 89 *Int’l L. Stud.* 123)

Wannenburg G ‘Putting paid to the untouchables?- The effects of dissolving the directorate of Special Operations and Specialized Commercial Crime Units’ 2008 24 *SACQ* 17 at 17- 20 (Wannenburg 2008 24 *SACQ* 17)

Warren S D & Brandies L D ‘The right to privacy’ 4 *Harv. L Rev* 193 (1890) 196, 197, 200, 205 (Warren & Brandies 1890 4 *Harv. L Rev* 193)

Watney M ‘Admissibility of electronic evidence in criminal proceedings: An outline of the South African legal position’ 2009 (1) *Journal of Information, Law & Technology* (*JILT*) 1 (Watney 2009 (1) *Journal of Information, Law & Technology* (*JILT*) 1)

Weber R H ‘Internet of things-need for a new legal environment?’ 2009 25 *Computer Law & Security Report* 522 (Weber 2009 25 *Computer Law & Security Report* 522)

Whitcomb C M ‘A historical perspective of the digital evidence: A forensic scientist’s view’ 2002 1 *International Journal of Digital Evidence* 1-4 (Whitcomb 2002 1 *International Journal of Digital Evidence* 1)

Whitman J Q ‘The two western cultures of privacy: Dignity versus liberty’ 2004 113 *Yale LJ* 1181 (Whitman 2004 113 *Yale LJ* 1181)

Wolf L ‘The prosecuting discretion: A Power under administrative law or criminal law?’ 2011 *TSAR* 4 703 (Wolf 2011 *TSAR* 4 703)

Wong K C ‘Policing in Hong Kong’ 2012 85 *Police Journal* 4 347 (Wong 2012 85 *Police Journal* 2)

Zinn R ‘Inside information- Sourcing crime intelligence from incarcerated armed robbers’ 2010 32 *SACQ* 27 (Zinn 2010 32 *SACQ* 27)

CONFERENCE PAPERS

Anon 'Drug Trafficking and organised Crimes (Amendment) Bill 2000- Note on "reasonable grounds to suspect", "reasonable grounds believe" and "reasons for introducing two money laundering offences using different mental elements"' (Paper No CB(2)820/00-01(01) (Anon 'Drug Trafficking and organised Crimes (Amendment) Bill 2000- Note on "reasonable grounds to suspect", "reasonable grounds believe" and "reasons for introducing two money laundering offences using different mental elements"')

Pieterse N B 'Electronic Crime Unit: Directorate for Priority Crime Investigation' (Paper delivered at the workshop for policy design towards digital security, cybercrime and cybercrime prevention 2015 (Pieterse 'Electronic Crime Unit: Directorate for Priority Crime Investigation')

Ratcliffe J H "Intelligence-led Policing", (Paper No. 248 delivered at the Trends and Issues in Crime and Criminal Justice, in April 2003, Australian Institute of Criminology) (Ratcliffe "Intelligence-led Policing")

WIPO 'Copyright in the global information infrastructure' (Paper delivered at WIPO Worldwide Symposium held between 22-24 May, 1995 WIPO Mexico) (WIPO 'Copyright in the global information infrastructure')

Veeraraghavan M and Wang H "A comparison of in-band and out-of-band transport options for signaling" (Paper delivered at the Conference: Global Telecommunications Conference Workshops, held on 29 November -3 December 2004 IEEE USA) (Veeraraghavan and Wang "A comparison of in-band and out-of-band transport options for signaling")

Von Heinegg W H 'Legal implications of the territorial sovereignty in cyberspace' in *International Conference on Cyber Conflict* (Papers delivered at the 4th ed. *International Conference on Cyber Conflict* between 5-8 June, 2012 NATO CCD COE Publications Estonia) (Von Heinegg 'Legal implications of the territorial sovereignty in cyberspace')

MAGAZINES AND NEWSPAPERS

Vlok M ‘The vultures preying on your social network- Criminals can exploit even the most innocent pictures or posts on social media-here’s how to protect yourself’ 2017-02-23 *You* 24 - 25 (Vlok 2017-02-23 *You* 24 - 25)

Hosken G et. al. ‘SA blows Nigeria away as drug capital- organised crime rampant, statistics show’ 2015-09-30 *The Times* 1-2 (Hosken et. al. 2015-09-30 *The Times* 1-2)

Godkin E L ‘The rights of the citizen IV-To his own reputation’ 1890 July – December *Scribers Magazine* at 65 (Godkin 1890 July – December *Scribers Magazine* at 65)

Jurgens A and Savides M ‘Revealed: SA spies scary shopping list - WikiLeaks lays bare SA police and SARS agents inquires about espionage software’ 2015- 07-12 *Sunday Times* 1-2 (Jurgens and Savides 2015- 07-12 *Sunday Times* 1-2)

Maphumulo S ‘Senior official helped bring in grabber-assistant director at centre of Hawks probe was rewarded for his role’ 2015-11-03 *The Star* 2 (Maphumulo 2015-11-03 *The Star* 2)

Maphumulo S ‘Cops in spy gadget probe- Hawks’ damning investigation set to open can of worms’ 2016-08-30 *The Sunday Independent* 1 (Maphumulo 2016-08-30 *The Sunday Independent* 1)

R5Componets ‘Robots race it out in Tshwane’ 2017-07-19 *Dataweek* 8 (R5Componets 2017-07-19 *Dataweek* 8)

Shaikh N ‘Online “Cheaters” caught in the web-many put in compromising position by hackers’ 2015-08-30 *The Sunday Independent* 3 (Shaikh 2015-08-30 *The Sunday Independent* 3)

Puren S ‘Paedophiles, the web is closing in’ 2015-10- 29 *You* 136 (Puren 2015-10- 29 *You* 136)

INTERNET SOURCES

ABC News 'Lamola appoints Justice Catherine O'Regan as COVID-19 designate judge' https://www.sabcnews.com/sabcnews/lamola-appoints-justice-catherine-oregan-as-covid-19-designate-judge/accessed (Date of use: 5 April 2020) (ABC News https://www.sabcnews.com/sabcnews/lamola-appoints-justice-catherine-oregan-as-covid-19-designate-judge/accessed (Date of use: 5 April 2020)

Adam K 'Trump calls for investigation of U.S. leaks in Manchester bombing probe' https://www.washingtonpost.com/world/british-outrage-over-alleged-us-leaks-in-the-manchester-bomb-investigation/2017/05/25/f21349e2-4b0b-4afd-ba06-333621cfa634_story.html?utm_term=.0ad53e0d07ba (Date of use: 25 May 2017) (Adam https://www.washingtonpost.com/world/british-outrage-over-alleged-us-leaks-in-the-manchester-bomb-investigation/2017/05/25/f21349e2-4b0b-4afd-ba06-333621cfa634_story.html?utm_term=.0ad53e0d07ba) (Date of use: 25 May 2017)

Africa S and S Mlombile S 'Transforming the intelligence services: Some reflections on the South African experience' http://www.law.harvard.edu/programs/criminal-justice/south-africa.pdf (Date of use: 7 January 2018) (Africa and Mlombile http://www.law.harvard.edu/programs/criminal-justice/south-africa.pdf (Date of use: 7 January 2018)

Akwei I 'Nigerian Amina Mohammed interacts with Sophia the robot at the UN' http://www.africanews.com/2017/10/12/nigerian-amina-mohammed-interacts-with-sophia-the-robot-at-the-un-video// (Date of use: 18 October 2017) (Akwei http://www.africanews.com/2017/10/12/nigerian-amina-mohammed-interacts-with-sophia-the-robot-at-the-un-video//) (Date of use: 18 October 2017)

Altbeker A 'Introduction –Justice through specialization' http://www.issafrica.org/publications/monographs/monograph-76-justice-through-specialisation-the-case-of-the-specialised-commercial-crime-court-antony-altbeker (Date of use: 12 June 2016) (Altbeker http://www.issafrica.org/publications/monographs/monograph-76-justice-through-specialisation-the-case-of-the-specialised-commercial-crime-court-antony-altbeker (Date of use: 12 June 2016)

Altbeker A 'Paying for crime: South Africa spending on criminal justice' ISS Paper 115 July 2005 https://issafrica.org/research/papers/paying-for-crime-south-african-spending-on-criminal-justice (Date of use: 8 June 2016) (Altbeker https://issafrica.org/research/papers/paying-for-crime-south-african-spending-on-criminal-justice (Date of use: 8 June 2016)

AmaBhugane 'Advocacy: amaB challenges snooping law' http://amabhungane.co.za/article/2017-04-20-amab-challenges-snooping-law (Date of use: 20 April 2017) (AmaBhugane http://amabhungane.co.za/article/2017-04-20-amab-challenges-snooping-law (Date of use: 20 April 2017)

ANA Reporter 'Peter Jacobs appointed new SAPS crime intelligence boss' https://www.iol.co.za/news/south-africa/western-cape/peter-jacobs-appointed-new-saps-crime-intelligence-boss-14152684 (Date of use: 12 June 2018) (ANA Reporter https://www.iol.co.za/news/south-africa/western-cape/peter-jacobs-appointed-new-saps-crime-intelligence-boss-14152684 (Date of use: 12 June 2018)

ANA 'Sanef to start probe over Sunday Times 'fake news' https://citizen.co.za/news/south-africa/2023805/sanef-to-start-probe-over-sunday-times-fake-news/ (Date of use: 12 December 2018) (ANA https://citizen.co.za/news/south-africa/2023805/sanef-to-start-probe-over-sunday-times-fake-news/ (Date of use: 12 December 2018)

ANA 'Former Prasa acting CEO to break silence on 350% salary hike claims' https://www.iol.co.za/business-report/companies/former-prasa-acting-ceo-to-break-silence-on-350-salary-hike-claims-18528550 (Date of use: 18 December 2018) (ANA https://www.iol.co.za/business-report/companies/former-prasa-acting-ceo-to-break-silence-on-350-salary-hike-claims-18528550 (Date of use: 18 December 2018)

Anon 'Digital evidence gathering' - Anti cartel enforcement manual 2010 -Cartel working group-subgroup 2- enforcement techniques www.internationalcompetitionnetwork.org (Date of use: 14 July 2016 (Anon www.internationalcompetitionnetwork.org (Date of use: 14 July 2016)

Anon 'NIA says it is not monitoring Zille's calls' http://mg.co.za/article/2011-03-09-nia-says-it-is-not-monitoring-zilles-calls (Date of use: 18 April 2016) (Anon http://mg.co.za/article/2011-03-09-nia-says-it-is-not-monitoring-zilles-calls (Date of use: 18 April 2016)

Anon 'Probable cause' http://legal-dictionary.thefreedictionary.com/Probable+Cause+and+Reasonable+Suspicion (Date of use: 12 April 2016 (Anon http://legal-dictionary.thefreedictionary.com/Probable+Cause+and+Reasonable+Suspicion (Date of use: 12 April 2016)

Anon 'United Nations Office on Drugs and Crime 'Comprehensive study on cybercrime –draft' February 2013 124 http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (Date of use: 27 May 2016) (Anon http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (Date of use: 27 May 2016)

Anti-Corruption Authorities 'PROFILEs: South Africa' https://www.acauthorities.org/country/ZA (Date of use: 12 December 2016) (Anti-Corruption https://www.acauthorities.org/country/ZA (Date of use: 12 December 2016)

AP 'Zim High Court rules internet shutdown illegal, orders govt to restore full internet to the country' https://www.news24.com/Africa/Zimbabwe/just-in-zim-high-court-rules-internet-shutdown-illegal-orders-govt-to-restore-full-internet-to-the-country-20190121 (Date of use: 31 January 2019) (AP https://www.news24.com/Africa/Zimbabwe/just-in-zim-high-court-rules-internet-shutdown-illegal-orders-govt-to-restore-full-internet-to-the-country-20190121 Date of use: 31 January 2019)

Associated Press 'Trump threatens emergency declaration ahead of US-Mexico border visit' https://www.news24.com/World/News/trump-threatens-emergency-declaration-ahead-of-us-mexico-border-visit-20190110 (Date of use: 11 Januarry 2019) (Associated Press

https://www.news24.com/World/News/trump-threatens-emergency-declaration-ahead-of-us-mexico-border-visit-20190110 (Date of use: 11 Januarry 2019)

Association of Chief Police Officers (ACPO) 'Good practice guide for computer-based electronic evidence' 4 ed. - Official release version of e-crime working group www.acpo.police.uk (Date of use: 28 January 2016) (ACPO www.acpo.police.uk (Date of use: 28 January 2016)

AT 'Activists: We're shutting down Sudan government websites' https://africatimes.com/2018/12/26/activities-were-shutting-down-sudan-government-websites/ (Date of use: 3 January 2019) (AT https://africatimes.com/2018/12/26/activities-were-shutting-down-sudan-government-websites/ (Date of use: 3 January 2019)

Ax J 'U.S. judge orders Microsoft to submit customer's emails from abroad' http://www.reuters.com/article/2014/07/31/usa-tech-warrants-idUSL2N0Q61WN20140731 (Date of use: 18 March 2016) (Ax http://www.reuters.com/article/2014/07/31/usa-tech-warrants-idUSL2N0Q61WN20140731) (Date of use: 18 March 2016)

Bateman B 'SAPS, IPID working to avert conflict of interest in cases' http://ewn.co.za/2018/07/05/saps-ipid-working-to-avert-conflict-of-interest-in-cases (Date of use: 6 July 2018) (Bateman http://ewn.co.za/2018/07/05/saps-ipid-working-to-avert-conflict-of-interest-in-cases (Date of use**:** 6 July 2018)

Bateman C 'Paul O'Sullivan takes anti-McBride MPs on at their own game' https://www.biznews.com/undictated/2019/04/15/paul-o-sullivan-anti-mcbride-mps (Date of use: 15 April 2019 (Bateman https://www.biznews.com/undictated/2019/04/15/paul-o-sullivan-anti-mcbride-mps (Date of use: 15 April 2019)

Bennet D W 'The challenges facing computer forensic investigators in obtaining information from mobile devices for use in criminal investigations' https://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/ (Date of use: 2 December 2016) (Bennet

https://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/ (Date of use: 2 December 2016)

Berners-Lee T J 'World Wide Web Foundation' https://webfoundation.org/about/sir-tim-berners-lee/ (Date of use: 3 June 2016) (Berners-Lee https://webfoundation.org/about/sir-tim-berners-lee/ (Date of use: 3 June 2016)

Bizcommunity 'Africa's first professional body for supply chain management launched' https://www.bizcommunity.com/Article/196/760/178600.html (Date of use: 27 February 2019 (Bizcommunity https://www.bizcommunity.com/Article/196/760/178600.html (Date of use: 27 February 2019)

Boyer D 'NSA seizes phone records of Verizon customers' http://www.washingtontimes.com/news/2013/jun/5/nsa-seizes-phone-records-verizon-customers/ (Date of use: 10 June 2016) (Boyer http://www.washingtontimes.com/news/2013/jun/5/nsa-seizes-phone-records-verizon-customers/ (Date of use: 10 June 2016)

Botha A 'Terrorism in the Maghreb: The transnationalization of domestic terrorism' http://www.terrorismanalysts.com/pt/index.php/pot/article/view/101/html (Date of use: 27 June 2016) (Botha http://www.terrorismanalysts.com/pt/index.php/pot/article/view/101/html (Date of use: 27 June 2016)

Brocklin V V 'Legal, privacy concerns to consider before implementing iris-scanning technology Looking at some public concerns and legal issues can help law enforcement plan its use of the evolving technology' https://www.policeone.com/police-products/police-technology/biometrics-identification/articles/430150006-Legal-privacy-concerns-to-consider-before-implementing-iris-scanning-technology/ (Date of use: 15 July 2018) (Brocklin https://www.policeone.com/police-products/police-technology/biometrics-identification/articles/430150006-Legal-privacy-concerns-to-consider-before-implementing-iris-scanning-technology/ (Date of use: 15 July 2018)

Business Dictionary '*delegatus non potest non delegare*' http://www.businessdictionary.com/definition/delegatus-non-potest-delegare.html (Date of use: 23 August 2019 (Business Dictionary '*delegatus non potest non delegare*' http://www.businessdictionary.com/definition/delegatus-non-potest-delegare.html (Date of use: accessed 23 August 2019)

Business Tech 'Phone tapping and signal jamming threat in SA' https://businesstech.co.za/news/general/79800/phone-tapping-and-signal-jamming-threat-in-sa/ (Date of use: 18 November 2017) (Business Tech https://businesstech.co.za/news/general/79800/phone-tapping-and-signal-ja9mming-threat-in-sa/ (Date of use: 18 November 2017)

Cajani F 'Communication interception regarding Google, Microsoft and Yahoo! Tools and electronic data retention on foreign server: a legal perspective from the state which is conducting an investigation' www.iisfa.eu (Date of use: 8 June 2013) (Cajani www.iisfa.eu (Date of use: 8 June 2013)

Cajani F 'Interception of communications: Skype, Google, Yahoo! and Microsoft tools and electronic data retention on foreign servers: a legal perspective from a prosecutor conducting an investigation' http://journals.sas.ac.uk/deeslr/article/view/1884 (Date of use: 21 March 2016) (Cajani http://journals.sas.ac.uk/deeslr/article/view/1884 (Date of use: 21 March 2016)

Cajani F 'Technologies and business vs law- Cloud computing, data access and data retention: A legal perspective from the state which is conducting an investigation' 8 https://rm.coe.int/09000016802f241b (Date of use: 21 March 2016) (Cajani https://rm.coe.int/09000016802f241b (Date of use: 21 March 2016)

Callanan C and Gercke M 'Cooperation between law enforcement and Internet service providers against cybercrime: Towards common guidelines' Discussion paper for project on cybercrime version 2008 www.coe.int/cybercrime (Date of use: 2 April 2017) (Callanan and Gercke www.coe.int/cybercrime (Date of use: 2 April 2017)

Cassim F 'Addressing the growing spectre of cybercrime in Africa: Evaluating measures adopted by South Africa and other regional role players'

https://core.ac.uk/download/pdf/79170924.pdf (Date of use: 17 July 2017) (Cassim https://core.ac.uk/download/pdf/79170924.pdf (Date of use: 17 July 2017)

CBC Radio 'British student jailed for life in U.A.E. on spy charges 'totally innocent': PhD supervisor' https://www.cbc.ca/radio/asithappens/as-it-happens-thursday-edition-1.4916477/british-student-jailed-for-life-in-u-a-e-on-spy-charges-totally-innocent-phd-supervisor-1.4916485 (Date of use: 24 November 2018 (CBC Radio https://www.cbc.ca/radio/asithappens/as-it-happens-thursday-edition-1.4916477/british-student-jailed-for-life-in-u-a-e-on-spy-charges-totally-innocent-phd-supervisor-1.4916485 (Date of use: 24 November 2018)

Deaprtment of Public Service and Administration 'Senior Managemnt Servcie Handbook Chapter 9 Disclosure of Financial Interest 1/12/2003' http://www.dpsa.gov.za/dpsa2g/documents/sms/publications/CH9_SMS_2003.pdf (Date of use: 12 March 2014)

Chabalala J 'EXCLUSIVE: McBride 'begged' ex-NPA boss to prosecute IPID cases for months, Abrahams denies 'baseless' claims' https://www.news24.com/SouthAfrica/News/exclusive-mcbride-begged-ex-npa-boss-to-prosecute-ipid-cases-for-months-abrahams-denies-baseless-claims-20190302 (Date of use 14 April 2019)

CIA 'Training in investigative techniques' https://www.cia.gov/library/readingroom/docs/CIA-RDP57-00012A000200090081-3.pdf (Date of use: 11 September 2016) (CIA https://www.cia.gov/library/readingroom/docs/CIA-RDP57-00012A000200090081-3.pdf (Date of use: Date of use: 11 September 2016)

CIPS 'Charted Institute of Procurement and Supply' https://www.cips.org/en-za/ (Date of use: 29 January 2019) (CIPS https://www.cips.org/en-za/ (Date of use: 29 January 2019)

Cornell University Library 'Arab spring: A research & study guide' https://guides.library.cornell.edu/arab_spring/Syria (Date of use: 20 December 2018 (Cornell

University Library https://guides.library.cornell.edu/arab_spring/Syria (Date of use: 20 December 2018)

CIA 'Training in investigative techniques' https://www.cia.gov/library/readingroom/docs/CIA-RDP57-00012A000200090081-3.pdf (Date of use: 11 September 2016) (CIA https://www.cia.gov/library/readingroom/docs/CIA-RDP57-00012A000200090081-3.pdf (Date of use: 11 September 2016)

Cilluffo F J and Cardash S L 'With hacking of US utilities, Russia could move from cyberespionage toward cyberwar' https://mg.co.za/article/2018-08-05-with-hacking-of-us-utilities-russia-could-move-from-cyberespionage-toward-cyberwar (Date of use: 12 December 2018)(Cilluffo and Cardash https://mg.co.za/article/2018-08-05-with-hacking-of-us-utilities-russia-could-move-from-cyberespionage-toward-cyberwar (Date of use: 12 December 2018)

Citizen Reporter 'Mantashe admits to paying journalists R70K to make sex scandal go away– Ndlozi' https://citizen.co.za/news/south-africa/social-media/2196611/mantashe-admits-to-paying-journalists-r70k-to-make-sex-scandal-go-away-ndlozi/ (Date of use: 28 October 2019) (Citizen Reporter https://citizen.co.za/news/south-africa/social-media/2196611/mantashe-admits-to-paying-journalists-r70k-to-make-sex-scandal-go-away-ndlozi/ (Date of use: 28 October 2019)

CNN '2016 presidential campaign hacking fast facts' https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html (Date of use: 12 December 2018) **(**CNN https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html (Date of use: 12 December 2018)

Council of Europe (CoE) 'Chart of signatures and ratifications of treaty 185 - *Convention on Cybercrime* (CoCC) - Status as of 02/06/2017 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (Date of use: 2 June 2017) (CoE CoCC https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (Date of use: 2 June 2017)

Council of Europe 'Criminal justice access to evidence in the cloud' https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680654221 (Date of use: 28 August 2018) (CNN https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html (Date of use: 12 December 2018)

Corbet S et al 'Cryptocurrencies as a financial asset: A systematic analysis' https://doi.org/10.1016/j.irfa.2018.09.003Get rights and content (Date of use: 28 February 2019) (Corbet S et al https://doi.org/10.1016/j.irfa.2018.09.003Get rights and content (Date of use: 28 February 2019)

Cornwell R 'US declares cyber war on China: Chinese military hackers charged with trying to steal secrets from companies including nuclear energy firm' https://www.independent.co.uk/life-style/gadgets-and-tech/us-charges-chinese-military-hackers-with-cyber-espionage-bid-to-gain-advantage-in-nuclear-power-9397661.html (Date of use: 12 December 2018) (Cornwell https://www.independent.co.uk/life-style/gadgets-and-tech/us-charges-chinese-military-hackers-with-cyber-espionage-bid-to-gain-advantage-in-nuclear-power-9397661.html (Date of use: 12 December 2018)

Cornell University Library 'Arab spring: A research & study guide' https://guides.library.cornell.edu/arab_spring/Syria (Date of use: 20 December 2018 (Cornell University Library https://guides.library.cornell.edu/arab_spring/Syria (Date of use: 20 December 2018)

Cosatu 'Tripartite alliance' http://www.cosatu.org.za/show.php?ID=2051 (Date of use: 8 March 2019) (Cosatu http://www.cosatu.org.za/show.php?ID=2051 (Date of use: 8 March 2019)

Cowan K and Wa Afrika M 'Head of SAPS crime intelligence still has no security clearance' https://www.timeslive.co.za/politics/2017-07-23-head-of-saps-crime-intelligence-still-has-no-security-clearance/ (Date of use: 21 August 2017) (Cowan and Wa Afrika https://www.timeslive.co.za/politics/2017-07-23-head-of-saps-crime-intelligence-still-has-no-security-clearance/ (Date of use: 21 August 2017)

Cowan K ‘Here is the EFF's 'evidence' on Gordhan's daughter - and why their claims are bogus’ https://www.news24.com/SouthAfrica/News/here-is-the-effs-evidence-on-gordhans-daughter-and-why-their-claims-are-bogus-20181122 (Date of use: 30 November 2019) (Cowan https://www.news24.com/SouthAfrica/News/here-is-the-effs-evidence-on-gordhans-daughter-and-why-their-claims-are-bogus-20181122 (Date of use: 30 November 2019)

DA ‘Parties not happy with McBride recommendation’ http://news.howzit.msn.com/politics/parties-not-happy-with-mcbride-recommendation (Date of use: 15 November 2013 (DA http://news.howzit.msn.com/politics/parties-not-happy-with-mcbride-recommendation (Date of use: 15 November 2013)

Dauda M *Plain language in drafting legislation in Nigeria*: *The possible benefits* (LL.M dissertation) (2016) http: //ft.lk/2011/10/08/mathematical-language-can-language-legal-drafting-icta-chairman-prof-espasinghe (Date of use: 3 June 2018) (Dauda http: //ft.lk/2011/10/08/mathematical-language-can-language-legal-drafting-icta-chairman-prof-espasinghe (Date of use: 3 June 2018)

DATASTAX ‘Introduction to multi-data center operations with apache cassandra and dataStax enterprise- White Paper’ October 2013 http://www.datastax.com/wp-content/uploads/2012/09/WP-DataStax-MultiDC.pdf (Date of use: 7 July 2015) (DATASTAX http://www.datastax.com/wp-content/uploads/2012/09/WP-DataStax-MultiDC.pdf (Date of use: 7 July 2015)

Defenceweb ‘Former police crime intelligence officer guilty of phone spying available at https://www.defenceweb.co.za/security/national-security/former-police-crime-intelligence-officer-guilty-of-phone-spying/ (Date of use: 27 September 2018 (Defenceweb https://www.defenceweb.co.za/security/national-security/former-police-crime-intelligence-officer-guilty-of-phone-spying/ (Date of use: 27 September 2018)

Department of Defence and Military Veterans ‘Annual report FY 2012/13’ http://www.dod.mil.za/documents/annualreports/Annual%20Report%202013%20Final.pdf (Date of use: 12 March 2014)(Department of Defence and Military Veterans http://www.dod.mil.za/documents/annualreports/Annual%20Report%202013%20Final.pdf (Date of use: 12 March 2014)

Department of Justice and Constitutional Development 'Mutual legal assistance in criminal matters treaty between the republic of South Africa and the Argentine republic' (2017) http://www.justice.gov.za/legislation/notices/2017/20170714-gg40978_gen518-MLA-Arg.pdf (Date of use: 20 July 2017) (Department of Justice and Constitutional Development http://www.justice.gov.za/legislation/notices/2017/20170714-gg40978_gen518-MLA-Arg.pdf (Date of use: 20 July 2017)

Department of State Security 'Statement on Recent Developments Relating to the Management State Security Agency' http://www.ssa.gov.za/Portals/0/SSA%20docs/Media%20Releases/2013/Media%20Release%20Statement%20on%20recent%20developments%20relating%20to%20the%20State%20Security%20Agency%202%20August%202013.pdf (Date of use: 25 February 2014)(Department of State Security http://www.ssa.gov.za/Portals/0/SSA%20docs/Media%20Releases/2013/Media%20Release%20Statement%20on%20recent%20developments%20relating%20to%20the%20State%20Security%20Agency%202%20August%202013.pdf (Date of use: 25 February 2014)

Department of State Security 'Structure of the State Security Agency' http://www.ssa.gov.za/Branches.aspx (Date of use: 18 January 2014) (Department of State Security http://www.ssa.gov.za/Branches.aspx (Date of use: 18 January 2014)

De Vos P 'The South African Police Service Amendment Bill: Compliance with *Glenister v President of the Republic of South Africa*' http://constitutionallyspeaking.co.za/pierre-de-vos-memo-on-sa-police-service-amendment-bill/ (Date of use: 1 October 2013) (De Vos http://constitutionallyspeaking.co.za/pierre-de-vos-memo-on-sa-police-service-amendment-bill/ (Date of use: 1 October 2013)

De Vos P 'The South African Police Service Amendment Bill: Possible compliance with *Glenister v President of the Republic of South Africa*' https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2050861(Date of use: 2 November 2016) (De Vos https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2050861 (Date of use: 2 November 2016)

De Wet P ‘From bully boys to wimps: The decline of SA's military’ http://mg.co.za/article/2012-05-04-lack-of-funds-leaves-sa-vulnerable (Date of use: 12 October 2013 (De Wet http://mg.co.za/article/2012-05-04-lack-of-funds-leaves-sa-vulnerable (Date of use: 12 October 2013)

De Vos P ‘Law allowing for extension of McBride’s term of office probably unconstitutional’ https://www.dailymaverick.co.za/opinionista/2019-03-05-law-allowing-for-extension-of-mcbrides-term-of-office-probably-unconstitutional/ (Date of use: 11 March, 2019)

De Vos P ‘RICA: Is it unconstitutional?’ https://constitutionallyspeaking.co.za/rica-is-it-unconstitutional/ (Date of use: 12 June 2016)

Diamond A M ‘China’s surveillance State should scare everyone- The country is perfecting a vast network of digital espionage as a means of social control with implications for democracies worldwide’ https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/ (Date of use: 2 March 2019) (Diamond https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/ (Date of use: 2 March 2019)

Dlulane B 'Sharing sex video a violation of Malusi Gigaba's privacy' https://ewn.co.za/2018/10/28/people-who-share-malusi-gigaba-sex-video-could-get-in-trouble-with-the-law (Date of use: 27 April 2019 (Dlulane https://ewn.co.za/2018/10/28/people-who-share-malusi-gigaba-sex-video-could-get-in-trouble-with-the-law (Date of use: 27 January 2019)

Duncan J ‘New year’s resolution for 2017: Stop unaccountable state spying’ https://www.dailymaverick.co.za/article/2017-01-08-new-years-resolution-for-2017-stop-unaccountable-state-spying/#.WmX4OIVOLIU (Date of use: 20 September 2017) (Duncan https://www.dailymaverick.co.za/article/2017-01-08-new-years-resolution-for-2017-stop-unaccountable-state-spying/#.WmX4OIVOLIU (Date of use: 20 September 2017)

Duncan J ‘The politics of South Africa's intelligence priorities’ http://www.polity.org.za/article/the-politics-of-south-africas-intelligence-priorities-

2013-10-01 (Date of use: 2 December 2013) (Duncan http://www.polity.org.za/article/the-politics-of-south-africas-intelligence-priorities-2013-10-01 (Date of use: 2 December 2013)

EDRi 'Transborder data access: Strong critics on plans to extend CoE cybercrime treaty' https://edri.org/edrigramnumber11-11transborder-data-access-cybercrime-treaty/ (Date of use: 12 May 2017) (EDRi https://edri.org/edrigramnumber11-11transborder-data-access-cybercrime-treaty/ (Date of use: 12 May 2017)

Electronic Front Foundation 'International principles on the application of human rights to communications surveillance' https://necessaryandproportionate.org/text (Date of use: 5 August, 2017) (Electronic Front Foundation https://necessaryandproportionate.org/text (Date of use: 5 August 2017)

Electronic Frontier Foundation '13 International principles on the application of human rights to communications Surveillance - Necessary and Proportionate' https://www.eff.org/document/13-international-principles-application-human-rights-communication-surveillance (Date of use: May 20 2016)(Electronic Frontier Foundation https://www.eff.org/document/13-international-principles-application-human-rights-communication-surveillance (Date of use: May 20 2016)

Eloff D 'Unscrambling the general data protection regulation' http://www.derebus.org.za/unscrambling-the-general-data-protection-regulation/ (Date of use 18 January 2019) (Eloff D http://www.derebus.org.za/unscrambling-the-general-data-protection-regulation/ (Date of use 18 January 2019))

eNCA 'Ace Magashule says he has reported his phone being tapped to intelligence' http://www.702.co.za/articles/346668/ace-magashule-says-he-has-reported-his-phone-being-tapped-to-intelligence (Date of use: 3 May, 2019) (eNCA http://www.702.co.za/articles/346668/ace-magashule-says-he-has-reported-his-phone-being-tapped-to-intelligence (Date of use: 3 May, 2019)

eNCA 'Beware: big brother is listening' http://www.msn.com/en-za/news/national/beware-big-brother-is-listening/ar-AAqCyLp?li=BBqg6Q6&ocid=UE07DHP (Date of use: 24 August

2017) (eNCA http://www.msn.com/en-za/news/national/beware-big-brother-is-listening/ar-AAqCyLp?li=BBqg6Q6&ocid=UE07DHP (Date of use: 24 August 2017)

eNCA 'New gunshot detection system takes aim at Cape gangsterism' https://www.enca.com/new-gunshot-detection-system-takes-aim-cape-gangsterism (Date of use: 13 September 2017) (eNCA https://www.enca.com/new-gunshot-detection-system-takes-aim-cape-gangsterism (Date of use: 13 September 2017)

eNCA 'Inspector-General considers Magashule phone-tapping claims' https://www.enca.com/news/inspector-general-considers-magashule-phone-tapping-claims (Date of use: 3 May 2019) (eNCA https://www.enca.com/news/inspector-general-considers-magashule-phone-tapping-claims (Date of use: 3 May 2019)

ENCA 'Journalist Ranjeni Munusamy on special leave amidst slush fund payment claims' https://www.enca.com/news/journalist-ranjeni-munusamy-placed-special-leave-amid-state-capture-revelations (Date of use: 18 September 2019) (ENCA https://www.enca.com/news/journalist-ranjeni-munusamy-placed-special-leave-amid-state-capture-revelations (Date of use: 18 September 2019)

Eye Witness News 'Tripartite alliance to work together to ensure 'massive' 2019 election victory' https://ewn.co.za/2018/07/10/tripartite-alliance-to-work-together-to-ensure-massive-2019-election-victory (Date of use 8 March 2019) (Eye Witness News https://ewn.co.za/2018/07/10/tripartite-alliance-to-work-together-to-ensure-massive-2019-election-victory (Date of use 8 March 2019)

Ferreira E 'New secrecy bill recalls the failings of the old' https://www.iol.co.za/news/politics/new-secrecy-bill-recalls-the-failings-of-the-old-17106869 (Date of use: 25 September 2018) (Ferreira https://www.iol.co.za/news/politics/new-secrecy-bill-recalls-the-failings-of-the-old-17106869 (Date of use: 25 September 2018)

Fischer C 'EFF amicus brief: The privacy act requires the FBI to delete files of its Internet speech surveillance' https://www.eff.org/deeplinks/2018/08/eff-amicus-brief-privacy-act-requires-fbi-delete-files-its-internet-speech (Date of use: 10 August 2018 (Fischer

https://www.eff.org/deeplinks/2018/08/eff-amicus-brief-privacy-act-requires-fbi-delete-files-its-internet-speech Date of use: 10 August 2018)

France-Presse A 'China has shut down 13,000 websites since 2015 – Xinhua' https://www.rappler.com/technology/news/192173-china-shut-down-websites-since-2015 (Date of use: 7 May 2018) (France-Presse https://www.rappler.com/technology/news/192173-china-shut-down-websites-since-2015 (Date of use: 7 May 2018)

France24 'Failed presidential candidate names parallel government in Gabon' http://www.france24.com/en/20110126-andre-mba-obame-names-parallel-government-gabon-ivory-coast (Date of use: 2 October 2016)(France24 http://www.france24.com/en/20110126-andre-mba-obame-names-parallel-government-gabon-ivory-coast (Date of use: 2 October 2016)

Francis J 'Facebook's convergence conundrum- Merging Facebook Messenger, WhatsApp and Instagram is a risky gamble and there isn't a good enough reason to do so.' https://www.itweb.co.za/content/mYZRXv9Ppd8qOgA8 (Date of use: 12 February 2019 (Francis https://www.itweb.co.za/content/mYZRXv9Ppd8qOgA8 (Date of use: 12 February 2019)

Friggieri A, Michael K and Michael M G 'The legal ramifications of microchipping people in the United States of America - a state legislative comparison' file:///f:/li-us-%20art%20-%20legal%20aspects%20of%20implanting%20micro%20chips%20in%20us%20fulltext.pdf (Date of use: 12 June 2016) (Friggieri, Michael and Michael file:///f:/li-us-%20art%20-%20legal%20aspects%20of%20implanting%20micro%20chips%20in%20us%20fulltext.pdf (Date of use: 12 June 2016)

Gerber J 'Phahlane must explain why he shouldn't be suspended – Mbalula' https://www.news24.com/SouthAfrica/News/phahlane-must-explain-why-he-shouldnt-be-suspended-mbalula-20170601 (Date of use 3 June 2018) (Gerber https://www.news24.com/SouthAfrica/News/phahlane-must-explain-why-he-shouldnt-be-suspended-mbalula-20170601 (Date of use 3 June 2018)

Global Campaign for Free Expression 'Art 19 of Global Campaign for Free Expression – Statement on the right to communicate' https://www.article19.org/data/files/pdfs/publications/right-to-communicate.pdf (Date of use: 2 December 2017 (Global Campaign for Free Expression https://www.article19.org/data/files/pdfs/publications/right-to-communicate.pdf (Date of use: 2 December 2017)

Glover S 'Facebook's refusal to help police on murder case proves it is morally callous' http://www.dailymail.co.uk/debate/article-6132479/stephen-glover-Facebooks-refusal-help-police-murder-case-proves-morally-callous.html (Date of use: 5 September 2018) (Glover http://www.dailymail.co.uk/debate/article-6132479/stephen-glover-Facebooks-refusal-help-police-murder-case-proves-morally-callous.html (Date of use: 5 September 2018)

Goko C 'Crime intelligence boss Ngcobo on special leave, credentials probed' http://www.bdlive.co.za/national/2013/10/22/crime-intelligence-boss-ngcobo-on-special-leave-credentials-probed (Date of use: 18 January 2014 (Goko http://www.bdlive.co.za/national/2013/10/22/crime-intelligence-boss-ngcobo-on-special-leave-credentials-probed (Date of use: 18 January 2014)

Goud N 'Did United States declare a cyber war on Russia?' https://www.cybersecurity-insiders.com/did-united-states-declare-a-cyber-war-on-russia/ (Date of use 12 December 2018) (Goud https://www.cybersecurity-insiders.com/did-united-states-declare-a-cyber-war-on-russia/ (Date of use 12 December 2018)

Healy L M – 'Increasing the likelihood of admissible electronic evidence: Digital log handling excellence and a forensically aware corporate culture' 2008 Eastern Michigan University, College of Technology COT 704 Final Paper http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.559.1399&rep=rep1&type=pdf (Date of use: 19 June 2017) (Healy http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.559.1399&rep=rep1&type=pdf (Date of use: 19 June 2017)

Heyink M 'Elizabeth de Stadler and Paul Esselaar 'A guide to the Protection of Personal Information Act' http://www.derebus.org.za/guide-protection-personal-information-act/

http://www.derebus.org.za/guide-protection-personal-information-act/ (Date of use: 11 June 2018) (Heyink http://www.derebus.org.za/guide-protection-personal-information-act/ http://www.derebus.org.za/guide-protection-personal-information-act/ (Date of use: 11 June 2018))

Gedye L 'Faith Muthambi likely to bear brunt of the backlash over digital fail' https://mg.co.za/article/2016-06-02-backlash-likely-over-digital-fail (Date of use: 22 April 2019 (Gedye https://mg.co.za/article/2016-06-02-backlash-likely-over-digital-fail (Date of use: 22 April 2019)

Ghosh P 'UK judges to get scientific guides' http://www.bbc.com/news/science-environment-42057009 (Date of use: 22 November 2017) (Ghosh http://www.bbc.com/news/science-environment-42057009 (Date of use: 22 November 2017)

Glover S 'Facebook's refusal to help police on murder case proves it is morally callous' http://www.dailymail.co.uk/debate/article-6132479/STEPHEN-GLOVER-Facebooks-refusal-help-police-murder-case-proves-morally-callous.html (Date of use: 5 September 2018) (Glover http://www.dailymail.co.uk/debate/article-6132479/STEPHEN-GLOVER-Facebooks-refusal-help-police-murder-case-proves-morally-callous.html (Date of use: 5 September 2018)

Google 'Google offered in: Afrikaans Sesotho isiZulu IsiXhosa Setswana Northern Sotho' https://www.google.co.za/?gws_rd=ssl (Date of use: 20 May 2017) (Google https://www.google.co.za/?gws_rd=ssl (Date of use: 20 May 2017)

Goredema C 'Profiling money laundering in Eastern and Southern Africa' http://www.issafrica.org/publications/monographs/monograph-90-profiling-money-laundering-in-eastern-and-southern-africa-charles-goredema (Date of use: 1 May 2017) (Goredema http://www.issafrica.org/publications/monographs/monograph-90-profiling-money-laundering-in-eastern-and-southern-africa-charles-goredema (Date of use: 1 May 2017)

Goud N 'Did United States declare a cyber war on Russia?' https://www.cybersecurity-insiders.com/did-united-states-declare-a-cyber-war-on-russia/ (Date of use: 12 December 2018) (Goud https://www.cybersecurity-insiders.com/did-united-states-declare-a-cyber-war-on-russia/ (Date of use: 12 December 2018))

Gupta V 'What do you mean by parallel government and cooperative federalism in India?' https://www.quora.com/What-do-you-mean-by-parallel-government-and-cooperative-federalism-in-India (Date of use: 2 October 2016) (Gupta https://www.quora.com/What-do-you-mean-by-parallel-government-and-cooperative-federalism-in-India (Date of use: 2 October 2016)

Harper P 'Cele takes aim at crime intelligence' https://mg.co.za/article/2018-03-02-00-cele-takes-aim-at-crime-intelligence (Date of use: 19 June 2018 (Harper https://mg.co.za/article/2018-03-02-00-cele-takes-aim-at-crime-intelligence (Date of use: 19 June 2018)

Hartley W 'Single intelligence body wields great power' http://www.bdlive.co.za/national/2013/08/08/single-intelligence-body-wields-great-power (Date of use: 28 February 2017) (Hartley http://www.bdlive.co.za/national/2013/08/08/single-intelligence-body-wields-great-power (Date of use: 28 February 2017)

Hartley W 'Loopholes in interceptions law 'Raise Red Flag' available at http://www.bdlive.co.za/national/2014/03/25/loopholes-in-interceptions-law-raise-red-flag (Date of use: 28 March, 2014) (Hartley http://www.bdlive.co.za/national/2014/03/25/loopholes-in-interceptions-law-raise-red-flag (Date of use: 28 March, 2014)

HAWKS 'Vacancy in the Directorate for Priority Crime Investigation (DPCI)' http://www.policesecretariat.gov.za/downloads/posts/VACANCY_THE_DIRECTORATE_FOR%20PRIORITY_CRIME_INVESTIGATION_(DPCI).pdf (Date of use: 3 May, 2018) (HAWKS http://www.policesecretariat.gov.za/downloads/posts/VACANCY_THE_DIRECTORATE_FOR%20PRIORITY_CRIME_INVESTIGATION_(DPCI).pdf (Date of use: 3 May, 2018)

Head T "Not a k***** in sight" – SA tourist causes fury with "K-word" beach rant [video] https://city-press.news24.com/News/holidaymaker-to-face-charges-for-racist-viral-video-shot-abroad-20180822 (Date of use: 1 November, 2018 (Head https://city-press.news24.com/News/holidaymaker-to-face-charges-for-racist-viral-video-shot-abroad-20180822 (Date of use:1 November 2018)

Heyink M 'A guide to the Protection of Personal Information Act- De Stadler E and Esselaar P' http://www.derebus.org.za/guide-protection-personal-information-act/ (Date of use: 12 January, 2019 (Heyink http://www.derebus.org.za/guide-protection-personal-information-act/ (Date ofuse: 12 January 2019)

Hinnen T M 'Developing a legal framework to combat cybercrime- Providing law enforcement with the legal tools to prevent, investigate, and prosecute cybercrime' www.oas.org/juridico/spanish/cybGE_IIIinf6.ppt (Date of use:
12 June 2017) (Hinnen www.oas.org/juridico/spanish/cybGE_IIIinf6.ppt (Date of use: 12 June 2017)

Hoffman P 'Hawks in SAPS are neither effective nor sufficiently independent' http://www.ifaisa.org/Hawks_neither_effective_nor_sufficiently_independent.html (Date of use: 20 January 2017) (Hoffman http://www.ifaisa.org/Hawks_neither_effective_nor_sufficiently_independent.html (Date of use: 20 January 2017)

Hosken G and Quintal G 'Foreign cops do SA's job as FBI, UK agencies probe Guptas' https://www.timeslive.co.za/news/south-africa/2017-10-20-foreign-cops-do-sas-job-as-fbi-uk-agencies-probe-guptas/ (Date of use: 12 June 2018) (Hosken and Quintal https://www.timeslive.co.za/news/south-africa/2017-10-20-foreign-cops-do-sas-job-as-fbi-uk-agencies-probe-guptas/ (Date of use:12 June 2018)

Hunter M and Smith T *Spooked: Surveillance of journalists in South Africa* https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018) (Hunter and Smith https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use : 27 November 2018)

Human Rights Council 'The right to privacy in the digital age' https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (Date of use: 13 December 2017) (Human Rights Council https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (Date of use: 13 December 2017)

Hunter Q 'Cyril Ramaphosa 'give back' Gavin Watson's R500,000' https://www.timeslive.co.za/sunday-times/news/2019-02-03-cyril-ramaphosa-gives-back-gavin-watsons-r500000/ (Date of use: 24 June 2019) (Hunter https://www.timeslive.co.za/sunday-times/news/2019-02-03-cyril-ramaphosa-gives-back-gavin-watsons-r500000/ (Date of use: 24 June 2019)

Hunter M and Thakur C 'Advocacy: New privacy rules for Covid-19 tracking a step in the right direction, but …' https://www.news24.com/Columnists/GuestColumn/advocacy-new-privacy-rules-for-covid-19-tracking-a-step-in-the-right-direction-but-20200404-2 (Date ofuse: 6 April 2020 (Hunter and Thakur https://www.news24.com/Columnists/GuestColumn/advocacy-new-privacy-rules-for-covid-19-tracking-a-step-in-the-right-direction-but-20200404-2 (Date of use: 6 April 2020)

IPID 'POST 16/28:PROVINCIAL HEAD REF NO: Q9/2019/1' file:///F:/LI-SA-%20ART-%20IPID%20-%20ADVERT%20FOR%20PROVINCIAL%20HEAD%20OF%20IPID%20-%202019.pdf (Date of use : 21 May 2019 (IPID file:///F:/LI-SA-%20ART-%20IPID%20-%20ADVERT%20FOR%20PROVINCIAL%20HEAD%20OF%20IPID%20-%202019.pdf (Date of use: 21 May 2019)

Intelligence 'White paper on Intelligence' http://www.oigi.gov.za/Legislation/white_paper_on_intelligence.htm (Date of use: 20 January 2017)(Intelligence http://www.oigi.gov.za/Legislation/white_paper_on_intelligence.htm (Date of use: 20 January 2017)

Interpol ''Best practices' in combating terrorism' http://www.INTERPOL.int/Public/Region/Default.asp (Date of use: 12 April 2017) (Interpol http://www.INTERPOL.int/Public/Region/Default.asp (Date of use: 12 April 2017)

IOL News 'SANDF members protest at the Union Buildings' http://www.iol.co.za/news/sandf-members-protest-at-the-union-buildings-1.676456 (Date of use: 18 June 2012) (IOL News http://www.iol.co.za/news/sandf-members-protest-at-the-union-buildings-1.676456 (Date of use: 18 June 2012)

IOL 'NPA is the picture of success, says Ngcuka' https://www.iol.co.za/news/politics/npa-is-the-picture-of-success-says-ngcuka-205848 (Date of use: 7 February 2019) (IOL https://www.iol.co.za/news/politics/npa-is-the-picture-of-success-says-ngcuka-205848 (Date of use: 7 February 2019)

Jika T, Hunter Q and Wa Afrika M 'State Capture -Sink or sing for Duduzane' https://www.pressreader.com/ (Date of use: 12 June 2018 (Jika et al https://www.pressreader.com/ (Date of use: 12 June 2018)

Justice Information Sharing 'Electronic Communication Privacy Act 1986 (ECPA), 18 U.S.C s 2510-22' https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (Date of use: 2 April 2016) (Justice Information Sharing https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (Date of use: 2 April 2016))

Kaspersen H W K 'Cybercrime and internet jurisdiction' Discussion paper for project on cybercrime' version 2009 www.coe.int/cybercrime (Date of use: 24 June, 2016) (Kaspersen www.coe.int/cybercrime (Date of use: 24 June 2016)

Kaspersen H W K 'Cybercrime and internet jurisdiction' https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803042b7 (Date of use: 18 February 2017) Kaspersen https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803042b7 (Date of use: 18 February 2017)

Kerr O S 'Digital evidence and the new criminal procedure' - the George Washington University Law School Public Law and Legal Theory Working Paper No. 108

http://ssrn.com/abstract=594101 (Date of use: 16 April 2013) (Kerr http://ssrn.com/abstract=594101 (Date of use: 16 April 2013)

Kgosana C 'The great spook purge: Agents claim move is directed at flushing out 'Zuma's loyalists' https://www.timeslive.co.za/politics/2018-11-11-the-great-spook-purge-agents-claim-move-is-directed-at-flushing-out-zuma-loyalists/ (Date of use : 15 December, 2018 (Kgosana https://www.timeslive.co.za/politics/2018-11-11-the-great-spook-purge-agents-claim-move-is-directed-at-flushing-out-zuma-loyalists/ (Date of use: 15 December 2018)

Kok J N et al. 'Artificial intelligence: definition, trends, techniques, and cases' http://www.eolss.net/sample-chapters/c15/e6-44.pdf (Date of use: 22 November 2019) (Kok J N et al. 'Artificial intelligence: definition, trends, techniques, and cases' http://www.eolss.net/sample-chapters/c15/e6-44.pdf (Date of use: 22 November 2019))

Koops B and Goodwin M 'Cyberspace, the cloud and cross-border criminal investigation-Limits and possibilities of international law' www.tilburguniversity.edu/tilt (Date of use: 14 December 2016) (Koops and Goodwin www.tilburguniversity.edu/tilt (Date of use:14 December 2016)

Kravets D 'Obama administration says that the world's servers are ours: US says' https://www.google.co.za/?gws_rd=ssl#q=Obama+administration+says+the+world%E2%80%99s+servers+are+ours (Date of use: 2 July 2015) (Kravets https://www.google.co.za/?gws_rd=ssl#q=Obama+administration+says+the+world%E2%80%99s+servers+are+ours (Date of use: 2 July 2015)

Kravets D 'Microsoft tells US: The world's servers are not yours' http://arstechnica.com/tech-policy/2014/12/microsoft-tells-us-the-worlds-servers-are-not-yours-for-the-taking/ (Date of use: 2 July 2015) (Kravets http://arstechnica.com/tech-policy/2014/12/microsoft-tells-us-the-worlds-servers-are-not-yours-for-the-taking/ (Date of use: 2 July 2015)

Jika T, Hunter Q and Wa Afrika M 'State capture-sink or sing for Duduzane' https://www.pressreader.com/ (Date of use: 12 June 2018) (Jika et al https://www.pressreader.com/ (Date of use: 12 June 2018)

Joint Standing Committee on Intelligence 'Annual report of the Joint Standing Committee on Intelligence for financial year ending 31 March 2010' http://www.pmg.org.za/docs/2011/comreports/110921jcintelligencereport.htm accessed (Date of use: 13 October 2013 (Joint Standing Committee on Intelligence http://www.pmg.org.za/docs/2011/comreports/110921jcintelligencereport.htm (Date of use: 13 October 2013)

Laperruque J 'Facial recognition surveillance faces new legal limit' https://www.axios.com/facial-recognition-surveillance-faces-new-calls-legal-limits-e99794ee-5fe1-45f8-bbc8-0ef0450d93d1.html (Date of use: 14 April 2019) (Laperruque https://www.axios.com/facial-recognition-surveillance-faces-new-calls-legal-limits-e99794ee-5fe1-45f8-bbc8-0ef0450d93d1.html (Date of use: 14 April 2019))

Le Roux L 'The post-apartheid South African military: Transforming with the nation' *Evolution and Revolutions* 259 http://www.issafrica.org/pubs/Books/Evol_Revol%20Oct%2005/Chap9.pdf (Date of use: 6 March 2014) Le Roux http://www.issafrica.org/pubs/Books/Evol_Revol%20Oct%2005/Chap9.pdf (Date of use: 6 March 2014)

Letsoalo M 'Spooks' cash 'used to spy on Cyril Ramaphosa'' https://mg.co.za/article/2017-09-08-00-secret-funds-used-to-spy-on-cyril (Date of use: 8 September 2017) (Letsoalo https://mg.co.za/article/2017-09-08-00-secret-funds-used-to-spy-on-cyril (Date of use: 8 September 2017)

Louw J and Giliomee C L 'Corporate crime, fraud and investigations in South Africa: Overview' www.practicallaw.com/corporatecrime-mjg (Date of use: 28 June 2016 (Louw and Giliomee www.practicallaw.com/corporatecrime-mjg (Date of use: 28 June 2016)

Lotz B 'How wide spread is state surveillance in SA? Right2Know is trying to find out' http://www.htxt.co.za/2017/05/25/how-wide-spread-is-state-surveillance-in-sa-right2know-is-trying-to-find-out/ (Date of use: 31 May 2017) (Lotz

http://www.htxt.co.za/2017/05/25/how-wide-spread-is-state-surveillance-in-sa-right2know-is-trying-to-find-out/ (Date of use: 31 May 2017)

Luck R 'RICA' http://www.saflii.org/za/journals/DEREBUS/2014/6.html (Date of use: 27 June 2019) (Luck http://www.saflii.org/za/journals/DEREBUS/2014/6.html (Date of use: 27 June 2019))

Mabena S 'Uber operators must apply for operating licences: transport minister' https://www.timeslive.co.za/news/south-africa/2017-07-10-uber-operators-must-apply-for-operating-licences-transport-minister/ (Date of use: 10 July 2017) (Mabena https://www.timeslive.co.za/news/south-africa/2017-07-10-uber-operators-must-apply-for-operating-licences-transport-minister/ (Date of use: 10 July 2017)

Mabuza E 'EXPLAINER | What the law says about declaring a state of emergency' https://www.timeslive.co.za/news/south-africa/2017-12-12-explainer--what-the-law-says-about-declaring-a-state-of-emergency/ (Date of use: 12 March 2018) (Mabuza https://www.timeslive.co.za/news/south-africa/2017-12-12-explainer--what-the-law-says-about-declaring-a-state-of-emergency/ (Date of use: 12 March 2018)

Mabuza E 'Claims President Cyril Ramaphosa is being investigated for money-laundering bizarre: Chauke' https://www.timeslive.co.za/politics/2019-06-24-claims-president-cyril-ramaphosa-is-being-investigated-for-money-laundering-bizarre-chauke/ (Date of use: 24 June 2019) (Mabuza https://www.timeslive.co.za/politics/2019-06-24-claims-president-cyril-ramaphosa-is-being-investigated-for-money-laundering-bizarre-chauke/ (Date of use: 24 June 2019)

Maduna M of Power Digital 'Duduza Clinic remains closed after nurse tests positive for corona virus' https://www.power987.co.za/news/duduza-clinic-remains-closed-after-nurse-tests-positive-for-coronavirus/ (Date of use: 3 April 2020) (Maduna M of Power Digital https://www.power987.co.za/news/duduza-clinic-remains-closed-after-nurse-tests-positive-for-coronavirus/ (Date of use: 3 April 2020))

Mahome R and Bendimerad R 'Venezuela shuts down Internet amid protests' https://www.aljazeera.com/news/2019/01/venezuela-shuts-internet-protests-

190124124829727.html (Date of use 29 January 2019) (Mahome and Bendimerad https://www.aljazeera.com/news/2019/01/venezuela-shuts-internet-protests-190124124829727.html (Date of use 29 January 2019))

Mail and Guardian "Secret state tighten screws" http://mg.co.za/print/2011-10-14-secret-state-tightens-screws (Date of use: 17 September 2016) (Mail and Guardian http://mg.co.za/print/2011-10-14-secret-state-tightens-screws (Date of use: 17 September 2016)

Mail and Guardian 'Zille maintains her calls were being monitored' http://mg.co.za/article/2011-03-09-zille-maintains-her-calls-were-being-monitored (Date of use: 18 April 2016) (Mail and Guardian http://mg.co.za/article/2011-03-09-zille-maintains-her-calls-were-being-monitored (Date of use: 18 April, 2016)

Mail and Guardian 'Zuma: SA not immune to security threats' http://mg.co.za/article/2009-12-03-zuma-sa-not-immune-to-security-threats (Date of use: 18 April, 2016) (Mail and Guardian http://mg.co.za/article/2009-12-03-zuma-sa-not-immune-to-security-threats (Date of use: 18 April, 2016)

Mailovich C 'Cyril Ramaphosa set to sign proclamation to establish NPA directorate' https://www.businesslive.co.za/bd/national/2019-03-19-breaking-news-cyril-ramaphosa-set-to-sign-proclamation-on-npa-directorate/ (Date of use: 31March, 2019) (Mailovich https://www.businesslive.co.za/bd/national/2019-03-19-breaking-news-cyril-ramaphosa-set-to-sign-proclamation-on-npa-directorate/ (Date of use: 31March, 2019)

Mailovich C and Shange N 'Anthony Jacobs first new permanent head of crime intelligence in seven years'https://www.businesslive.co.za/bd/national/2018-03-29-anthony-jacobs-first-new-permanent-head-of-crime-intelligence-in-seven-years/ (Date of use: 21 December 2018) (Mailovich and Shange https://www.businesslive.co.za/bd/national/2018-03-29-anthony-jacobs-first-new-permanent-head-of-crime-intelligence-in-seven-years/ (Date of use: 21 December 2018)

Maphanga C ‘Police documents were classified to hinder intelligence investigations, Zondo commission hears’ https://www.news24.com/SouthAfrica/News/police-documents-were-classified-to-hinder-intelligence-investigations-zondo-commission-hears-20190917 (Date of use: 18 September 2019)(Maphanga https://www.news24.com/SouthAfrica/News/police-documents-were-classified-to-hinder-intelligence-investigations-zondo-commission-hears-20190917 (Date of use: 18 September 2019)

Maphumulo S ‘Cops in 'super-spy' machine probe’ https://www.iol.co.za/news/cops-in-super-spy-machine-probe-1907719 (Date of use: 17 August 2016) (Maphumulo https://www.iol.co.za/news/cops-in-super-spy-machine-probe-1907719 (Date of use: 17 August 2016) (Maphumulo https://www.iol.co.za/news/cops-in-super-spy-machine-probe-1907719 (Date of use: 17 August 2016)

Maphumulo S ‘Police training reduced to 8 months’ https://www.iol.co.za/news/police-training-reduced-to-8-months-2012636 (Date of use: 16 November 2018) (Maphumulo https://www.iol.co.za/news/police-training-reduced-to-8-months-2012636 (Date of use: 16 November 2018)

Maphumulo S ‘Phiyega facing criminal charges’ http://www.iol.co.za/news/crime-courts/phiyega-facing-criminal-charges-1.1597315#.U2jYZ08aLMw (Date of use: 13 March 2014) (Maphumulo http://www.iol.co.za/news/crime-courts/phiyega-facing-criminal-charges-1.1597315#.U2jYZ08aLMw (Date of use: 13 March 2014))

Maqhina M ‘Minister meddling in Icasa affairs’ https://www.iol.co.za/news/politics/minister-meddling-in-icasa-affairs-22163646 (Date of use: 1 May, 2019 (Maqhina https://www.iol.co.za/news/politics/minister-meddling-in-icasa-affairs-22163646 (Date of use: 1 May 2019)

Mare A and Duncan J ‘An analysis of the communications surveillance legislative framework in South Africa: Media policy and democracy project’ (2015)’ http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf (Date of use: 1 December 2017**)** (Mare and Duncan http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf (Date of use: 1 December 2017)

McAfee 'Certified Professional Criminal Investigator (CPCI') https://www.mcafeeinstitute.com/products/certified-professional-criminal-investigator-cpci (Date of use:1 February 2018) (McAfee https://www.mcafeeinstitute.com/products/certified-professional-criminal-investigator-cpci (Date of use:1 February 2018))

McKan J 'SAPS wanted to pay R45 million for cellphone spy hardware to fund Zuma' https://mybroadband.co.za/news/government/292800-saps-wanted-to-pay-r45-million-for-cellphone-spy-hardware-to-fund-zuma.html (Date of use: 28 January 2019) (McKan https://mybroadband.co.za/news/government/292800-saps-wanted-to-pay-r45-million-for-cellphone-spy-hardware-to-fund-zuma.html (Date of use: 28 January 2019)

McKinley D T 'New terrains of privacy in South Africa' https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/r2kmpdp_new_terrains_of_privacy_in_south__africa_masterset_small.pdf (Date of use: 5 July, 2018) (McKinley https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/r2kmpdp_new_terrains_of_privacy_in_south__africa_masterset_small.pdf (Date of use: 5 July 2018)

McLeod S 'Communication rights: Fundamental human rights for all' https://www.tandfonline.com/doi/full/10.1080/17549507.2018.1428687 (Date of use: 7 June 2018) (McLeod https://www.tandfonline.com/doi/full/10.1080/17549507.2018.1428687 (Date of use: 7 June 2018)

Mashego A and Masondo S 'Secret plot to oust Mbaks' https://www.news24.com/SouthAfrica/News/secret-plot-to-oust-mbaks-20170827-2 (Date of use: 30 August 2017) **(**Mashego and Masondo https://www.news24.com/SouthAfrica/News/secret-plot-to-oust-mbaks-20170827-2 (Date of use: 30 August 2017)

Martin C V S 'Jurisdictional aspects of cloud computing' 2009 https://rm.coe.int/16802f2627 (Date of use: 18 July 2017) (Martin https://rm.coe.int/16802f2627 (Date of use: 18 July 2017)

Mawson N 'SA's spy bill edges closer' http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=30776:sas-

spy-bill-edges-closer&catid=49:National%20Security&Itemid=115 (Date of use: 13 June 2016) (Mawson http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=30776:sas-spy-bill-edges-closer&catid=49:National%20Security&Itemid=115 (Date of use: 13 June 2016)

Mbhele Z 'Professionalise the police and start with its leaders' https://www.news24.com/Columnists/GuestColumn/professionalise-the-police-and-start-with-its-leaders-20190328 (Date of use: 31 March 2019) (Mbhele https://www.news24.com/Columnists/GuestColumn/professionalise-the-police-and-start-with-its-leaders-20190328 (Date of use: 31 March 2019)

Merten M 'Glynnis Breytenbach: Decision to withdraw from 'dream job' made easier due to other competent candidates' https://www.dailymaverick.co.za/article/2018-11-14-glynnis-breytenbach- decision-to-withdraw-from-dream-job-made-easier-due-to-other-competent-candidates/ (Date of use: 16 November 2018 (Merten https://www.dailymaverick.co.za/article/2018-11-14-glynnis-breytenbach- decision-to-withdraw-from-dream-job-made-easier-due-to-other-competent-candidates/ (Date of use: 16 November 2018)

Michalson 'United Nations concerned about privacy and interception in South Africa' https://www.michalsons.com/blog/un-human-rights-committee-concerned-about-privacy-and-interc (Date of use: 18 January 2019) (Michalson https://www.michalsons.com/blog/un-human-rights-committee-concerned-about-privacy-and-interc (Date of use: 18 January 2019)

Michaels R 'Some fundamental jurisdictional conceptions as applied in Judgment Conventions' https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2281&context=faculty_scholarship (Date of use: 21 March 2016) (Michaels https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=2281&context=faculty_scholarship (Date of use: 21 March 2016)

Microsoft 'Set a password to help protect your outlook information' https://support.office.com/en-us/article/Set-a-password-to-help-protect-your-Outlook-

information-2589f1b1-c911-4b94-bceb-30ea098d6401 (Date of use: 12 June 2016) (Microsoft https://support.office.com/en-us/article/Set-a-password-to-help-protect-your-Outlook-information-2589f1b1-c911-4b94-bceb-30ea098d6401 (Date of use: 12 June 2016)

Miller G and Jaffe G 'Trump revealed highly classified information to Russian foreign minister and ambassador' https://www.washingtonpost.com/world/national-security/trump-revealed-highly-classified-information-to-russian-foreign-minister-and-ambassador/2017/05/15/530c172a-3960-11e7-9e48-c4f199710b69_story.html?utm_term=.6c16f1420aae (Date of use: 15 May 2017) (Miller and Jaffe https://www.washingtonpost.com/world/national-security/trump-revealed-highly-classified-information-to-russian-foreign-minister-and-ambassador/2017/05/15/530c172a-3960-11e7-9e48-c4f199710b69_story.html?utm_term=.6c16f1420aae (Date of use: 15 May 2017)

Mills B 'Why we should consider the privacy of animals' https://www.theguardian.com/commentisfree/cif-green/2010/apr/30/animals-privacy-wildlife-ethical (Date of use: 12 January 2016) (Mills https://www.theguardian.com/commentisfree/cif-green/2010/apr/30/animals-privacy-wildlife-ethical (Date of use: 12 January 2016)

Ministry of State Security 'Statement on recent developments relating to the management of State Security Agency' http://www.ssa.gov.za/Portals/0/SSA%20docs/Media%20Releases/2013/Media%20Release%20Statement%20on%20recent%20developments%20relating%20to%20the%20State%20Security%20Agency%202%20August%202013.pdf (Date of use:14 October 2013) (Ministry http://www.ssa.gov.za/Portals/0/SSA%20docs/Media%20Releases/2013/Media%20Release%20Statement%20on%20recent%20developments%20relating%20to%20the%20State%20Security%20Agency%202%20August%202013.pdf (Date of use:14 October 2013)

Mitchley A 'Crime Intelligence boss position up for grabs available at https://www.news24.com/SouthAfrica/News/crime-intelligence-boss-position-up-for-grabs-20180117 (Date of use: 16 November 2018 (Mitchley https://www.news24.com/SouthAfrica/News/crime-intelligence-boss-position-up-for-grabs-20180117 (Date of use: 16 November 2018)

Monks K 'Forget wearable tech, embeddable implants are already here' http://edition.cnn.com/2014/04/08/tech/forget-wearable-tech-embeddable-implants/ (Date of use: 12 June 2014) (Monks http://edition.cnn.com/2014/04/08/tech/forget-wearable-tech-embeddable-implants/ (Date of use: 12 June 2014)

Moorcroft J 'POPI and the legal profession: What should you know? http://www.derebus.org.za/popi-legal-profession-know/ (Date of use: 18 January 2019) (Moorcroft http://www.derebus.org.za/popi-legal-profession-know/ (Date of use: 18 January 2019)

Moyo A 'Only 3.5% of SA's households don't have phones' https://www.itweb.co.za/content/JOlx4z7kVpv56kmW (Date of use: 26 June 2017) (Moyo https://www.itweb.co.za/content/JOlx4z7kVpv56kmW (Date of use: 26 June 2017)

Mukadam S and Van Vuuren H 'Written submission: General Intelligence Laws Amendment Bill [B25-2011]' http://db3sqepoi5n3s.cloudfront.net/files/docs/120322iss_1.rtf (Date of use: 3 March 2013) **(**Mukadam and Van Vuuren http://db3sqepoi5n3s.cloudfront.net/files/docs/120322iss_1.rtf (Date of use: 3 March 2013**)**

Mutsaka F 'Former Zimbabwe fin min Tendai Biti convicted of making false election declaration' https://www.iol.co.za/news/africa/former-zimbabwe-finmin-tendai-biti-convicted-of-making-false-election-declaration-19362547 (Date of use: 12 February 2019) (Mutsaka https://www.iol.co.za/news/africa/former-zimbabwe-finmin-tendai-biti-convicted-of-making-false-election-declaration-19362547 (Date of use: 12 February 2019)

Naidoo S 'SAPS should boost its crime intelligence division: ISS' http://www.sabcnews.com/sabcnews/saps-boost-crime-intelligence-division-iss/ (Date of use 18 March 2018 (Naidoo http://www.sabcnews.com/sabcnews/saps-boost-crime-intelligence-division-iss/ (Date of use:18 March 2018)

Nakashima E 'Pentagon launches first cyber operation to deter Russian interference in midterm elections' https://www.washingtonpost.com/world/national-security/pentagon-launches-first-cyber-operation-to-deter-russian-interference-in-midterm-elections/2018/10/23/12ec6e7e-d6df-11e8-83a2-d1c3da28d6b6_story.html?utm_term=.481584E67641 (Date of use :12

December 2018) (Nakashima https://www.washingtonpost.com/world/national-security/pentagon-launches-first-cyber-operation-to-deter-russian-interference-in-midterm-elections/2018/10/23/12ec6e7e-d6df-11e8-83a2-d1c3da28d6b6_story.html?utm_term=.481584E67641 (Date of use :12 December 2018)

National Defence Force Intelligence Division 'Intelligence' http://www.globalsecurity.org/intell/world/rsa/df_id.htm (Date of use: 12 January 2014)(National Defence Force Intelligence Division http://www.globalsecurity.org/intell/world/rsa/df_id.htm (Date of use: 12 January 2014))

National Rapporteur on Trafficking in Human Beings, 'Child pornography – First report of the Dutch National Rapporteur' (2011) http://www1.umn.edu/humanrts/research/Netherlands/Netherlands_child-pornography_report_2011_en.pdf. (Date of use: 12 December 2016)(National Rapporteur on Trafficking in Human Beings (2011) http://www1.umn.edu/humanrts/research/Netherlands/Netherlands_child-pornography_report_2011_en.pdf. (Date of use: 12 December 2016)

Naughton J 'We have been harmonised: Life in China's surveillance State by Kai Strittmatter – review - A remarkable analysis identifies 'Mao 2.0' as the west's new cold war adversary' https://www.theguardian.com/books/2019/jun/30/we-have-been-harmonised-life-china-surveillance-state-kai-strittmatter-review (Date of use: 2 July 2019) (Naughton https://www.theguardian.com/books/2019/jun/30/we-have-been-harmonised-life-china-surveillance-state-kai-strittmatter-review (Date of use: 2 July 2019))

Necessary and Proportionate 'Necessary and proportionate principles' http://es.necessaryandproportionate.org (Date of use: 12 December 2016) (Necessary and Proportionate http://es.necessaryandproportionate.org (Date of use: 12 December 2016)

Negres M C 'The passing of the general Intelligence Law Amendment Bill [B25-2011] http://www.pmg.org.za/report (Date of use: 5 June 2016) (Negres http://www.pmg.org.za/report (Date of use: 5 June 2016)

News24 Wire ‘Sanef shocked by allegations Mantashe paid reporters for sex story to ‘go away’’ https://citizen.co.za/news/south-africa/politics/2196647/sanef-shocked-by-allegations-mantashe-paid-reporters-for-sex-story-to-go-away/ (Date of use: 28 October 2019) (News24 Wire https://citizen.co.za/news/south-africa/politics/2196647/sanef-shocked-by-allegations-mantashe-paid-reporters-for-sex-story-to-go-away/ (Date of use: 28 October 2019))

News24 ‘Mantashe denies bribing journos R70K to make sex scandal go away’ https://citizen.co.za/news/south-africa/politics/2197320/mantashe-denies-bribing-journos-r70k-to-make-sex-scandal-go-away/ (Date of use: 11 November 2019) (News24 https://citizen.co.za/news/south-africa/politics/2197320/mantashe-denies-bribing-journos-r70k-to-make-sex-scandal-go-away/ (Date of use: 11 November 2019))

News24 ‘Loyalty to factions vs the state: A blurring of lines’ https://www.news24.com/Columnists/GuestColumn/loyalty-to-factions-vs-the-state-a-blurring-of-lines-20190407 (Date of use: 4 August 2019) (News24 https://www.news24.com/Columnists/GuestColumn/loyalty-to-factions-vs-the-state-a-blurring-of-lines-20190407 (Date of use: 4 August 2019)

Ngqakamba S ‘New NPA boss: Advisory panel veers away from the usual appointment process’ https://www.news24.com/SouthAfrica/News/new-npa-boss-selection-panel-met-for-first-time-set-time-frame-20181022 (Date of use: 16 November 2018) (Ngqakamba https://www.news24.com/SouthAfrica/News/new-npa-boss-selection-panel-met-for-first-time-set-time-frame-20181022 (Date of use: 16 November 2018)

Nicholaides G ‘Could artificial intelligence become our greatest enemy?’ http://www.702.co.za/articles/604/could-artificial-intelligence-become-our-greatest-enemy (Date of use: 12 January 2017) (Nicholaides http://www.702.co.za/articles/604/could-artificial-intelligence-become-our-greatest-enemy (Date of use: 12 January 2017)

Nicolson G ‘State capture: Madonsela needs funds to investigate as Jonas speaks out again’ https://www.dailymaverick.co.za/article/2016-06-08-state-capture-madonsela-needs-funds-to-investigate-as-jonas-speaks-out-again/ (Date of use: 9 May 2018) (Nicolson https://www.dailymaverick.co.za/article/2016-06-08-state-capture-madonsela-needs-funds-to-investigate-as-jonas-speaks-out-again/ (Date of use: 9 May 2018)

NRSO ‘FAQ: National register for sex offenders (NRSO)’ http://www.justice.gov.za/vg/nrso.html#sthash.l1ApZaBz.dpuf (Date of use: 12 June 2016)(NRSO http://www.justice.gov.za/vg/nrso.html#sthash.l1ApZaBz.dpuf (Date of use: 12 June 2016)

NYU ‘What is research design?’ https://www.nyu.edu/classes/bkg/methods/005847ch1.pd f (Date of use: 23 October 2018) (NYU https://www.nyu.edu/classes/bkg/methods/005847ch1.pd f (Date of use: 23 October 2018)

OECD “Effective means of investigation and prosecution of corruption” http://www.oecd.org/corruption/acn/47588859.pdf (Date of use: 21 March 2016) (OECD http://www.oecd.org/corruption/acn/47588859.pdf (Date of use: 21 March 2016)

OIGI ‘Effective investigation-White paper on intelligence’ http://www.oigi.gov.za/Legislation/white_paper_on_intelligence.htm (Date of use: 20 January 2014) (OIGI http://www.oigi.gov.za/Legislation/white_paper_on_intelligence.htm (Date of use: 20 January 2017)

Michalson ‘ United Nations concerned about privacy and interception in South Africa’ https://www.michalsons.com/blog/un-human-rights-committee-concerned-about-privacy-and-interc (Date of use: 18 January 2019) (Michalson https://www.michalsons.com/blog/un-human-rights-committee-concerned-about-privacy-and-interc (Date of use: 18 January 2019)

OIGI ‘White paper on intelligence’ http://www.oigi.gov.za/Legislation/white_paper_on_intelligence.htm (Date of use 20 January 2014 (OIGI http://www.oigi.gov.za/Legislation/white_paper_on_intelligence.htm (Date of use: 20 January 2014)

Olivarez-Giles N ‘United Nations report: Internet access is a human right’ https://latimesblogs.latimes.com/technology/2011/06/united-nations-report-internet-access-is-a-human-right.html (Date of use: 25 December 2018) (Olivarez-Giles https://latimesblogs.latimes.com/technology/2011/06/united-nations-report-internet-access-is-a-human-right.html (Date of use: 25 December 2018)

Olschimke M 'Dual sovereignty and parallel government' http://www.olschimke.eu/2012/01/14/dual-sovereignty-and-parallel-government/ (Date of use: 2 Octobber 2016) (Olschimke http://www.olschimke.eu/2012/01/14/dual-sovereignty-and-parallel-government/ (Date of use: 2 Octobber 2016))

Omarjee L 'Mboweni vs Makhura: Tense standoff over e-tolls' https://www.fin24.com/Economy/mboweni-vs-makhura-tense-standoff-over-e-tolls-20190705 (Date of use: 5 September 2019 (Omarjee https://www.fin24.com/Economy/mboweni-vs-makhura-tense-standoff-over-e-tolls-20190705 (Date of use: 5 September 2019)

Osula A 'Accessing extraterritorially located data: Options for states' 2015 https://ccdcoe.org/sites/default/files/multimedia/pdf/Accessing%20extraterritorially%20located%20data%20options%20for%20States_Anna-Maria_Osula.pdf (Date of use: 16 February 2017) (Osula https://ccdcoe.org/sites/default/files/multimedia/pdf/Accessing%20extraterritorially%20located%20data%20options%20for%20States_Anna-Maria_Osula.pdf (Date of use: 16 February 2017)

Oneale L 'Crime Intelligence of South Africa is a complete fiasco' http://guardianlv.com/2014/01/crime-intelligence-of-south-africa-is-a-complete-fiasco/ (Date of use: 20 January, 2014) (Oneale http://guardianlv.com/2014/01/crime-intelligence-of-south-africa-is-a-complete-fiasco/ (Date of use: 20 January 2014)

O'Regan K and McKaiser E 'Regulation is clear, information contained will only be used to fight COVID-19' http://www.702.co.za/articles/379998/regulation-is-clear-information-contained-will-only-be-used-to-fight-covid-19 (Date of use: 6 April 2020 (O'Regan and McKaiser http://www.702.co.za/articles/379998/regulation-is-clear-information-contained-will-only-be-used-to-fight-covid-19 (Date of use: 6 April 2020)

Oxford University Press 'Secret' http://www.oxforddictionaries.com/definition/english-thesaurus/secret (Date of use: 6 February 2016)

Oxford Analytica ‘South Africa Army incapacity mars foreign policy goals’ https://www.oxan.com/display.aspx?ItemID=DB190015 (Dated of use: 15 April 2014 (Oxford Analytica https://www.oxan.com/display.aspx?ItemID=DB190015 (Date of use: 15 April 2014)

Pagliery J ‘How the NSA can 'turn on' your phone remotely’ https://money.cnn.com/2014/06/06/technology/security/nsa-turn-on-phone/ (Date of use: 27 April 2016) (Pagliery https://money.cnn.com/2014/06/06/technology/security/nsa-turn-on-phone/ (Date of use: 27 April 2016)

Parliamentary Monitoring Group ‘Question 842 of 2013/17B Parliamentary Monitoring Group question posed to the Minister of Police’ http://www.pmg.org.za/node/36638 (Date of use: 12 December 2013) (Parliamentary Monitoring Group http://www.pmg.org.za/node/36638 (Date of use: 12 December 2013)

PMG ‘Report of the Joint Standing Committee on Intelligence on activities of the committee after 5 months of establishment, as stipulated in the Intelligence Services Oversight Act, Act 40 of 1994, dated 10 February 2015’ https://pmg.org.za/tabled-committee-report/2307/ (Date of use: 5 April 2016) (PMG https://pmg.org.za/tabled-committee-report/2307/ (Date of use: 5 April 2016)

Phakathi B ‘Police committee agrees on not renewing Robert McBribe’s contract as IPID boss-DA MPs have criticised the committee’s decision and boycotted the session during which the report was adopted’ https://www.timeslive.co.za/politics/2019-02-28-police-committee-agrees-on-not-renewing-robert-mcbrides-contract-as-ipid-boss/ (Date of use: 8 March 2019 **(**Phakathi https://www.timeslive.co.za/politics/2019-02-28-police-committee-agrees-on-not-renewing-robert-mcbrides-contract-as-ipid-boss/(Date of use : 8 March 2019**)**

Phakgadi P ‘KZN premier Mchunu has 21 days to study the Moerane report on political killings’ http://ewn.co.za/2018/06/13/kzn-premier-mchunu-has-21-days-to-study-moerane-report-on-political-killings accessed 10 July, 2018 (Date of use: 10 July 2018) (Phakgadi http://ewn.co.za/2018/06/13/kzn-premier-mchunu-has-21-days-to-study-moerane-report-on-political-killings accessed 10 July, 2018 (Date of use: 10 July 2018)

Phillip B 'Interception of communication applications decrease' http://www.sabcnews.com/sabcnews/interception-of-communication-applications-decrease/ (Date of use: 12 January 2019) (Phillip http://www.sabcnews.com/sabcnews/interception-of-communication-applications-decrease/ (Date of use: 12 January 2019)

Picotti L and Salvadori I 'National legislation implementing the convention on cybercrime-Comparative analysis and good practices' Discussion paper for project on cybercrime – version 28 August 2008 www.coe.int/cybercrime (Date of use: 8 March 2016) (Picotti and Salvadori www.coe.int/cybercrime (Date of use: 8 March 2016)

Pieterse N B 'Establishment of specialised capacity' http://www.nstf.org.za/wp-content/uploads/2015/09/ICTEMPERORS15MAY.pdf (Date of use: 12 December 2016) **(**Pieterse http://www.nstf.org.za/wp-content/uploads/2015/09/ICTEMPERORS15MAY.pdf (Date of use: 12 December 2016**)**

Pieterse N B 'Cybercrime: A South African perspective' - Workshop for Policy Design towards Digital Security (2015) https://docobook.com/electronic-crime-unit-the-national-science-and.html (Date of use: 18 November 2017) **(**Pieterse https://docobook.com/electronic-crime-unit-the-national-science-and.html (Date of use: 18 November 2017)

Pieters C 'Institutional independence: Why is it important and what are we doing?' http://www.ngopulse.org/article/2016/02/10/institutional-independence-why-it-important-and-what-we-are-doing (Date of use: 16 February 2019) (Pieters http://www.ngopulse.org/article/2016/02/10/institutional-independence-why-it-important-and-what-we-are-doing (Date of use: 16 February 2019)

Pijoos I 'Home Affairs DG Mkuseli Apleni resigns' https://mg.co.za/article/2018-07-23-home-affairs-dg-mkuseli-apleni-resigns (Date of use: 24 August 2018)(Pijoos https://mg.co.za/article/2018-07-23-home-affairs-dg-mkuseli-apleni-resigns (Date of use: 24 August 2018))

Pillay V '13 reasons you should be very worried about your government spying on you' http://www.huffingtonpost.co.za/2016/12/22/13-reasons-you-should-be-very-worried-about-your-government-spyi_a_21633335/ (Date of use: 2 January 2017) (Pillay

http://www.huffingtonpost.co.za/2016/12/22/13-reasons-you-should-be-very-worried-about-your-government-spyi_a_21633335/ (Date of use: 2 January 2017)

Pilling D and Cotterill J 'Captured: How Jacob Zuma 'sold' South Africa to the Guptas -One family has gained extraordinary influence over a country and its politics' https://www.irishtimes.com/news/world/africa/captured-how-jacob-zuma-sold-south-africa-to-the-guptas-1.3311139 (Date of use: 12 June 2018) (Pilling and Cotterill https://www.irishtimes.com/news/world/africa/captured-how-jacob-zuma-sold-south-africa-to-the-guptas-1.3311139 (Date of use: 12 June 2018)

Parliamentary Monitoring Group 'SAPS & IPID 2018/19 annual performance, with minister and deputy' https://pmg.org.za/committee-meeting/26410/ (Date of use: 12 July 2018)(Parliamentary Monitoring Group https://pmg.org.za/committee-meeting/26410/ (Date of use: 12 July 2018)

Parliamentary Monitoring Group 'Question 855 of 2013/17B Parliamentary Monitoring Group question posed to the minister of police' http://www.pmg.org.za/node/36638 (Date of use: 12 December 2013) (Parliamentary Monitoring Group http://www.pmg.org.za/node/36638 (Date of use: 12 December 2013)

Parliamentary Monitoring Group 'Question 720 of 2013/17B parliamentary monitoring group question posed to the minister of police' http://www.oigi.gov.za/Legislation/IntelServRegs_2003Oct.htm (Date of use: 14 December 2013)(Parliamentary Monitoring Group http://www.oigi.gov.za/Legislation/IntelServRegs_2003Oct.htm (Date of use: 14 December 2013)

PMG 'Nomination: Appointment of the inspector general for intelligence' https://pmg.org.za/call-for-comment/418/ (Date of use: 31 January 2018) (PMG https://pmg.org.za/call-for-comment/418/ (Date of use: 31 January 2018)

Phakathi B 'Bheki Cele has until Monday to give reasons for not renewing Robert McBride's contract' https://www.businesslive.co.za/bd/national/2019-02-14-bheki-cele-has-until-monday-to-give-reasons-for-not-renewing-robert-mcbrides-contract/(Date of use: 14 February

2019) (Phakathi https://www.businesslive.co.za/bd/national/2019-02-14-bheki-cele-has-until-monday-to-give-reasons-for-not-renewing-robert-mcbrides-contract/(Date of use: 14 February 2019)

Pieterse N B 'Electronic Crime Unit: Directorate for Priority Crime Investigation' Workshop for Policy Design towards Digital Security, Cybercrime and Cybercrime Prevention (2015) http://www.nstf.org.za/wp-content/uploads/2015/10/BrigPieterse.pdf (Date of use: 27 August 2017) (Pieterse http://www.nstf.org.za/wp-content/uploads/2015/10/BrigPieterse.pdf (Date of use: 27 August 2017)

Pillay V '13 reasons you should be very worried about your government spying on you' http://www.huffingtonpost.co.za/2016/12/22/13-reasons-you-should-be-very-worried-about-your-government-spyi_a_21633335/ (Date of use: 2 January 2017 (Pillay http://www.huffingtonpost.co.za/2016/12/22/13-reasons-you-should-be-very-worried-about-your-government-spyi_a_21633335/ (Date of use: 2 January 2017)

Politics Webs 'WCape High Court rules Hawks Act unconstitutional-HSF Helen Suzman Foundation' http://www.politicsweb.co.za/politicsweb/view/politicsweb/en/page71654?oid=480785&sn=Detail&pid=71616 (Date of use: 20 February 2017) (Politics Webs http://www.politicsweb.co.za/politicsweb/view/politicsweb/en/page71654?oid=480785&sn=Detail&pid=71616 (Date of use: 20 February 2017)

Popov A 'Legal aspects of deploying voice biometrics and other speech technologies in connection with GDPR enforcement' https://www.linkedin.com/pulse/legal-aspects-deploying-voice-biometrics-other-speech-alexey-popov (Date of use: 15 July 2018)(Popov https://www.linkedin.com/pulse/legal-aspects-deploying-voice-biometrics-other-speech-alexey-popov (Date of use: 15 July 2018)

PricewaterhouseCooper 'Electronic evidence gathering and analysis' www.pwc.com/ca/forensics (Date of use: 29 July 2016 (PricewaterhouseCooper www.pwc.com/ca/forensics (Date of use: 29 July 2016)

Privacy International 'State of privacy South Africa' https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa (Date of use: 25 April 2019 (Privacy International https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa (Date of use: 25 April 2019)

Public Service Commission 'Chapter 3 of the Public Service Regulation 2001' http://www.psc.gov.za/documents/docs/legislation/PUBLIC%20SERVICE%20REGULATIONS.pdf (Date of use: 12 March 2014) (Public Service Commission http://www.psc.gov.za/documents/docs/legislation/PUBLIC%20SERVICE%20REGULATIONS.pdf (Date of use: 12 March 2014)

Reuters 'North Korea denies cyberattacks on South Korea officials' http://www.reuters.com/article/us-northkorea-korea-cyber-idUSKCN0WF05V (Date of use: May 20 2016) (Reuters http://www.reuters.com/article/us-northkorea-korea-cyber-idUSKCN0WF05V (Date of use: May 20 2016)

Rijksoverheid 'Memorie van Toelichting Wetsvoorstel Computercriminaliteit III' https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/23/memorie-van-toelichting-wetsvoorstel-computercriminaliteit-iii (Date of use: 3 March 2017 (Rijksoverheid https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/23/memorie-van-toelichting-wetsvoorstel-computercriminaliteit-iii (Date of use: 3 March 2017)

Richardson M 'Cyber Protection Act too broad, infringes on our privacy rights' http://thehill.com/blogs/congress-blog/technology/223805-cyber-protection-act-too-broad-infringes-on-our-privacy-rights- (Date of use: 18 May 2016) (Richardson http://thehill.com/blogs/congress-blog/technology/223805-cyber-protection-act-too-broad-infringes-on-our-privacy-rights- (Date of use: 18 May 2016)

R2K 'Big brother exposed: Stories of South Africa's intelligence structures monitoring and harassing activist movements' http://bigbrother.r2k.org.za/wp-content/uploads/Big-Brother-Exposed-R2K-handbook-on-surveillance-web.pdf (Date of use: 5 July 2018) (R2K http://bigbrother.r2k.org.za/wp-content/uploads/Big-Brother-Exposed-R2K-handbook-on-surveillance-web.pdf (Date of use: 5 July 2018)

Robertson G 'Only an international court can bring Khashoggi's killers to justice' Https://www.theguardian.com/commentisfree/2018/oct/23/international-court-jamal-khashoggi-killers-un (Date of use: 21 October 2018) (Robertson Https://www.theguardian.com/commentisfree/2018/oct/23/international-court-jamal-khashoggi-killers-un (Date of use: 21 October 2018)

Rose M and Baker L 'Can France's leader-less 'yellow vests' become a true political force?' https://globalnews.ca/news/4743632/yellow-vest-political-movement-france/ (Date of use: 9 December 2019) (Rose and Baker https://globalnews.ca/news/4743632/yellow-vest-political-movement-france/ (Date of use: 9 December 2019)

Rosenblatt B 'Principles of jurisdiction' https://cyber.harvard.edu/property99/domain/Betsy.html. (Date of use: 12 June 2016 (Rosenblatt https://cyber.harvard.edu/property99/domain/Betsy.html. (Date of use: 12 June 2016)

Rosen J 'The Supreme Court's cell phone case went even further than privacy advocates had hoped' http://www.newrepublic.com/article/118396/supreme-court-cellphone-case-went-further-privacy-advocates-hoped (Date of use: 30 June 2017 (Rosen http://www.newrepublic.com/article/118396/supreme-court-cellphone-case-went-further-privacy-advocates-hoped (Date of use: 30 June 2017)

Right2Know 'Spooked- surveillance of journalists in SA' https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use 27 November 2018) (Right2Know https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf (Date of use: 27 November 2018)

RSA 'Mutual legal assistance in criminal matters in the treaty between the United States of America and South Africa (2001)' https://www.state.gov/documents/organization/124466.pdf (Date of use: 28 March 2016) (RSA https://www.state.gov/documents/organization/124466.pdf (Date of use: 28 March 2016)

Roque P C 'Angola: Parallel governments, oil and neopatrimonial' *Institute for Security Studies- Situation Report* http://dspace.africaportal.org/jspui/bitstream/123456789/32306/1/6June2011Angola.pdf?1 (Date of use: 2 October 2016) (Roque http://dspace.africaportal.org/jspui/bitstream/123456789/32306/1/6June2011Angola.pdf?1 (Date of use: 2 October 2016)

SABC News 'ACDP leader Reverend Kenneth Meshoe tests positive for coronavirus' https://www.sabcnews.com/sabcnews/acdp-leader-reverend-kenneth-meshoe-tests-positive-for-coronavirus/ (28 March 2020) (SABC News https://www.sabcnews.com/sabcnews/acdp-leader-reverend-kenneth-meshoe-tests-positive-for-coronavirus/ (28 March 2020)

SAHA 'General Intelligence Laws Amendment Bill' http://db3sqepoi5n3s.cloudfront.net/files/docs/120322saha_1.pdf (Date of use: 17 July 2017) (SAHA http://db3sqepoi5n3s.cloudfront.net/files/docs/120322saha_1.pdf (Date of use: 17 July 2017)

Salazar A "Mini documentary reveals full extent of a United States domestic spy program" http://www.infowars.com/mini-documentary-reveals-full-extent-of-stellar-wind-domestic-spy-program/ (Date of use: 1 September 2017) (Salazar http://www.infowars.com/mini-documentary-reveals-full-extent-of-stellar-wind-domestic-spy-program/ (Date of use: 1 September 2017)

Salifu U 'The Nigerian citizen's recent conviction in a Johannesburg high court of 13 terrorism charges confirms South Africa`s commitment to the global fight against terrorism.' https://issafrica.org/iss-today/henry-okah-counter-terrorism-ruling-is-a-judicial-triumph-for-south-africa-and-the-continent (Date of use:12 June 2016)(Salifu https://issafrica.org/iss-today/henry-okah-counter-terrorism-ruling-is-a-judicial-triumph-for-south-africa-and-the-continent (Date of use:12 June 2016)

SALRC 'Discussion paper 109- Project 124 – Privacy and data protection' (2005) http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016 (SALRC http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016)

SALRC 'Privacy and data protection,' Paper 109-Project, Chapter 2 at 10 and 14 **(**SALRC http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016) **(**SALRC http://www.justice.gov.za/salrc/dpapers/dp109.pdf (Date of use: 27 June 2016))

SAPA 'Phiyega does "Structural change" on Crime Intelligence' http://www.enca.com/south-africa/phiyega-does-structural-change-crime-intelligence (Date of use: 21 February 2014 (SAPA http://www.enca.com/south-africa/phiyega-does-structural-change-crime-intelligence (Date of use 21 February 2014)

SAPA-AFP 'NSA is tracking mobile phones all over the world' https://businesstech.co.za/news/general/50542/nsa-is-tracking-mobile-phones-all-over-the-world/ (Date of use: 12 January 2017) (SAPA-AFP https://businesstech.co.za/news/general/50542/nsa-is-tracking-mobile-phones-all-over-the-world/ (Date of use: 12 January 2017)

SAPS 'Careers in SAPS' https://www.saps.gov.za/careers/downloads/saps_career_booklet_part1.pdf (Date of use: 16 November 2018 (SAPS https://www.saps.gov.za/careers/downloads/saps_career_booklet_part1.pdf (Date of use:16 November 2018)

SAPS Civilian Secretariat for Police 'Green paper on policing' http://www.policesecretariat.gov.za/downloads/green_paper_policing.pdf (Date of use: 18 September 2013 (SAPS Civilian secretariat for police http://www.policesecretariat.gov.za/downloads/green_paper_policing.pdf (Date of use: 18 September 2013)

SAPS 'Crime Intelligence (Pretoria) REFERENCES: Post No 18/01/3027(1 post), no stipulation of academic or skill acquisition requirement' file:///I:/LI-SA-%20CI-SAPS%20-%20ADVERT%20FOR%20CRIME%20INTELLIGENCE%20-%20CI%203027.pdf. (Date

of use: 17 September 2019) (SAPS file:///I:/LI-SA-%20CI-SAPS%20-%20ADVERT%20FOR%20CRIME%20INTELLIGENCE%20-%20CI%203027.pdf. (Date of use: 17 September 2019))

SAPS 'Location: Crime Intelligence (Pretoria): References: CI 07/07/2018' file:///C:/Users/Microlab/Downloads/CI%203027.pdf (Date of use: 17 September 2018)(SAPS file:///C:/Users/Microlab/Downloads/CI%203027.pdf (Date of use: 17 September 2018)

SAPS 'New class of police officers' https://www.saps.gov.za/careers/downloads/new_class_police_officer.pdf (Date of use: 16 November 2018) (SAPS https://www.saps.gov.za/careers/downloads/new_class_police_officer.pdf (Date of use: 16 November 2018))

SAPS 'National police commissioner General Riah Phiyega streamlines the South African Police Service crime intelligence environment' http://www.gov.za/speeches/view.php?sid=43031 (Date of use: 21 January 2014 (SAPS http://www.gov.za/speeches/view.php?sid=43031 (Date of use: 21 January 2014)

SAPS 'Serious Organised Crime Investigation at the Directorate of Priority Crime Investigation' file:///I:/LI-SA-%20SAPS-%20ADVERT%20PLACEMENT%20FOR%20SECTION%20HEAD%20OF%20SERIOUS%20ORGANISED%20CRIME%20INVESTIGATION%20NORTH%20WEST%20-2018%20DPSI%20SMS%2011%202018.pdf (Date of use: 16 November 2018) (SAPS file:///I:/LI-SA-%20SAPS-%20ADVERT%20PLACEMENT%20FOR%20SECTION%20HEAD%20OF%20SERIOUS%20ORGANISED%20CRIME%20INVESTIGATION%20NORTH%20WEST%20-2018%20DPSI%20SMS%2011%202018.pdf (Date of use: 16 November 2018)

SAPS 'Specialised training' https://pmg.org.za/committee-meeting/14743/(Date of use: 19 July 2016) (PMG https://pmg.org.za/committee-meeting/14743/ (Date of use: 19 July 2016)

SAQA 'Resolving of crime' http://regqs.saqa.org.za/showQualification.php?id=59989 (Date of use: 9 May 2019) (SAQA http://regqs.saqa.org.za/showQualification.php?id=59989 (Date of use: 9 May 2019)

Savini L 'Human microchipping is here and it's about to rock your skin's world' https://www.allure.com/story/rfdi-microchip-implant-in-skin (Date of use: 12 December 2018)(Savini https://www.allure.com/story/rfdi-microchip-implant-in-skin (Date of use: 12 December 2018)

Schneier B 'Anonymity and the Internet' https://www.schneier.com/blog/archives/2010/02/anonymity_and_t_3.html (Date of use: 4 January 2017) (Schneier https://www.schneier.com/blog/archives/2010/02/anonymity_and_t_3.html (Date of use: 4 January 2017)

Seetharaman D and Bindley K 'Facebook controversy: What to know about cambridge analytica and your data Facebook Inc.'s crisis centers on the company's most precious asset: the personal data of nearly two billion people' https://www.wsj.com/articles/facebook-scandal-what-to-know-about-cambridge-analytica-and-your-data-1521806400 (Date of use: 2 April 2018) (Seetharaman and Bindley https://www.wsj.com/articles/facebook-scandal-what-to-know-about-cambridge-analytica-and-your-data-1521806400 (Date of use: 2 Apri 2018)

Serrao A 'Senior crime intelligence officials without top secret clearance' https://www.news24.com/SouthAfrica/News/senior-crime-intelligence-officials-without-top-secret-clearance-20171130 (Date of use: 1 December 2017) (Serrao https://www.news24.com/SouthAfrica/News/senior-crime-intelligence-officials-without-top-secret-clearance-20171130 (Date of use: 1 December 2017**)**

Serrano R A and Loiko S L 'Snowden hopscotches globe, staying just out of U.S. reach' *Los Angeles Times* http://articles.latimes.com/2013/jun/25/world/la-fg-snowden-20130626 (Date of use: 28 June 2016) (Serrano http://articles.latimes.com/2013/jun/25/world/la-fg-snowden-20130626 (Date of use: 28 June 2016)

Serrao A and Mitchley A, N 'DA calls on inspector general of intelligence to probe alleged 'Project wonder' plot' https://www.news24.com/SouthAfrica/News/da-calls-on-inspector-general-of-intelligence-to-probe-alleged-project-wonder-plot-20170827 (Date of use: 26 July 2018) (Serrao and Mitchley https://www.news24.com/SouthAfrica/News/da-calls-on-inspector-general-of-intelligence-to-probe-alleged-project-wonder-plot-20170827 (Date of use: 26 July 2018))

Shange N 'New crime intelligence boss is squeaky clean…his bosses say' https://www.timeslives.co.za/news/south-africa/2018-03-29-new-crime-intelligence-boss-is-squeaky-clean-his-bosses-say/ (Date of use: 12 June 2018) (Shange https://www.timeslives.co.za/news/south-africa/2018-03-29-new-crime-intelligence-boss-is-squeaky-clean-his-bosses-say/ (Date of use: 12 June 2018)

Shaw M 'Organised crime in post-apartheid South Africa' Safety and Governance Programme, Institute for Security Studies Occasional Paper No 28-January 1998 file:///C:/Users/36262331/Desktop/Paper_28.pdf (Date of use: 11 September 2017) (Shaw file:///C:/Users/36262331/Desktop/Paper_28.pdf (Date of use: 11 September 2017)

Sherfinski D 'British leaders tapped phones, e-mails during 2009 G-20 summit: report' http://www.washingtontimes.com/news/2013/jun/17/british-leaders-tapped-officials-phones-emails-dur/ (Date of use: 18 June 2016) (Sherfinski http://www.washingtontimes.com/news/2013/jun/17/british-leaders-tapped-officials-phones-emails-dur/ (Date of use: 18 June 2016)

Snyder T 'America lost a cyberwar to Russia in 2016. When will we have the truth?' https://www.theguardian.com/commentisfree/2018/feb/12/america-cyberwar-russia-2016-memo-truth (Date of use: 2 December 2018) (Snyder https://www.theguardian.com/commentisfree/2018/feb/12/america-cyberwar-russia-2016-memo-truth (Date of use: 2 December 2018))

Sole S 'Surveillance: The silent spy on citizens and journalists faces court challenge' https://mg.co.za/article/2017-04-20-surveillance-silent-killer-of-journalism-and-democracy-1 accessed (Date of use: 5 April 2018) (Sole https://mg.co.za/article/2017-04-20-surveillance-silent-killer-of-journalism-and-democracy-1 accessed (Date of use: 5 April 2018)

Solidarity 'Matric only requirement for position as provincial head of crime intelligence https://solidariteit.co.za/en/matric-only-requirement-for-position-as-provincial-head-of-crime-intelligence/ (Date of use: 19 June 2016) (Solidarity https://solidariteit.co.za/en/matric-only-requirement-for-position-as-provincial-head-of-crime-intelligence/ (Date of use: 19 June 2016)

Solove D J '"I've got nothing to hide" and other misunderstandings of privacy' http://ssrn.com/abstract=998565 (Date of use: 3 March 2016) (Solove http://ssrn.com/abstract=998565 (Date of use: 3 March 2016)

South African History Archives 'General Intelligence Laws Amendment Bill' http://db3sqepoi5n3s.cloudfront.net/files/docs/120322saha_1.pdf (Date of use: 17 July 2013) (South African History Archives http://db3sqepoi5n3s.cloudfront.net/files/docs/120322saha_1.pdf (Date of use: 17 July 2013)

South African Police Service 'Strategic plan 2010-2014' http://www.saps.gov.za/about/stratframework/strategic_plan/2010_2014/strategic_plan_2010_2014.pdf (Date of use: 6 June 2013) (South African Police Service http://www.saps.gov.za/about/stratframework/strategic_plan/2010_2014/strategic_plan_2010_2014.pdf (Date of use: 6 June 2013)

South African Police Service '*Annual report 2012/13'* http://www.saps.gov.za/about/stratframework/annualreports.php (Date of use: 6 June 2013) (South African Police Service http://www.saps.gov.za/about/stratframework/annualreports.php (Date of use: 6 June 2013)

South African Police Service SAPS 'Location: Crime Intelligence (Pretoria): References: CI 07/07/2018' file:///C:/Users/Microlab/Downloads/CI%203027.pdf (Date of use: 17 September 2018) (South African Police Service SAPS file:///C:/Users/Microlab/Downloads/CI%203027.pdf (Date of use: 17 September 2018)

Sowetan 'Nkandla Committee dissolved for now' http://www.sowetanlive.co.za/news/2014/04/29/nkandla-committee-dissolved-for-now (Date

of use: 30 April 2014 (Sowetan http://www.sowetanlive.co.za/news/2014/04/29/nkandla-committee-dissolved-for-now (Date of use: 30 April 2014)

Spahn T E and Woods M 'The ethics of email and social media: A top ten list' http://media.mcguirewoods.com/publications/Ethics-Programs/6312230.pdf (Date of use: 29 July 2018) (Spahn and Woods http://media.mcguirewoods.com/publications/Ethics-Programs/6312230.pdf (Date of use: 29 July 2018)

Standing A and van Vuuren H 'The role of auditors: Research into organised crime and money laundering' Institute for Security Studies ISS Paper 73 May 2003 https://issafrica.org/research/papers/the-role-of-auditors-research-into-organised-crime-and-money-laundering (Date of use: 13 September 2016) (Standing and van Vuuren https://issafrica.org/research/papers/the-role-of-auditors-research-into-organised-crime-and-money-laundering (Date of use: 13 September 2016)

Staff Reporter 'Deputy Chief Justice Raymond Zondo to head commission of inquiry into state capture' https://mg.co.za/article/2018-01-09-deputy-chief-justice-raymond-zondo-to-head-state-capture-commission-of-inquiry (Date of use: 13 July 2019) (Staff Reporter https://mg.co.za/article/2018-01-09-deputy-chief-justice-raymond-zondo-to-head-state-capture-commission-of-inquiry (Date of use: 13 July 2019)

Staff Reporter 'NIA says it is not monitoring Zille's calls' http://mg.co.za/article/2011-03-09-nia-says-it-is-not-monitoring-zilles-calls (Date of use: 18 April 2016) (Staff Reporter http://mg.co.za/article/2011-03-09-nia-says-it-is-not-monitoring-zilles-calls (Date of use: 18 April 2016)

Staff Reporter 'Zille maintains her calls were being monitored' http://mg.co.za/article/2011-03-09-zille-maintains-her-calls-were-being-monitored (Date of use: 18 April 2016) (Staff Reporter http://mg.co.za/article/2011-03-09-zille-maintains-her-calls-were-being-monitored (Date of use: 18 April 2016)

Staff Writer 'The 30 worst areas in South Africa for crime in 2017' https://businesstech.co.za/news/lifestyle/207191/the-30-worst-areas-in-south-africa-for-crime-in-2017/ (Date of use: 12 March 2018) (Staff Writer

https://businesstech.co.za/news/lifestyle/207191/the-30-worst-areas-in-south-africa-for-crime-in-2017/ (Date of use: 12 March 2018)

State Security Agency 'Computer Security Incident Response Team' (CSIRT) http://www.ssa.gov.za/csirt.aspx (Date of use: 18 February 2018) (State Security Agency http://www.ssa.gov.za/csirt.aspx (Date of use: 18 February 2018)

SSA 'White paper on intelligence' http://www.ssa.gov.za/Portals/0/SSA%20docs/Legislation/White%20Paper%20on%20Intelligence.PDF (Date of use: 21 January 2014) (SSA http://www.ssa.gov.za/Portals/0/SSA%20docs/Legislation/White%20Paper%20on%20Intelligence.PDF (Date of use: 21 January 2014)

State Security Agency 'About us' http://www.ssa.gov.za/AboutUs.aspx (Date of use: 19 April 2019) (State Security Agency http://www.ssa.gov.za/AboutUs.aspx (Date of use: 19 April 2019)

State Security Agency 'National Communications Branch' http://www.ssa.gov.za/AboutUs/Branches/NationalCommunications.aspx (Date of use: 12 January 2018)(State Security Agency http://www.ssa.gov.za/AboutUs/Branches/NationalCommunications.aspx (Date of use: 12 January 2018)

Straitstimes 'South Sudan president blasts UN for wanting 'parallel' government' http://www.straitstimes.com/world/south-sudan-president-blasts-un-for-wanting-parallel-government (Date of use: 2 October 2016) (Straitstimes http://www.straitstimes.com/world/south-sudan-president-blasts-un-for-wanting-parallel-government (Date of use: 2 October 2016)

Swart H 'Communication surveillance by the South African intelligence services' 2016 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use: 13 August 2016) (Swart http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf (Date of use: 13 August 2016)

Swart H 'Joburg's new hi-tech surveillance cameras: A threat to minorities that could see the law targeting thousands of innocents' https://www.dailymaverick.co.za/article/2018-09-28-joburgs-new-hi-tech-surveillance-cameras-a-threat-to-minorities-that-could-see-the-law-targeting-thousands-of-innocents/ (Date of use:12 December 2018) (Swart https://www.dailymaverick.co.za/article/2018-09-28-joburgs-new-hi-tech-surveillance-cameras-a-threat-to-minorities-that-could-see-the-law-targeting-thousands-of-innocents/ (Date of use:12 December 2018)

Swart H 'Say nothing – the spooks are listening' https://mg.co.za/article/2015-12-17-say-nothing-the-spooks-are-listening (Date of use: 13 August 2016) (Swart https://mg.co.za/article/2015-12-17-say-nothing-the-spooks-are-listening (Date of use: 13 August 2016)

Swart H 'Secret state: How the government spies on you' https://mg.co.za/article/2011-10-14-secret-state/ (Date of use: 12 December 2016) (Swart https://mg.co.za/article/2011-10-14-secret-state/ (Date of use: 12 December 2016)

Swart H 'Your cellphone records and the law: The legal loophole that lets state spying run rampant' https://www.dailymaverick.co.za/article/2018-05-20-your-cellphone-records-and-the-law-the-legal-loophole-that-lets-state-spying-run-rampant/ (Date of use: 12 January 2019 (Swart https://www.dailymaverick.co.za/article/2018-05-20-your-cellphone-records-and-the-law-the-legal-loophole-that-lets-state-spying-run-rampant/ accessed (Date of use: 12 January 2019)

Swart H Communication 'Surveillance by the South African Intelligence Services' 2016 http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf. (Date of use:13 August 2016) (Swart http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf. (Date of use:13 August 2016)

The New York Times 'U.S. said to find North Korea ordered cyberattack on Sony' http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-

hacking.html?_r=0 (Date of use: May 20 2016) (The New York Times http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0 (Date of use: May 20 2016)

The Free Dictionary 'Maxim' https://legal-dictionary.thefreedictionary.com/%22He+who+comes+into+equity+must+come+with+clean+hands.%22 (Date of use:19 August 2019) (The Free Dictionary https://legal-dictionary.thefreedictionary.com/%22He+who+comes+into+equity+must+come+with+clean+hands.%22 (Date of use:19 August 2019)

The Times 'DA has Police Chief McBride in its Sights' http://news.howzit.msn.com/da-has-police-chief-mcbride-in-its-sights (Date of use: 5 March 2014 (The Times http://news.howzit.msn.com/da-has-police-chief-mcbride-in-its-sights (Date of use: 5 March 2014)

Thompson S A and Warzel C 'How to track President Trump' https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html (Date of use:12 January 2018) (Thompson and Warzel https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html (Date of use:12 January 2018)

UNESCO 'UNESCO launches its publication on Internet and freedom of expression' http://www.unesco.org/new/en/member-states/single-view/news/unesco_launches_in_panama_a_publication_on_internet_and_fre/ (Date of use: 17 May 2018) (UNESCO http://www.unesco.org/new/en/member-states/single-view/news/unesco_launches_in_panama_a_publication_on_internet_and_fre/ (Date of use: 17 May 2018)

United Nations 'Concluding observations on the initial report of South Africa' CCPR/C/ZAF/CO/1https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fZAF%2fCO%2f1&Lang=en (Date of use:18 January 2019 (United Nations https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fZAF%2fCO%2f1&Lang=en (Date of use: 18 January 2019)

United Nations Office on Drugs and Crime 'Comprehensive study on cybercrime' (2013) 122 http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (Date of use: 10 January 2017) (United Nations Office on Drugs and Crime http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (Date of use: 10 January 2017)

United Nations Office on Drugs and Crime 'Current practices in electronic surveillance in the investigation of serious and organized crime' https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf (Date of use: 2 May 2013) (United Nations Office on Drugs and Crime 'Current practices in electronic surveillance in the investigation of serious and organized crime' https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf (Date of use: 2 May 2013)

United Nations Radio 'Robots can and will "walk among us" robotics chief tells UN' http://www.unmultimedia.org/radio/english/2017/10/robots-can-and-will-walk-among-us-says-ceo-of-hanson-robotics/#.WhvkxlWWaUk (Date of use: 18 October 2017) (United Nations Radio http://www.unmultimedia.org/radio/english/2017/10/robots-can-and-will-walk-among-us-says-ceo-of-hanson-robotics/#.WhvkxlWWaUk (Date of use: 18 October 2017)

UN 'Report of the Preparatory Commission for the International Criminal Court: Part II Finalised draft text of the elements of crimes' PCNICC/2000/1/Add.2 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/724/27/PDF/N0072427.pdf?OpenElement (Date of use 12 January 2017) (UN https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/724/27/PDF/N0072427.pdf?OpenElement (Date of use 12 January 2017)

Vakof P 'Electronic evidence gathering & analysis' (Toronto, ICC FraudNet Spring Conference in San Jose, Costa Rica- Jurisdiction- Multijurisdictional 2010) http://www.icc-ccs.org.uk/home/publications/viewdownload/3/180 (Date of use: 12 June 2016) (Vakof

http://www.icc-ccs.org.uk/home/publications/viewdownload/3/180 (Date of use: 12 June 2016)

Valdes R and D Roos D 'How VoIP works' http://www.people/emson.edu (Date of use: 17 April 2016) (Valdes and Roos http://www.people/emson.edu (Date of use: 17 April 2016)

Van der Watt M 'Decriminalisation of sex work in South Africa will only bring more harm' https://www.dailymaverick.co.za/opinionista/2019-04-17-decriminalisation-of-sex-work-in-south-africa-will-only-bring-more-misery/ (Date of use: 15 May 2019) (Van der Watt https://www.dailymaverick.co.za/opinionista/2019-04-17-decriminalisation-of-sex-work-in-south-africa-will-only-bring-more-misery/ (Date of use: 15 May 2019)

Vaughan-Nichols S J 'How to keep your smart TV from spying on you- Opinion: You could worry about Windows 10 spying on you, or you could worry about something a bit more serious -- like your TV listening in on you and passing on the information to intelligence agencies' https://www.zdnet.com/article/how-to-keep-your-smart-tv-from-spying-on-you/ (Date of use: 21 March 2018) (Vaughan-Nichols https://www.zdnet.com/article/how-to-keep-your-smart-tv-from-spying-on-you/ (Date of use: 21 March 2018)

Ujazdowskie A 'OSCE/ODIHR comments on legislative treatment of "Cyberterror" in domestic law of individual States' www.legislationline.org (Date of use: 12 February 2016) (Ujazdowskie www.legislationline.org (Date of use: 12 February 2016)

Van der Berg J 'Mobile phone evidence: Implications for privacy in South African law' http://ohrh.law.ox.ac.uk/mobile-phone-evidence-implications-for-privacy-in-south-african-law/(Date of use: 25 June 2017 (Van der Berg http://ohrh.law.ox.ac.uk/mobile-phone-evidence-implications-for-privacy-in-south-african-law/ (Date of use: 25 June 2017)

Van Genderen R V 'Cybercrime investigation and the protection of personal data and privacy' Version 2008 www.coe.int/cybercrime (Date of use: 24 June 2016) (Van Genderen www.coe.int/cybercrime (Date of use: 24 June 2016)

VOA 'China says it shut down 128,000 websites in 2017' https://www.voanews.com/a/china-says-it-shut-down-128000-websites-in-2017/4199229.html (Date of use: 23 January 2018)

(VOA https://www.voanews.com/a/china-says-it-shut-down-128000-websites-in-2017/4199229.html (Date of use: 23 January 2018)

Wakefield A 'SA to miss digital migration deadline, but govt. says don't worry' http://www.news24.com/SouthAfrica/News/SA-to-miss-digitial-migration-deadline-but-govt-says-dont-worry-20150616 (Date of use: 4 July 2015) (Wakefield http://www.news24.com/SouthAfrica/News/SA-to-miss-digitial-migration-deadline-but-govt-says-dont-worry-20150616 (Date of use: 4 July 2015)

Waldron S , Wood C and Kemp N 'Use of predictive text in text messaging over the course of a year and its relationship with spelling, orthographic processing and grammar: Predictive text and literacy skills' https://www.researchgate.net/publication/302917761_Use_of_predictive_text_in_text_messaging_over_the_course_of_a_year_and_its_relationship_with_spelling_orthographic_processing_and_grammar_Predictive_Text_and_Literacy_Skillshttps://www.researchgate.net/publication/302917761_Use_of_predictive_text_in_text_messaging_over_the_course_of_a_year_and_its_relationship_with_spelling_orthographic_processing_and_grammar_Predictive_Text_and_Literacy_Skills (Date of use: 21 February 2020) (Waldron, Wood and Kemp https://www.researchgate.net/publication/302917761_Use_of_predictive_text_in_text_messaging_over_the_course_of_a_year_and_its_relationship_with_spelling_orthographic_processing_and_grammar_Predictive_Text_and_Literacy_Skillshttps://www.researchgate.net/publication/302917761_Use_of_predictive_text_in_text_messaging_over_the_course_of_a_year_and_its_relationship_with_spelling_orthographic_processing_and_grammar_Predictive_Text_and_Literacy_Skills (Date of use: 21 February 2020)

Warlen S C 'Crime scene photography: the silent witness' http://www.ncjrs.gov/App/Publication/abtract.aspx?ID=155223 (Date of use: 16 December 2016) (Warlen http://www.ncjrs.gov/App/Publication/abtract.aspx?ID=155223 (Date of use: 16 December 2016)

White A 'A brief history of surveillance in America: With wiretapping in the headlines and smart speakers in millions of homes, historian Brian Hochman takes us back to the early days of eavesdropping' https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/ (Date of use: 18 June 2018) (White

https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/ (Date of use:18 June 2018)

Wijayatunga C 'Internet and network security fundamentals' https://www.pacnog.org/pacnog10/track3/Security-Part-1.pdf (Date of use: 11 April 2017 (Wijayatunga https://www.pacnog.org/pacnog10/track3/Security-Part-1.pdf (Date of use: 11 April 2017)

Wikipedia 'Portal mathematics' http://en.wikipedia.org/wiki/portal:mathematics (Date of use: 18 December 2017) (Wikipedia http://en.wikipedia.org/wiki/portal:mathematics (Date of use: 18 December 2017)

Yi S 'Talk of US cyber war on China ridiculous' http://www.globaltimes.cn/content/1107699.shtml (Date of use:12 December 2018) (Yi http://www.globaltimes.cn/content/1107699.shtml (Date of use:12 December 2018)

Zinn R 'The value of Crime Intelligence in combating violent crime' Inaugural lecture delivered at the Department of Police Practice, University of South Africa 2011' http://uir.unisa.ac.za/bitstream/handle/10500/7649/R_Zinn_Inaugural%20Speech.pdf?sequence=1 (Date of use: 12 December 2013) (Zinn at 10 http://uir.unisa.ac.za/bitstream/handle/10500/7649/R_Zinn_Inaugural%20Speech.pdf?sequence=1 (Date of use:12 December 2013)

CASE LAW

A. REPUBLIC OF SOUTH AFRICA

Abdi v Minister of Home Affairs 2011 3 SA 37 (SCA) 51 (*Abdi v Home Affairs*)

Absa Insurance and Financial Advisers (Pty) Ltd v Christaan Johannes Stephanus Moller & others Case number: 20216/2014 (*Absa v Moller*)

Alex Cartage (Pty) Ltd v Minister of Transport 1986 (2) SA 838 (E) (*Alex Cartage (Pty) Ltd v Minister of Transport*)

Allen v Kirkinis Case No. 20428/2014 (*Allen v Kirkinis*)

AmaBhungane Centre for Investigative Journalism & Another v Minister of Justice & Correctional Services & Others Suit No 25978/17, the appeal of which was pending at the Constitutional Court at the time of submission (*Amabhungane v Minister of Justice*)

Ashok Rama Mistry v The Interim National Medical and Dental Council of South Africa & Others CCT 13/97 (*Mistry v Medical and Dental Council*)

Azanian Peoples Organization (AZAPO) v President of the Republic of South Africa 1996 ZACC 16; 1996 4 SA 671 (CC); 1996 8 BCLR 1015 (CC) (*AZAPO v President*)

Bane and Others v D'Ambrosi (279/08) 2009 (ZASCA) 98 (*Bane v D'Ambrosi*)

Barkhuizen v Napier 2007 (ZACC) 5; 2007 (5) SA 323 (CC); 2007 (7) BCLR 691 (CC)(*Barkhuizen v Napier*)

B C C Pharmaceuticals (Pty) Ltd v Minister of Health & Others 2007 3 SA 72 (C) (‘*BCC*’)

Beinash & Another v Ernst & Young & Others (CCT12/98) ZACC19, 1999 (2) SA 91, 1999 (2) BCLR 125 (*Beinash v Ernst & Young*)

Beheersmaatschappij Helling I NV and Others v Magistrate, Cape Town and Others 2007 1 SACR 99(C) (*Helling v Mag*)

Bernstein v Bester NO 1996 2 SA 751 (CC) 792 (*Bernstein v Bester NO*)

Bhe and Others v Khayelitsha Magistrate and Others (CCT 49/03) 2004 (ZACC) 17, 2005 (1) SA 580, 2005(1) BCLR 1 (CC) (*Bhe v Khayelitsha Magistrate*)

Bosasa Operation (Pty) Ltd v Basson and Another (09/29700) 2012 (ZAGPJHC) (*Bosasa v Basson*)

Botha v State A163/2014 2015 (ZAFSHC) 34 (*Botha v State*)

C v Minister of Correctional Services 1996 4 SA 292 (T) (*C v Minister of Correctional Services*)

Carmichele v Minister of Safety and Security and Another 2001 (ZACC) 22; 2001 (4) SA 938 (CC); 2001 (10) BCLR 995 (CC) (*Carmichele v Minister of Safety and Security*)

Cecilia Goliath v Member of the Executive Council for Health, Eastern Cape (085/2014) 2014 (ZASCA) 182 (*Goliath v MEC, Health, Eastern Cape*)

Christian Education South Africa v Minister of Education CCT13/98 1998 (ZACC) 16, 1999 (2) SA 83, 1998(12) BCLR 1449 27(*Christian Education v Minister of Education*)

Cine Films (Pty) Ltd v Commissioner of Police 1971 (4) SA 574 (W)(*Cine Films v Commissioner of Police*)

Craig Smith & Associates v Minister of Home Affairs and Others 12756/2014 (ZAWCHC) (*Craig v Home Affairs*)

Curtis v Minister of Safety and Security and Others 1996 3 SA 617 (CC) (*Curtis*)

Dawood v Minister of Home Affairs 2000 3 SA 936 (CC) (*Dawood v Home Affairs*)

De Lille v Speaker of the National Assembly 1998 3 SA 430 (C) 37(*De Lille v Speaker of the National Assembly*)

Deliwe Muriel Njongi v Member of the Executive Council, Department of Welfare, Eastern Cape CCT 37/07 2008 (ZACC) 4 (*Njongi v MEC*)

Democratic Alliance v President of the Republic of South Africa and others Case CCT 122/11 2012 (ZACC) 24 (*DA v President*)

Dunn and Bradstreet (Pty) Ltd v SA Merchants Combined Credit Bureau (Cape) (Pty) Ltd 1968 1 SA 209 (C) (*Dunn and Bradstreet v SA Merchants Combined Credit Bureau*)

Estate Agency Affairs Board v Auction Alliance (Pty) Ltd and Others CCT 94/13 (ZACC) (*Estate Board v Auction Alliance*)

Ex Parte Minister of Safety and Security and Others: In Re S v Walters and Another CCT28/01 2002 (ZACC) 6; 2002 (4) SA 613; 2002 (7) BCLR 663 (21 May 2002) (*Ex Parte Minister of Safety and Security and Others: In Re S v Walters and Another*)

F & Another v The Minister of Safety & Security CCT 20/95 (ZACC) 91 (*F v Min of Safety*)

Famanda v State 930/2017 2018 (ZASCA) 139 (*Famanda v State*)

FAWU obo Kapesi and 31 others v Premier Foods Limited t/a Blue Ribbon Salt River & Another (2010) Case NO: C640-07 (ZALC) *FAWU v Premier Foods Limited*)

Ferreira v Levin Others CCT No 5/95 (CC)(*Ferreira v Levin*)

Fikizolo Norman Khosana and Another v The Minister of Safety & Security N.O. & Others Case No.:2512/08 (ZAFSHC) (*Khosana v Min of Safety*)

Financial Mail (Pty) Ltd v Sage Holdings Ltd 1993 2 SA 451(A) (ZASCA) (*Financial Mail v Sage*)

Foodcorp (Pty) Ltd v The Deputy Director-General - Department of Environmental Affairs and Tourism: Branch Marine and Coastal Management and Others Case No: 3519/02 (ZASCA) (*Foodcorp v Deputy Director- General*)

Fose v Minister of Safety and Security 1997 (ZACC) 6; 1997 (3) SA 786 (CC); 1997 (7) BCLR 851 (CC) (*Fose v Minister of Safety and Security*)

Gays and Lesbians v Minister of Justice CCT 11/98 (ZACC) 15 (*Gays and Lesbians v Minister of Justice*)

Glenister v President of the Republic of South Africa and Others 2011 (ZACC) 6; 2011 (3) SA 347 (CC); 2011 (7) BCLR 651 or 176 (CC) (*Glenister II*)

Goqwana v Minister of Safety NO & others (20668/14) 2015 (ZASCA) 186 (*Goqwana*)

Haysom v Additional Magistrate, Cape Town and another 1979(3) SA 155 (C) (*Haysom*)

Helen Suzman Foundation v Judicial Service Commission 2018 (ZACC) 8 (*Suzman Foundation v JSC*)

Helen Suzman Foundation v President of the Republic of South Africa and Others in: *Glenister v President of the Republic of South Africa and Others* 2014 (ZACC) 32 (*Suzman Foundation v President of the RSA* in: *Glenister v President of the RSA*)

Helen Suzman Foundation v The Minister of Police and Others HC Case No: 1054/2015 (*Suzman Foundation v Min of Police*)

Independent Newspaper Pty Ltd v Minister of Intelligence Services and others 2008 (ZACC)(*Independent Newspaper Pty Ltd v Minister of Intelligence Services*)

Intercape Ferreira Mainliner (Pty) Limited v Pro-Haul Transport Africa CC & Another Case No. 44350/2012 (ZAGPJHC) (*Intercape v Pro-Haul*)

Inter-Science Research and Development Services (Pty) v Republica Popular de Mocambique 1980 (2) SA 111 (T) (*Inter-Science Research and Development Services (Pty) v Republica Popular de Mocambique*)

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributor (Pty) Ltd v SmitNO 2001 (1) SA 545 (CC) (*Investigating Directorate v Hyundai and Smit No*)

Isaac Metsing Magajane v The Chairperson, North West Gambling Board and Others Case CCT 49/05 (CC) (*Magajane v North West Gambling Board*)

Jackie Sello Selebi v State Case No. 240/2011 (ZASCA) (*Selebi v State*)

Jafta v Ezemvelo KZN Wildlife 2008 10 BLLR 954 (LC) or (2009) 30 ILJ 131 (LC) (*Jafta v Ezemvelo*)

Jamieson v Sabingo 2002 (4) SA 49 (SCA) 5 (*Jamieson v Sabingo*)

Johncom Media Investments Limited v M and Others (CCT08/08) 2009 (ZACC) 5(*Johncom Media Investments Limited v M and Others*)

Jwara v S (916)/13 2015 (ZASCA) 33 (*Jwara v S*)

Kaffraria Property v Government of the Republic of Zambia 1980 (2) SA 709 (E) (*Kaffraria Property v Government of the Republic of Zambia*)

Kaunda & others v President of the Republic Case CCT 23/04 (*Kaunda v President*)

KLD Residential v Empire Earth Investments (1135/2016) 2017 (ZASCA) 98(*KLD Residential v Empire Earth Investments*)

Klein v Attorney-General, WLD 1995 (3) SA 848, 865 (W) (*Klein v Attorney-General*)

Laugh It Off Promotions CC v South African Breweries International (Finance) BV t/a Sabmark International and Another CCT42/04 2005 (ZACC) 7; 2006(1) SA 144(CC), 2005(8) BCLR 743(CC) (*Laugh It Off Promotions CC v South African Breweries International*)

Lenco Holdings Ltd v Eckstein 1996(2) SA 693 (N) 700 (*Lenco Holdings Ltd v Eckstein*)

Loureiro and Others v iMvula Quality Protection (Pty) Ltd 2014 (ZACC) 4 (*Loureiro v iMvula*)

LSD v Vachell 1918 WLD 127 (*LSD v Vachell*)

Mathias International Limited & Another v Monique Baillache &Others Case No.23347/09 (ZAWCHC) (*Mathias Int. Ltd v Baillache*)

McBride v Minister of Police and Another 2016 (ZACC) 30 (*McBride v Minister of Police*)

Meter Systems Holdings Ltd v Venter and Another 1993 (1) SA 409 (W) 428 - 430 (*Meter Systems Holdings Ltd v Venter*)

Mgomezulu v NDPP (338/06) 2007 (ZASCA) 129 (RSA) (*Mgomezulu v NDPP*)

Mholongo v Bailey & another 1958 (1) SA 370 (W) (*Mholongo*)

Minister of Finance v Gore NO 2007(1) SA 111 (SCA) (*Minister of Finance v Gore*)

Minister of Safety & Security v Antus Van Niekerk 2007 (ZACC) 15 (*Min of Safety v Van Nierkerk*)

Minister of Safety & Security v Sekhoto 2011 (5) SA 367 (SCA) (*Minister of Safety & Security v Sekhoto*)

Minister of Safety and Security & another v Swart (194/11) 2012 (ZASCA) (*Minister of Safety and Security v Swart*)

Minister of Safety and Security & another v Van der Merwe & others 2010 JOL 26089 (SCA) (*Min of Safety and Security v Van der Merwe*)

Minister of Safety and Security v Luiters 2006 (ZACC) 21; 2007 (2) SA 106 (CC); 2007 (3) BCLR 287 (CC) (*Minister of Safety and Security v Luiters*)

Mistry v Interim National Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC) 28 ('*Mistry v Medical and Dental Council*')

Mnyungala v Minister of Safety & Security 2004 (1) SACR 219 (TK)(*Mnyungala v Minister of Safety & Security*)

Mohunran & Another v NDPPP & Others 2007 (6) BCLR 575 (CC)(*Mohunran v NDPPP*)

National Coalition for Gay and Lesbian Equality & Others v The Minister of Home Affairs & Others CCT 10/99 1999 1 SA (CC) ('*Gay and Lesbian v Min of Home Affairs*')

National Commissioner of South African Police & Another v Forensic Data Analysts (Pty) Ltd & Others Case number: 24570/2018 (ZAGPPHC) (*SAPS v Forensic Data*)

National Commissioner of The South African Police Service v Southern African Human Rights Litigation Centre and Another CCT 02/14 2014 (ZACC) 30 ('*SAPS v Zim & Dugard*)

National Director of Public Prosecutions v Zuma 2009 2 SA 277 (SCA)(*NDPP v Zuma*)

National Directorate of Public Prosecution and others v *Freedom under Law* Case No. 67/2014 (ZSCA) (*NDPP v Freedom Under Law*)

National Directorate of Public Prosecution v Geyser 2008 (ZASCA) (*NDPP v Geyser*)

National Directorate of Public Prosecution v Mahomed 2007 (SCA) 138 (*NDPP v Mahomed*)

National Directorate of Public Prosecution v Stander & Others 2008 1 SACR (E) 116 (*NDPP v Standers*)

National Directorate of Public Prosecution v Van Staden & others (730/2011) 2012 (ZASCA) 171(*NDPP v Van Staden*)

National Directorate of Public Prosecution v Vermaak 2008 (1) SACR 157 (SCA) (*NDPP v Vermaak*)

National Media Ltd & another v Jooste 1996 (3) SA 262 (A) (ZASCA) (*National Media v Jooste*)

Ndabeni v Minister of Law & Order 1984 (3) SA 500 (D) (*Ndabeni v Minister of Law & Order*)

Nel v Le Roux No & Others Case No CCT30/95 (ZACC) (*Nel v Le Roux*)

NJJ Webb v Road Accident Fund Case No: 2203/14 (ZAGPPHC) (*NJJ Webb v RAF*)

Njongi v Member of the Executive Council, Department of Welfare, Eastern Cape CCT 37/07 2008 (ZACC) 4 (*Njongi v MEC*)

NM & Others v Smith & Others 2007 7 BCLR 751 (CC) (*NM v Smith*)

N v The State (469/2007) 2008 (ZASCA) 30 (*N v The State*)

Okah v State (19/2014) 2016 (ZASCA) 155 (*Okah v State*)

O' Keffe v Argus Printing and Publishing Co Ltd 1954 (3) SA 244 (C) (*O' Keffe v Argus Printing*)

Okundu v State CA&R117/16 2016 (ZAECGHC) 131 (*Okundu v State*)

Patrick Lorenz Martin Gaertner & others v Minister of Finance & Others 2013 (ZACC) 38 (*Gaertner v Min of Finance*)

Pharmaceutical Manufacturers Association of SA: In Re Ex parte President of the Republic of South Africa 2000 (2) SA 674 (CC) (*Pharmaceutical Manufacturers Association of SA: In Re Ex parte President of the Republic of South Africa*)

Pioneer Foods (Pty) Ltd t/a Sasko Milling & Baking (Duens Bakery) v CCMA 2011 32 ILJ 1988 (LC) (*Pioneer Foods v CCMA*)

Powell NO and Others v Van der Merwe and Others (503/2002) 2004 (ZASCA) 25; 2005 1 All SA 149 (SCA) (*Powell v Van der Merwe Powell*)

President of the Republic of South Africa v Hugo 1997 (4) SA 1 (CC) (*President v Hugo*)

Primemedia Broadcasting & Others v Speaker of the National Assembly & Others Case No 2749/ 2015 (ZAWCHC) (*Primemedia v Speaker, National Assembly*)

Protea Technology Ltd v Wainer 1997 (9) BCLR 1225 (W) 1241 or 1997 3All SA 594 (W) 608 (*Protea Technology Ltd v Wainer)*

Ralekwa v Minister of Safety & Security 2004 (2) SA 342 (*Ralekwa v Minister of Safety & Security*)

Rautenbach v Minister of Safety & Security 2017 (2) SACR 610 (WCC) (*Rautenbach v Minister of Safety & Security*)

Rex v Buchanan 1914 AD 509-519 (*Rex v Buchanan*)

R v Abelson 1933 TPD 227 231 (*R v Abelson*)

R v Van Heerden 1958 (3) SA 150 (T) (*R v Van Heerden*)

SAA v BDFM Publishers (Pty) Ltd Case No. 2015/33205 (ZAGPJHC) (*SAA v BDFM*)

SABC v Avusa Limited & Others 2010 (1) SA 280 (GSJ) (*SABC v Avusa Limited*)

SABC v NDPP Case No. CCT 58/06 (ZACC) (*SABC v NDPP*)

SABC v Thatcher Case No: 8924/2004 (ZAWCHC) (*SABC v Thatcher*)

SANEF & ors v EFF and ors 90405/18 (*SANEF & ors v EFF*)

Secombe v Attorney-General 1919 TPD 270 (*Secombe v Attorney-General*)
Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others (CCT1/00) 2000 (ZACC) 12; 2000 (10) BCLR 1079; 2001 (1) SA 545 (CC) (25 August 2000) (‘*Hyundai’*)

Simataa v Magistrate of Windhoek and others 2012 (2) NR 658 (HC) (*Simataa v Magistrate of Windhoek*)

Singh v Ebrahim (413/09) 2010 (ZASCA) 145 (*Singh v Ebrahim*)

Soobramoney v Minister of Health (Kwazulu-Natal) (CCT 32/97) (ZACC) 54 (*Soobramoney v Minister of Health*)

South African National Defence Union v Minister of Defence (CCT/27/98) 1999 (ZACC) 7; 1999(4) SA 469; 1999(6) BCLR 615 25-27 (*South African National Defence Union v Minister of Defence*)

South African National Roads Agency Limited v The City of Cape Town and others case no. 6165/2012 (ZAWCHC) (*South African National Roads Agency Limited v The City of Cape Town*)

State v Cwele & another 2011 (1) SACR 409 (KZP) (*State v Cwele*)

State v de Vries and others 2009(1) SACR 613 (C) (*State v de Vries*)

State v Dodo (2001) 1 *SACR* 594 (CC) (*State v Dodo*)

State v Hena 2006 2 SACR 33 (SE) (*State v Hena*)

State v Ivan Andries Muller CASE NO: 2SH98/2005 (ZAGPHC) (*State v Muller*)

State v Jackie Sello Selebi Case No. 25/09 (ZAGPHC) (*State v Selebi*)

State v Jordan (CCT31/01) 2002 (ZACC) 22, 2002(6) SA 642, 2002(11) BCLR 1117 (*S v Jordan*)

State v Joseph Arthur Walter Brown (681/2013) 2014 (ZASCA) 217 (*State v Joseph Brown*)

State v Jordan (CCT31/01) 2002 (ZACC) 22 (*State v Jordan*)

State v Kleinhans 2014 (2) SACR 575 (WC) (*State v Kleinhans*)

State v Madiba 1998 1 BCLR 38(D) (*State v Madiba*)

State v Makwanyane and Mchunu CCT/3/94 (*State v Makwanyane*)

State v Malgas (2001) 1 SACR 469 (SCA) (*State v Malgas*)

State v Mamabolo (CCT44/00) 2001 (ZACC) 17; 2001 (3)SA 409(CC); 2001(5) BCLR 449(CC) 41 (*State v Mamabolo*)

State v Manamela 2000 (3) SA 1 (CC) (*State v Manamela*)

State v Mark 2001 1 *SACR* 572 (*State v Mark*)

State v Matisonn 1981(3) SA 302 (A) (*State v Matisonn*)

State v Mavinini 2009 (1) SACR 523 (SCA) 26(*State v Mavinini*)

State v Mkhize 2 SACR 632 (W) (*State v Mkhize*)

State v Mshinini & another 2012 (1) SACR 604 (SCA) (*State v Mshinini*)

State v Naidoo 1998 1 *SACR* 479 (N) (*State v Naidoo*)

State v Nkanbinde 1998(8) BCLR 996(N) (*State v Nkanbinde*)

State v Norbert Glenn Agliotti case No SS 154/2009 (ZAGPHC) 136 (*State v Agliotti*)

State v Philip Miller and 8 others 2016 (1) SACR 251 (WCC) (*State v Miller*)

State v Pillay and others 2004 (2) SACR 419(SCA)(*State v Pillay*)

State v Odugo 2001 (1) SACR 560 (W) (*State v Odugo*)

State v Tandwa and Others 2008 (1) SACR 613 (SCA) (*State v Tandwa*)

State v Terrence Stephan Brown 2016 (1) SACR 206 (WCC) (*State v Terrence Brown*)

State v kidson 1999 (1) SACR 338(W) (*State v kidson*)

State v Nombewa 1996 2 *SACR* 396 (E) (*State v Nombewa*)

State v Odugo 2001 (1) SACR 560 (W) (*State v Odugo*)

State v Nel 1967 4 SA 489 (SWA) (*State v Nel*)

State v Philip Miller and 8 Others 2016 (1) SACR 251 (WCC) (*State v Miller*)

State v R 2000 (1) SACR 33 (W) (*State v R*)

State v Tshilo 2000 (4) SA 1078 (CC); 2000 (11) BCLR 1252 (CC) (*State v Tshilo*)

State v Williams 1998 (4) SA 49 (W) (*State v Williams*)

S v A 1971 (2) SA 293 (T) (*S v A*)

S v Nell 1967 (4) SA 489(SWA) (*S v Nell*)

Sydney v Minister of Safety & Security Case No.: CA115/2009 (ZAECGHC) 5 (*Sydney v Minister of Safety & Security*)

Thatcher v Minister of Justice and Constitutional Development and Others 2005 (4) SA 543 (C) (*Thatcher v Minister of Justice*)

The Citizen 1978 (Pty) Ltd and Another v Robert John Mcbride Case CCT 23/10 2011 (ZACC) (*Citizen v Mcbride*)

Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others 2008 (2) SACR 421 (CC) (‘*Thint v NDPP’*)

Universiteit van Pretoria v Tommie Meyer Films 1977(4) SA 376 (T) (*Universiteit van Pretoria v Tommie Meyer Films*)

Van Castricum v Theunissen and Another 1993 (2) SA 726 (T) 731-2 (*Van Castricum v Theunissen*)

Veldman v Director of Public Prosecutions (*Witwatersrand Local Division*) (CCT19/05) 2005 (ZACC) 22, 2007(3) SA 210(CC), 2007 (8) BCLR 827(CC) (*Veldman v DPP*)

Web Call (Pty) Ltd v Stephen Andre Botha & Another Case No: A 50/2014 (ZAWCHC) (*Web Call v Botha*)

B. FOREIGN CASE LAW

BELGIUM

Yahoo! Inc [2015] Court of Cassation of Belgium P.13.2082.N. (*Yahoo! Inc* [2015])

Yahoo! Inc [2013] Belgium Court of Appeal of Antwerp, 12th chamber for criminal cases 2012/CO/1054 (*Yahoo!Inc* [2013])

CANADA

CanadianOxy Chemicals Ltd v Canada (Attorney-General) (1999) 1 S.C.R 743,133, C.C.C. (3d) 426 para 14 (*CanadianOxy v Canada*)

eBay Canada Ltd v M.N.R.(2008), 330 D.L.R (4^{th}) 360, 53 B.L.R (4^{th}) 202 (F.C.A) (*eBay Canada*)

Gloria Bartnicki and Anthony F. Kane, Jr., v Frederick W. Vopper, et al. Nos. 99-1687, 99-1728 72 and 76

Lahaie v Canada (Attorney-General) (2010), 320 D.L.R (4th) 385, 190 A.C.W.S. (3d) 421 (Ont. C.A.). 327 D.L.R (4th)

R v Brand (2006), 216 C.C.C. (3d) 65, 71 W.C.B (2d) 609 (B.C.S.C.)

R v Bryntwick (2002) O J, No 3618(QL), 55 W.C.B (2d) 207(S.C.J)

R v Burke (2011) 275 C.C.C (3d) 90, 965 A. P R 255 (N.B.C.A)

R v Caissey [2008] 3 S.C.R 451, 299, D.L.R (4th) 432, affg. 227 C.C.C (3d) 322, 299 D.L.R (4th) 432 at 433 (Alta C.A.)

R v Chesson (1988) 43 C.C.C (3d) 353, [1988] 2 S.C.R 148

R v Chow [2005] 1 S.C.R. 384

R v Collins 1987 28 *CRR* 122 (SCC) (*R v Collins*)

R v Debot (1989) 52 C.C.C. (3d) 193, [1989] 2 S.C.R. 1140

R v Feeney 1997 44 CRR 2d 1 (SCC)

R v Garafoli [1990] 2 S.C.R 1421 at 1468 or 60 C.C.C (3d) 161

R v Grant (2009) 2 SCR 353 74

R v Hillgardener (2010)252 C.C.C. (3d) 486, 483 W.A.C 200 (Alta.C.A.)

R v Jir (2010) 264, C.C.C (3d) 64, 80 C.R (6th) 53

R v Kokesch 1990 50 CRR 285(SCC) 5, 23 and 26-28 (*R v Kokesch*)

R v Madrid [1994] B.C.J. No 1786 (C.A.)

R v Pangman [2000] 8 W.W.W R. 536, 147 Man. R. (2d) 93 (QB);

R v Schreinert (2002), 165 C.C.C. (3d) 295, 159 O.A.C. 174 (Ont. C.A.)

R v Steel (1995), 34 Alta. L.R. (3d) 440

R v Taylor (1997), 121 C.C.C (3d) 353, 42 C.R.R (2d) 371 (B.C.C.A.), affd [1998] 1 S.C.R. 26, 121 C.C.C. (3d) 353

R v Telus Communication Co. 2011 105 O.R (3d) 411, 93 W.C.B. (2d) 292 (S.C.J)

R v Thompson [1990] 2 S.C.R 1111 at 1137 and 1138 or 59 C.C.C (3d) 225

R v Willis No 99-1492 (7th Cir. 08/29/2002)

R v Willis (1997), 204 A.R.161 [1997] A.J. No 632 (QL) (Prov. Ct.)

R v Wright (1990) 56 C.C.C (3d) 503 at p 517, 40 O.A.C. 171 (CA)

FRANCE

UEJF et Licra c. *Yahoo! Inc. et Yahoo France* 22 mai 2000 (Tribunal de Grande Instance Paris), 2000 Communication et Commerce Electronique (Comm. Com. Electr. Comm. n°92, note J-Chr. Galloux (*UEJF et Licra* c. *Yahoo! Inc. et Yahoo France*)

UNITED KINGDOM

Bishopsgate Investment Management Ltd v Maxwell [1992] 2 All ER 856 (CA)

Commissioner of Corporate Affairs v. Guardian Investments Pty Ltd [1984] VR 1019 at 1023-1025)

Davis v Secretary of State for the Home Department [2015] EWHC 2092 (17/07/2005)

Entores Ltd v Miles Far East Corporation [1955] 2 QB 327(CA) 327 [1955] 2 All ER 493 (*Entores Ltd v Miles*)

Malone v United Kingdom 8691/79 [1984] ECHR 10 (2 August 1984) 7 EHRR 14, (1985) 7 EHRR 14, [1984] ECHR 10

Re Arrows Ltd (No 4) Hamilton v Naviede [1994] 3 All ER 814 (HL),

Schtraks v Government of Israel [1964] AC 556 at 583 (HL)

UNITED STATES OF AMERICA

Bartnicki & others v Vopper, et al. Nos. 99-1687, 99-1728 paras 72 and 76.

Benusan Restaurant Corp. v. King 126 F.3d 25 (2d Cir. 1997)

Calder v Jones 465 U.S. 783 (1984)

Carroll v United States 267 U.S. 132 (1925) at 153

CBS Butler Ltd v Brown & Ors [2013] EWHC 3944 (QB) 32; (CCT25/99) [2000]ZACC 5; 2000(3)SA; 2000(5)BCLR 491 32

CompuServe, Inc. v. Patterson 89 F.3d 1257 (6th Cir. 1996)

Cybersell, Inc v Cybersell, Inc No. 96-17087

David Leon Riley v California and *United States v Brima Wurie* 573 U.S. 2014 (*Riley v California* and *US v Wurie*)

Doe v Bolton, 410 U.S. 179, 213(1967)

Eisenstadt v Baird, 405 U.S 438, 454 (1972)

Ex-Parte Jackson, 96 US 727 (1877)

Filártiga v Peña-Irala 630 F 2d 876 (2d Cir 1980) (*Filártiga*) at 880 and 890;

Gloria Bartnicki and Anthony F. Kane, Jr. v Frederick W. Vopper, et al. Nos. 99-1687

Graphic Controls Corp. v. Utah Medical Prods., Inc. No. 97-1551

Griffin v Wisconsin 483 US 868 at 887(1987),

Hearst Corp. v. Goldberger 1997 U.S. Dist. LEXIS 2065 1997 WL 97097

Illinois v Gates 462 U.S. 213, 232 (1983)

Illinois v Wardlow 528 U.S 119, 125 (2000)

In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 13 Mag. 2814 WL 1661004 (S.D.N.Y. 2014) (*Microsoft I*)

In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., No. 14–2985 (2d Cir. 2016) (*Microsoft II*)

In re Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 840 (S.D.Tex. 2010)

Inset Systems, Inc. v. Instruction Set, Inc 937 F. Supp. 161

Interscope v Duty (05-CV-3744 PHX-FJM, D Ariz, 14 April 2006)

Katz v United States 389 U.S 347 (1967) 350 (*Katz*)

Kent v Dulles 357 U.S 116, 126 (1958)

Kiobel v Royal Dutch Petroleum Co 133 S Ct 1659 (2013)

Lock International Plc v Beswick and Others [1989] 1 WLR 1268 (Ch) at 1280-1283

Maritz Inc v Cybergold 947 F. Supp. 1328 (E.D. Mo. 1996)

McDonough v. Fallon McElligott, Inc 1996 U.S. Dist. Lexis 15139 (S.D. Cal. August 5, 1996)

Maryland Penitentiary v Hayden, 387 U.S 294 (1967)

Olmstead v United States 277 U.S 438 (1928) 466 and 478 (‘*Olmstead’*)

Ornelas v U.S 517 1996 U.S. 695-696

Osborne v Ohio 495 US 103,110 SCt 1691 (1990) (*Osborne v Ohio)*

Panavision International L.P v Toeppen No. 97-55467

People v Diaz Cal Rptr. 3d 105, 2011

Smith v Maryland 25 Cr. L. 3192(U.S. Sup. Ct 1979) (*Smith*)

Sosa v Alvarez-Machain (US Supreme Court) (2004) 43 *ILM* 1390

Stanley v Gorgia, 394 U.S 557, 564(1969)

Union Pac. Ry. Co v Botsford, 141 U.S 250, 251 (1891)

United States of America v Brijido Aguilera 2008 U.S. Dits. LEXIS 10103, ADGN/2008-093

United States v Arvizu 534 U.S. 266 (2002)

United States Department of Justice v Reporters Committee for Freedom of the Press 489 U.S 763-765 (1989) (*United States v Freedom of the Press*)

United States v Arvizu 534 U.S. 266 (2002)

United States v Brima Wurie (*US v Wurie*) 573 U.S. 2014

United States v Cortez 449 U.S. 411(1981) at 417 - 418

United States v Giordano 416 U.S 505 (1974) (*Giordano*)

United States v Jones 565 U.S (2002) 3

United States v Knotts 460 U.S. 276, 282, 103 S. Ct. 1081, 75 L.Ed 2d 55 (1983)

United States v Levin 15-10271-WGY, 2016 WL 2596010 (D. Mass. 2016) 14 (*Levin*)

United States v Mansoori No 99-1492 (7th Cir. 08/29/2002)

United States v Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010)

United States v New York Telephone Co. 35 U.S 360 (1977) (*New York Telephone*)

United States v Pineda-Moreno, 617 F.3d 1120, 1126 (9th cir. 2010)

United States v Verdugo-Urquidez 494 U.S. 259 (1990)

United States v Mansoori No 99-1492 (7th Cir. 08/29/2002)

United States v Ozar 50 F.3d 1440, 1448(8th Cir.)

United States v Quintana, 508 F. 2d 867, 874 (7th Cir. 1975)

United States v Sokolow 490 U.S 1 (1989) 7

Whalen v Roe 429 U.S 589 (1977)

Zippo Manufacturing v Zippo Dot Com Inc. 952 F. Supp. 1119 (W.D. Pa. 1997)

EUROPEAN COURT OF HUMAN RIGHTS

Klass v Germany ECHR [1978] 5029/71

Malone v United Kingdom 8691/79 [1984] ECHR 10 (2 August 1984) 7 EHRR 14, (1985) 7 EHRR 14, [1984] ECHR 10

C. INTERNATIONAL CASE LAW

SS Lotus, France v Turkey 1927 P.C.I .J. (Ser A) No. 10 (decision No. 9) 45 (*Lotus*)

Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (*Bosnia-Herzegovina v Serbia and Montenegro*), 26 February 2007 (ICJ)
Advisory Opinion to the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) ICJ Rep. 2004, 136

Nicaragua case 1986 ICJ Reports

LEGISLATIONS

A. REPUBLIC OF SOUTH AFRICA

Armament Corporation of South Africa Limited Act 51 of 2003

Companies Act 71 of 2008

Constitution of the Republic of South Africa Act 108 of 1996 (Constitution)

Consumer Protection Act 68 of 2008 (COPA)

Correctional Services Act 111 of 1998 (CSA)

Criminal Law Amendment Act 105 of 1997(CLAA)

Criminal Procedure Act 51 of 1977 (CPA)

Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007 (SORMAA)

Customs and Excise Act 91 of 1964

Defence Act 42 of 2002 (DA)

Diamond Act 56 of 1986

Disaster Management Act 57 of 2002 (DMA)

Drugs and Drug Trafficking Act 140 of 1992

Electronic Communications Act 36 of 2005 (ECA)

Electronic Communications and Transactions Act 25 of 2002 (ECTA)

Electronic Communications Amendment Act ('ECAA') 1 of 2014

Extradition Act 67 of 1962

Financial Intelligence Centre Act 38 of 2001(FICA)

Financial Intelligence Centre Amendment Act 1 of 2017 (FICAA)

Firearms Control Act 60 of 2000, which has a regulation title Firearms Controls Regulations 2004

General Intelligence Laws Amendment Act 52 of 2003 (GILAA *I*)

General Intelligence Law Amendment Act ('GILAA *II*) 11 of 2013 (GILAA *II*).

Implementation of the Rome Statute of the International Criminal Court Act 27 of 2002 (Rome Statute)

Income Tax Act 58 of 1962

Independent Police Investigative Directorate Act 1 of 2011(IPIDA)

Intelligence Services Act 65 of 2002 (ISA)

Intelligence Services Control Amendment Act 42 of 1999 (ISCAA 42 of 1999)

Intelligence Services Control Amendment Act 66 of 2002(ISCAA 66 of 2002)

Interception and Monitoring Prohibition Act 127 of 1992

Intimidation Act 72 of 1982

Judges' Remuneration and Conditions of Employment Act 47 of 2001

Maintenance Act 99 of 1998

Maintenance Amendment Act 9 of 2015

Maritime Zones Act 15 of 1994

Merchant Shipping Act 57 of 1951

National Prosecuting Authority Act NPA Act 32 of 1998 (NPAA)

National Sex Offenders Register [section 42 of the Criminal Law (Sexual Offences and Related Matters) Amendment Act, 2007 (Act 32 of 2007)]

National Strategic Intelligence Act 39 of 1994 (NSIA)

Post Office Act 44 of 1958

Prevention and Combating of Corrupt Activities Act 12 of 2004 (PRECCA)

Prevention and Combating of Torture of Persons Act 13 of 2013

Prevention of Organized Crime Act 121 of 1998 (POCA)

Proceeds of Crime Act 76 of 1996

Proclamation 20 of 2019 – Government Gazette No. 42383 of 4 April, 2019

Promotion of Access to Information Act 2 of 2000 (PAIA)

Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004

Protection of Personal Information Act 4 of 2013 (POPIA)

Public Audit Act 25 of 2004 ('PAA')

Public Service Act 103 of 1994 ('PSA')

Secret Services Act 56 of 1978 ('SSA')

South African Police Service Act 68 of 1995 ('SAPSA')

South African Police Service Amendment Act 10 of 2012 (SAPSAA)

Special Investigating Units and Special Tribunal Act 74 of 1996 (SIU Act)

Standards Act 29 of 1993 ('SA')

Regulation of Gathering Act 205 of 1993

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

Regulation of Interception of Communications and Provision of Communication-related Information Act (Amendment) 48 of 2008 (RICAA)

Telecommunications Act 103 of 1996

Terrorism Act 33 of 2004

B. FOREIGN LEGISLATIONS

AUSTRALIA

Listening Devices Act 1984 of the New South Wales, Australia

BELGIUM

Criminal Code of the Kingdom of Belgium (1867, as of 2018) (French version)

CANADA

Criminal Code of Canada (R.S.C., 1985, c. C-46)

NETHERLANDS

Criminal Code of the Kingdom of Netherlands (1881, amended 2012) (English version)

UNITED KINGDOM

Interception of Communications Act of 1985

Regulation of Investigatory Powers Act 2000

UNITED STATES OF AMERICA

Alien Torts Statute of 1789

Title 18 of U.S.C.

Title 19 U.S.C.

Title 35 U.S.C.

Title 47 U.S.C.

Title 50 of U.S.C.

BILLS

Cybercrime and Cybersecurity Bill 2015 (‘CCB of B-2015)

Cybercrime and Cybersecurity Bill (CCB) B6 – 2017, published in Gazette No 40487 of 9 December, 2016 (CCB B6-2017)

Cybercrime Bill (CB) 2018– Amendments Proposed to Bill – B6 2017 published on the 23 of October, 2018 without a Gazette number (CB 2018 – Amendments Proposed to Bill B6-2017)

Electronic Communications and Transactions Bill 2012 published in Notice No. 888 of 2012 in Gazette No. 35821 of 2012

Private Security Industry Regulation Amendment Bill No 27D- 2012 (PSIRAB)

Protection of State Information Bill [B 6D -2010] (PSIB or Secrecy Bill)

DIRECTIVES, POLICIES AND REGULATIONS

American Bar Association 'Standards on Prosecutorial Investigations' (2014)

Code of Conduct for Members of the NPA under s 22(6) of NPAA No. 32 of 1998 published under GN R1257 in GG 33907 of December, 2010

Correctional Services Regulation (2012)

COVID-19 Regulation of 2 April, 2020

Criminal Procedure Act and Commentary Service No 34, 2005

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in Criminal Matters (OJ L 130, 1.5.2014) 12(4) (Directive 2014/41/EU)

Disaster Management Act 2002: Amendment of Regulations Issued in Terms of Section 27(2) in Gazette No 43148 of 25 March, 2020 (DMA COVID-19 Regulation of 25 March, 2020)

Disaster Management Act 2002: Amendment of Regulations Issued in Terms of Section 27(2) in Gazette No 43199 of 2 April, 2020 (DMA COVID-19 Regulation of 2 April, 2020).

Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean '*Interception of Communication: Model Policy Guideline & Legislative Text'* (2012) (HIPCAR *Interception of Communication: 'Model Policy Guideline & Legislative Text* 2012)

Ministry for Intelligent Services 'Regulation 4 -Profile of an intelligence officer' Notice No. 1505 Regulation No. 7797 Gazette No. 25592 of 2003

NPA *Lawyers for the people- South African prosecuting service* (2011) (NPA '*Prosecuting Service'*)

NPA ‘Prosecution Policy’ (2013)

Regulation 4 -Profile of an intelligence officer’ of the Ministry for Intelligent Services, Notice No 1505 Regulation No. 7797 Gazette No. 25592 of 2003 (Regulation 4 -Profile of an intelligence officer)

Regulation 8(4)(a) of Correctional Services Act (111/1998): Promulgation of Correctional Services Regulations with Amendments Incorporated No 35277 of 2012 (Correctional Services Regulation)

Schedule A of Directive for Fixed Line Operators in terms of section 30(7)(a) read with section 30(2) of the Regulation of Interception of Communications and Provision of communication Related Information Act No - 70 of 2002 - No. 28271 Government Gazette, Notice 1325 of 28 November 2005 (Schedule A of RICA)

Schedule B of Directive for Mobile Cellular Operators in terms of Section 30(7)(a) read with Section 30(2) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002) No. 28271 Government Gazette, Notice 1325 of 28 November 2005 (Schedule B of RICA)

Schedule C of Directive for Internet Service Providers in terms of Section 30(7)(a) read with section 30(2) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 OF 2002’ - No. 28271 Government Gazette, Notice 1325 of 28 November 2005 (Schedule C of RICA)

State Security Agency: National Cybersecurity Policy Framework for South Africa No. 609 Government Gazette No 39475 4 December, 2015 (‘National Cybersecurity Policy Framework No 39475 of 2015’)

OFFICIAL REPORTS

Department of Defence and Military Veterans 'Annual Report FY 2012/13'

Department of Justice and Constitutional Development 'National Prosecuting Authority; Asset Forfeiture Unit, Special Investigating Unit, Directorate of Special Operations: budget hearing'

Department of National Treasury 'Public Sector Supply Chain Management Review' (2015)

IPID 'Briefing to the Select Committee on Security & Justice on IPID's Budget 2017/18 and Annual Performance Plan (2017/18)' (2017)

Kaspersen H W K 'Cybercrime and Internet jurisdiction' (Discussion Paper (draft) 28) delivered to the Project on Cybercrime of the Council of Europe Version 5, March 2009

National Rapporteur on Trafficking in Human Beings, 'Child Pornography – First Report of the Dutch National Rapporteur' (2011)

NIA 'Office of the inspector-general of intelligence, executive summary of the final eport of the findings of an investigation into the legality of the surveillance operations carried out by NIA on Mr. S Macozoma – 23 March, 2006' (NIA 'Investigations on Mr. Macozoma')

Nuggent R *Commission of inquiry into tax administration and governance by SARS report* (2018) (Nuggent *Commission of inquiry into tax administration and governance by SARS report*)

Office of the Public Protector 'State of Capture Report No. 6 of 2016/17' (OPP 'State of Capture Report')

Parliament 'Annual Report of the Joint Standing Committee on Intelligence for the Financial Year ending 31 March 2017' (JSCI Report 2017)

Parliament 'Committee Report' No 164-2016 40

Parliament of the Republic of South Africa 'Announcements, Tablings and Committee Report' No 164-2016 (JSCI Report 2016)

Phakgadi P 'KZN premier Mchunu has 21 days to study Moerane report on political killings'

Secretary General 'Report of the Secretary-General on UN United Nations Activities in Support of Mediation (2017) 19

South African Police Service Annual Report 2008/2009

South African Police Service 'Annual Report 2011/2012'

South African Police Service 'Annual Report 2012/2013'

South African Police Service 'Annual Report 2017/2018'

Secretary General 'Report of the Secretary-General on UN United Nations Activities in Support of Mediation (2017) 19

United Nations Office on Drugs and Crime 'Comprehensive Study on Cybercrime' (2013) 222 (UNODC *Study on Cybercrime* (2013))

INTERNATIONAL CONVENTIONS, TREATIES AND INSTRUMENTS

African Charter on the Rights and Welfare of the Child 1990

African Union Convention on Cyber Security and Personal Data Protection (AUCCSPDA) 2014

Agreement on Trade-Related Aspects of Intellectual Property Rights of 1994 (TRIPS)

Antarctica Treaty 1959

Charter of the United Nations (United Nations Charter) 1945

Chicago Convention of 1948

Convention on International Trade in Endangered Species of Wild Fauna and Flora 2009

Convention on the Prevention and Punishment of the Crime of Genocide, 9 December 1948

Council of Europe on the Convention on Cybercrime 2004 - Budapest, 23.XI.2001 (CoE CoCC)

Council of Europe European Convention on Mutual Assistance in Criminal Matters ETS no. 030 1959, which is pursuance of the Schengen Convention

Council of Europe 'Chart of Signatures and Ratifications of Treaty 185 - *Convention on Cyber Crime* -Status as at 02/06/2017 (CoE CoCC)

Council of Europe 'Drafts Elements of Additional Protocol to the Budapest Convention on Cybercrime Regarding Transborder Access to Data' (2013) T-CY (2013) 14

Department of Justice and Constitutional Development 'Mutual Legal Assistance in Criminal Matters Treaty between the Republic of South Africa and the Argentine Republic' (2017)

Department of Justice and Constitutional Development 'Mutual Legal Assistance in Criminal Matters in the Treaty between the United States of America and South Africa' (1999) (MLA-USA-RSA)

Department of Justice and Constitutional Development 'Mutual Legal Assistance in Criminal Matters Treaty between the Republic of South Africa and the Argentine Republic' and RSA 'Mutual Legal Assistance in Criminal Matters in the Treaty between the United States of America and South Africa' (1999) but entered into force in 2001

Directive 2014/41/EU of the European Parliament and of the Council on European Investigation Order in Criminal Matters of 3 April 2014 (OJ L 130, 1.5.2014) 12(4) 2014

Directive 2002/58/EC of the European Parliament and of the Council on Privacy an Electronic Communications of 12 July 2002 ('Directive 2002/58/EC')

Directive 95/46/EC of the European Union Data Protection (EUDP)

Extradition Agreement between the Republic and China, GNR 34 GG 27168 of January 2005

European Convention on Human Rights 1953

Framework Decision 2002/584/JHA (European Arrest Warrant) Official Journal L 190, 18.07.2002 1-20

Geneva Convention 1929

General Assembly Resolution 55/25 of 15 November 2000 titled 'United Nations Convention against Transnational Organized Crime' ('TOCC')

International Convenant on Civil and Political Rights 1966

ITU 'Interception of Communications: Model Policy Guidelines and Legislative Text' (2012) (ITU 'Interception Policy & Legislative Text' (2012)

ITU ‘HIPCAR *Interception of Communication: ‘Model Policy Guideline & Legislative Text* 2012 (ITU ‘HIPCAR Interception of Communication 2012’)

ISO/IEC 7498-1:1994 “Information technology – Open systems interconnection – Basic reference model: The basic model”

Patent Cooperation Treaty 1978

Protocol against the Smuggling of Migrants by Land, Sea and Air, Supplementing the United Nations Convention against Transnational Organized Crime 2000 *Annex III* of TOCC (SOPLSA)

Resolution 2525 (XXV), Paust and Blaustein 1974 68 *AJIL* 410

Rome Statute of the International Criminal Court 2002

Security Council Resolution 1593 of 31 March, 2005

United Nations Convention on the Use of Electronic Communications in International Contract 2007 (‘UNECOMIC’)

United Nations Office on Drugs and Crime *Handbook on police accountability, oversight and integrity* (2011)

United Nations Office on Drugs and Crime ‘Model Legislative Provisions against Organised Crime’ 2012 (UNODC ‘Model Legislative Provisions Against Organised Crime’ 2012)

United Nations Office on Drugs and Crime *Comprehensive Study on Cybercrime –Draft* 2013

Universal Declaration on Human Rights 1948