ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS

Thesis Presented for the Degree of

DOCTOR OF PHILOSPHY

In the Department of Public Law

UNIVERSITY OF CAPE TOWN

July 2020

By Nerisha Singh with student number SNGNER009

Faculty of Law

Supervisor: Professor PJ Schwikkard

DECLARATION

I am now presenting the thesis for examination for the degree of Doctor of Philosophy. I, Nerisha Singh, hereby declare that the work on which this thesis is based is my own unaided work, both in concept and execution, and that apart from the normal guidance from my supervisor, I have received no assistance (except where acknowledgments indicate otherwise). I further declare that neither the substance nor any part of the above thesis has been in the past, or is being, or is to be submitted for a degree at this University, or any other University. I authorise the University to reproduce for the purpose of research either the whole or any portion of the contents in any manner whatsoever.

Signed by candidate

Nerisha Singh

July 2020

ABSTRACT

The research question central to the thesis is stated as follows: what are the implications of new technological phenomena in South African law to the existing legal frameworks in relation to (i) investigatory powers of law enforcement and security and intelligence agencies to obtain electronic evidence, and (ii) its subsequent admissibility in criminal proceedings? Written with an emphasis on South African law, but also taking into account aspects of foreign and international law, the thesis seeks to investigate how our existing legal frameworks which regulate the use of and access to electronic evidence in criminal proceedings, including its admissibility, integrate and adapt to challenges raised by new and rapidly changing technological developments.

The thesis provides a critical analysis of the existing legal framework regulating certain key investigative powers of law enforcement and security and intelligence agencies in the current modern environment of the information age in which they operate. Key among them is the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002. New technology has not only increased opportunities for criminal activity, it has also created opportunities for law enforcement and security and intelligence agencies to have access to more sophisticated and new capabilities. The range of intrusive capabilities now available to law enforcement and security and intelligence agencies triggers a range of issues and challenges for individual rights, including how those capabilities are used in investigation activities, the scale of their use, the extent to which such capabilities intrude on privacy rights, legislative authority for their use and safeguards that constrain and regulate such new technological capabilities. The challenges of regulating investigative powers in an era of new and fast-paced technological developments is explored in relation to (i) interception of communications (ii) acquisition and retention of communications data, and (iii) access to encrypted information.

The introduction of electronic evidence in criminal legal proceedings raises unique challenges in the South African law on evidence. The most interesting perhaps is the extent to which the nature of the evidence presented, in this instance electronic evidence, impacts on admissibility in criminal proceedings. Potential anomalies arise as the relevant legislation, the Electronic Communications and Transactions Act 25 of 2002, is based on an electronic commerce model law concerned with commercial activities. In this regard, two separate issues are the focus of research interest. The thesis offers a rethinking of (a) admissibility of electronic evidence and (b) its weight. The meaning and application of certain statutory provisions, insofar as it applies to electronic evidence as hearsay or real evidence, or both, are key and controversial issues. Another relates to the business records exceptions, which directly translated for electronic records appears to have created a problematic presumption. On matters of evidential weight, there is no ‘one-size-fits-all’ approach that will work. While a robust consideration of authentication is required in the court’s assessment of evidential weight of electronic evidence, it should not be subject to inflexible tests that make it difficult for authentic electronic evidence to be admitted into evidence.

A central premise of the thesis is that evolving technological phenomena can and do present challenges to existing legal concepts on evidence and the investigatory powers of law enforcement and the security and intelligence agencies to obtain electronic evidence and for its admissibility in criminal proceedings. This is done in the context of understanding whether South African law has developed appropriately in response to advancements in technology. In the final analysis, the thesis considers appropriate and meaningful reform towards a modern and transparent legal framework in South African law.

To my parents, Dhuneshwur and Lallitha Singh,
whose love and courage make everything possible.

"Piglet noticed that even though he had a very small heart, it could hold a rather large amount of gratitude" (A.A. Milne)

ACKNOWLEDGEMENTS

Pride of place belongs to my parents, Johnny and Lallitha Singh and to my siblings, Nerika, Shameel and Kerisha—all of whom have been a great inspiration in my life. I continue to be deeply grateful to them for their love and support. I have been equally blessed with the love of my niece Shreya, and nephews, Aryan, Veer, Shivan and Shreemaan.

I am sincerely indebted to my supervisor, Professor PJ Schwikkard, whose wise and tactful criticism was always accompanied by encouragement. I am grateful for her insights and comments on earlier drafts and, no less, her inspiring and scholarly lead.

In more pressing moments, thought-provoking discussions and welcome inspiration have been readily and wholeheartedly offered by a truly extraordinary friend and mentor, Mustafizur Rahman, especially at times when writing was challenging, and spirits low. This thesis emerged amid many friendships and this note would not be complete without a gesture of appreciation and gratitude to the University of Cape Town and University of Witwatersrand law library staff, and postgraduate class of 2016 for their kindness and support.

Most of all, this thesis would not have been completed with the strength, patience and companionship of Gloria Ryoo. When I went through some of my toughest times, she was my beacon of strength. Her superpower—keeping me calm while I had panic attacks over comma placement. As my place of possibility, she got me to think about another way, a better way. I dedicate this thesis to her, my very own *aman cara*. I forever remain grateful for her love, sense of humour, awe-inspiring confidence, and belief in me, especially at times when writing was challenging, and spirits low.

In a year that has changed, and challenged, the world in so many ways, today feels exactly how I imagined—ineffable.

Nerisha Singh
Johannesburg
July 2020

ABBREVIATIONS

The following abbreviations have been used in this thesis:

2016 Act	Investigatory Powers Act 2016
CID	Crime Intelligence Division
CPA 51 of 1977	Criminal Procedure Act 51 of 1977
DIA	Digital Illustrative Aids
DRE	Digital Reconstruction Evidence
ECT Act 2002	Electronic Communications and Transactions Act 25 of 2002
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
LEA Act 1988	Law of Evidence Amendment Act 45 of 1988
MD5	Message Digest 5
MLEC	Model Law on Electronic Commerce
NCC	National Communications Centre
NIA	National Intelligence Authority
NPA	National Prosecuting Authority
NPAA 32 of 1998	National Prosecuting Authority Act 32 of 1998
NPAAA 61 of 2000	National Prosecuting Authority Amendment Act 61 of 2000
NSIA 39 of 1993	National Strategic Intelligence Act 39 of 1994
OIC	Office for Interception Centres
RICA 2002	Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002
SANDF	South African National Defence Force
SAPS	South Africa Police Service
SHA	Secure Hash Algorithm
SSA	State Security Agency
UNCITRAL	United Nations Commission on International Trade Law
URL	Uniform Resource Locator
USB	Universal Serial Bus

CONTENTS

TABLE OF CASES

South African:

ABSA Bank Ltd v Le Roux and Others 2014 (1) SA 475 (WCC).

amaBhungane Centre for Investigative Journalism NPC and SP Sole v Minister of Justice and Correctional Services and Others Case No: 25978/2017 (16 September 2019).

Bernstein and Others v Bester NO and Others 1996 (2) SA 751 (27 March 1996).

Bossasa Operations (Pty) Ltd v Basson & Another 2013 (2) SA 570 (GSJ).

Case and Another v Minister of Safety and Security and Others, Curtis v Minister of Safety and Security and Others 1996 (3) SA 617 (CC).

Coetzee v Government of the Republic of South Africa 1995 (4) SA 631 (CC).

Director of Public Prosecution v Modise 2012 (1) SACR 553 (GSJ).

Dotcom Trading 121 (Pty) Ltd t/a Live Africa Network News v The Honourable Mr Justice King NO and Others 2000 (4) All SA 128 (C).

Ex parte the Minister of Justice: In re R v Jacobson and Levy 1931 AD 466.

Ex parte Minister of Justice: In re R v Matheba 1941 AD 75.

Ex Parte Rosche [1988] 1 All ER 318 (W).

Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and Another (612/90) [1993] 2 All SA 109 (A) (18 February 1993).

Firstrand Bank Limited v Venter 2012 JDR 1676 (SCA).

Fedsure Life Insurance v Greater Johannesburg Transitional Metropolitan Council 1999 (1) SA 374 (CC).

Ferreira v Levin NO and Others; Vryenhoek and Others v Powell NO and Others 1996 (1) SA 984 (CC).

Gaertner and Others v Minister of Finance and Others 2014 (1) SA 442 (CC).

Glenister v President of the Republic of South Africa and Others 2011 (3) SA 347 (CC) (referred to as 'Glenister II).

Golden Fried Chicken (Pty) Ltd v Yum Restaurants International (Pty) Ltd 2005 BIP 269 (T).

Goorpurshad v R 1914 35 NLR 87.

Government of RSA v The Sunday Times 1995 (2) BCLR 182 (T).

Johncom Media Investments Limited v M and Others 2009 (4) SA 7 (CC).

Haysom v Additional Magistrate, Cape Town and Another 1979 (3) SA 155 (C).

Helen Suzman Foundation v President, RSA: in re Glenister v President, RSA 2014(4) BCLR 841 (WCC).

S v Veldthuizen 1982 (3) SA 413 (A).

S v Williams and Others 1995 (3) SA 632 (CC).

S v Zuma and Others 1995 (1) SACR 568 (CC).

Seccombe and Others v Attorney-General 1919 TPD 270.

Scagell and Others v Attorney-General of the Western Cape and Others 1997 (2) SA 368 (CC).

South African National Defence Union v Minister of Defence and Another 1999 (4) SA 469 (CC).

Sublime Technologies (Pty) Ltd v Jonker and Another 2010 (2) SA 522 (SCA).

Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others 2009 (1) SA 1 (CC).

Trend Finance (Pty) Ltd and Another v Commission for SARS and Another [2005] 4 All SA 657 (C).

Wehmeyer v Lane 1994 2 BCLR (C); 1994 4 SA 441 (C).

Zuma v Democratic Alliance and Others 2018 (1) SA 200 (SCA).

Foreign:

Canada:

R v Collins (1987) 33 CCC (3d) 1 (SCC) ((1987) 38 DLR (4th) 508 (SCC).

R v Stillman (1997) 113 CCC (3d) 321 (SCC) ((1997) 144 DLR (4th) 193 (SCC).

Court of Justice of the European Union:

Joined cases of *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications and Others Kärntner Landesregierung and Others (C-594/12)* CJEU (08 April 2014).

European Court of Human Rights:

Amann v Switzerland EctHR 27798/95 (16 February 2000).

Association for European Integration and Human Rights and Ekimhzhiev EctHR 62540/00 (28 June 2007).

Big Brother Watch & Ors v United Kingdom 58170/13 (13 September 2018).

Centrum för Rättvisa v Sweden EctHR 35252/08 (19 June 2018).

Funke v France (1993) 16 EHRR 297.

Goodwin v United Kingdom EctHR 17488/90 (27 March 1996).

Huvig v France (1990) 12 EHRR 528.

Iordachi and others v Moldova 25198/02 (10 February 2009).

United States v Hubbell 530 U.S. 27 43 (2000)

United States v Fricosu 841 F. Supp. 2d 1232, 1237 (D Colo 2012).

United States v Jones,565 U.S. ___, ___ (2012).

United States v Kirschner 823 F. Supp. 2d 665, 669 (ED Mich 2010).

United States v Meienberg 263 F.3d 1177 (10th Cir 2001).

United States v Mitchell II 76 M.J. 413, 424–25 & n.5 (CAAF 2017).

United States v Pearson No. 1:04-cr-340, 2006 U.S. Dist. LEXIS 32982 (NDNY May 24, 2006).

United States v Siddiqui 235 F.3d 1318, 1322-23 (11th Cir 2000).

United States v Spencer No. 17-cr-00259-CRB-1, 2018 WL 1964588 (ND Cal Apr 26, 2018).

United States v United States District Court for the Eastern District of Michigan et al 407 US 297 (1972).

United States v Wade 388 U.S. 218, 222, 87 S.Ct. 1926, 18 L.Ed.2d 1149 (1967).

United States v White 401 U.S. 745 (1971).

Williams v Sprint/United Mgmt Comp 230 FRD. 640, 655 (D Kan 2005).

TABLE OF STATUTES

Primary Sources

Constitution

Constitution of the Republic of South Africa, 1996.

Statutes – Domestic

Criminal Procedure Act 51 of 1977.

Electronic Communications and Transactions Act 25 of 2002.

Law of Evidence Amendment Act 45 of 1988.

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

Statutes – Foreign

Australia:

Surveillance Devices Act 2004.

Telecommunications Act 1997.

Telecommunications (Interception and Access) Act 1979.

Canada:

Canadian Security Intelligence Service Act 1984.

Criminal Code (R.S.C. 1985).

Protection of Privacy Act 1974.

New Zealand:

New Zealand Security Intelligence Service Act 1969.

The Search and Surveillance Act 2010.

United Kingdom:

Criminal Justice Act 2003.

Human Rights Act 1998.

Investigatory Powers Bill 2015.

Investigatory Powers Act 2016.

Police and Criminal Evidence Act 1984.

Regulation of Investigatory Powers Act 2000.

United Stated of America:

Electronic Communications Privacy Act 1986.

The Wiretap Act 1968.

The Stored Communications Act (codified at 18 U.S.C. Chapter 121 §§ 2701–2712).

The Pen Register Act (codified at 18 U.S.C., Chapter 206).

BIBLIOGRAPHY

Secondary Sources

Books

Akhgar, B & A Staniforth, F Bosco *Cyber Crime and Cyber Terrorism Investigator's Handbook* (2014) Elsevier, Amsterdam.

Ashworth, A *Human Rights, Serious Crime and Criminal Procedure* (2002) Sweet and Maxwell, London.

Bartlett, J *Orwell vs Terrorists: Crypto-wars and the future of surveillance* (2015) Penguin, London.

Buys, R & F Cronjé, *Cyberkaw@SA II: The Law of the Internet in South Africa* 2ed (2004) Van Schaik, Pretoria.

Bainbridge, D *Introduction to Computer Law* 5ed (2004) Longman Publisher Group, London

Cairncross, F *The Death of Distance: How the Communications Revolution Will Change our Lives* (1997) Harvard Business School Press, Boston, Massachusetts.

Cairncross, F The Death of Distance: How the Communications Revolution is Changing our Lives (2001) Harvard Business Review Press, Boston, Massachusetts.

Casey, E *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (2004) Elsevier, Amsterdam.

Choo, A *The Privilege against Self-incrimination and Criminal Justice* (2013) Hart Publishing, Oxford.

Clayton, R & M Tomlinson *The Law of Human Rights* (2000) Oxford University Press, Oxford.

Cohen, A & S Park 'Compelled decryption and the Fifth Amendment: Exploring the technical boundaries' (2018) 32.1 *Harvard Journal of Law & Technology* 170.

Currie, I & J de Waal *The Bill of Rights Handbook* 6ed (2013) Juta, Cape Town.

Davis, H *Human Rights and Civil Liberties* (2003) Taylor & Francis Group, London.

Dennis, I *The Law of Evidence* (2007) 3ed Sweet & Maxwell, London.

Gillespie, AA *Cybercrime: Key Issues and Debates* 2ed (2019) Routledge, Abbingdon.

Glover, R *Murphy on Evidence* 15ed (2015) Oxford University Press, Oxford.

Grabosky, PN & RG Smith *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities* (1998) Transaction Publishers, New Brunswick.

Hoffmann, LH & DT Zeffertt *South African Law of Evidence* 4ed (1988) Butterworth, Durban.

Keane, A *The Modern Law of Evidence* (2008) Oxford University Press, Oxford.

Lyon, D *The Electronic Eye: The Rise of Surveillance Society* (1994) University of Minnesota Press, Minnesota.

Menezes, AJ & PC van Oorschot & SA Vanstone *Handbook of Applied Cryptography* (1997) CRC Press, Boca Raton.

Reed, C *Computer Law* 7ed (2012) Oxford University Press, Oxford.

Rule, JB *Private Lives and Public Surveillance* (1973) Shocken Books, New York.

Schwikkard, PJ & SE van der Merwe in collaboration with DW Coller, WL de Vos, A St Q Skeen and E van der Berg *Principles of Evidence* 2ed (2002) Juta, Cape Town.

Schwikkard, PJ & SE van der Merwe *Principles of Evidence* 4ed (2015) Juta, Cape Town.

Stone, R *Textbook on Civil Liberties and Human Rights* 5ed (2004) Oxford University Press, Oxford.

Tapper, C *Computer Law* (1989) Longman Group, London.

Tapper, C *Cross and Tapper on Evidence* (2007) Oxford University Press, Oxford.

Van der Merwe DP *Information and Communications Technology Law* (2008) LexisNexis, South Africa.

Walden, I *Computer Crimes and Digital Investigations* (2007) Oxford University Press, Oxford.

Wasik, M *Crime and the Computer* (1991) Oxford University Press, Oxford.

Westin, AF *Privacy and Freedom* (1967) Atheneum. New York.

Zeffertt, DT & DT Paizes *The South African Law of Evidence* 2ed (2003) LexisNexis, South Africa.

Journal articles / chapters in books / newspapers / Internet references

Akdeniz, Y 'New privacy concerns: ISPs, crime prevention and consumer rights' (2000) 14.1 *International Review of Law, Computers and Technology* 55.

Albrechtslund, A 'Online social networking as participatory surveillance' (2008) available at *http://firstmonday.org/article/view/2142/1949*, accessed 26 October 2016.

Albrechtslund, A 'Surveillance and ethics in film: *Rear window and the conversation*' (2008) *Albany Journal of Criminal Justice and Popular Culture* available at h*ttp://www.albany.edu/scj/jcjpc/vol15is2/Albrechtslund.pdf*, accessed 26 October 2016.

Baldwin, DA 'The concept of security' *Review of International Studies* 1997.23 available at *https://www.princeton.edu/~dbaldwin/selected%20articles/Baldwin%20%281997%29%20The%20Concept%20of%20Security.pdf*, accessed 22 May 2019.

Bernal, P 'Data gathering, surveillance and human rights: recasting the debate' (2016) 1.2 *Journal of Cyber Policy* 243.

Bilchitz, D 'Privacy, surveillance and the duties of corporations' (2016) *TSAR* 45.

Boland, T & G Fisher 'Selection of hashing algorithms' (2000) available at *https://www.nist.gov/software-quality-group/nsrl-technical-papers*, accessed 21 July 2019.

Brown, LR 'Redefining national security' (1986) 29(3) *Challenge* 25.

Bruce, P 'The price of writing about the Guptas' 29 June 2017 available at *https://www.businesslive.co.za/bd/opinion/columnists/2017-06-29-peter-bruce--the-price-of-writing-about-the-guptas/*, accessed 5 July 2019.

Bucher, B 'WhatsApp, WeChat and Facebook Messenger Apps – Global messenger usage, penetration and statistics' available at *https://www.messengerpeople.com/global-messenger-usage-statistics/*, accessed 04 August 2019.

Chaffey, D 'Global social media research summary 2019' available at *https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/*, accessed 04 August 2019.

Clark, MW 'Cell phones as tracking devices' (2007) 41 *Valparaiso University LR* 1414.

Clough, J 'Cybercrime' (2011) 37 *Commonwealth Legal Bulletin* 671.

Clough, J 'A world of difference: The Budapest convention on cybercrime and the challenges of harmonisation' (2014) 40.3 *Monash University LR* 698.

Coetzee, J 'The Electronic Communications and Transactions Act 25 of 2002: Facilitating electronic commerce' (2003) 3 *Stellenbosch LR* 501.

Cohen, A & S Park 'Compelled decryption and the Fifth Amendment: Exploring the technical boundaries' (2018) 32.1 *Harvard Journal of Law and Technology* 169.

Collier, DW 'Electronic evidence and related matters' in PJ Schwikkard & SE van der Merwe 3ed *Principles of Evidence* (2009) Juta, Cape Town.

Colvin, M 'Surveillance and the Human Rights Act 1998' in J Beatson (ed) *The Human Rights Act and the Criminal Justice and Regulatory Process* (1999) Bloomsbury, London.

Cushing, T 'State appeals court says unlocking a phone with a fingerprint doesn't violate the Fifth Amendment, TECHDIRT (January 2017) available at *https://www.techdirt.com/articles/20170121/08510936531/state-appeals-court-says-unlocking-phone-with-fingerprint-doesnt-violate-fifth-amendment.shtml*, accessed 14 April 2020.

De Hert, P & PC Bocos 'Case of *Roman Zakharov v. Russia*: The Strasbourg follow up to the Luxembourg Court's *Schrems* judgment' available at *https://strasbourgobservers.com*

/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/, accessed 16 May 2019.

Du Toit, P 'A judge's report shows SA's police, spies are requesting more wiretapping' (20 December 2012) available at *https://www.huffingtonpost.co.uk/2016/12/20/parliament-isnt-happy-sas-police-spies-are-requesting-more-wi_a_21631740/?ncid=other_saredirect_m2afnz7mbfm&guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAF0JXcRNtaqmbU0M1DUehHr_KRF8Y7ABWanPQPhf9XF1wlLJ4bqRtlV_Cc4GxHplyB7a7Uzw2w3L7hvyFjLxxOyFzyEH0_UG2Qb_Ojp8kZUqubNd2L9zenl3UJaCwg_ctoDTxaAY2kl_029xhnFkD2LDRinvH-sWw4QdHss7trCw*, accessed 22 June 2019.

Duncan, J 'Communications surveillance in South Africa: The case of the Sunday Time's newspaper' available at *https://www.academia.edu/9170517/Communications_surveillance_in_South_Africa_the_case_of_the_Sunday_Times_newspaper*, accessed 19 June 2019. This report was originally published as part of a larger compilation: 'Global Information Society Watch: Communications surveillance in the digital age" available at *http://www.giswatch.org/2014-communications-surveillance-digital-age*.

Duncan, J 'The bugging of South Africa' (29 July 2013) available at *http://sacsis.org.za/site/article/1739*, accessed 17 May 2016.

Duncan, J 'Spies are all set to grab your metadata' (11 September 2015) available at *https://mg.co.za/article/2015-09-10-spies-are-all-set-to-grab-your-metadata*, accessed 30 June 2019.

Duncan, J 'New year's resolution for 2017: Stop unaccountable state spying' (8 January 2017) available at *https://www.dailymaverick.co.za/article/2017-01-08-new-years-resolution-for-2017-stop-unaccountable-state-spying/*, accessed 22 June 2019.

Duncan, J 'Op-Ed: What Ramaphosa needs to do to fix state spying, Part One: Rica and lawful interception' (19 February 2018) available at *https://www.dailymaverick.co.za/article/2018-02-19-op-ed-what-ramaphosa-needs-to-do-to-fix-state-spying-part-one-rica-and-lawful-interception/*, accessed 22 June 2019.

Duncan, J 'Government's thinking on surveillance law is regressive' (5 June 2019) available at *https://mg.co.za/article/2019-06-05-governments-thinking-on-surveillance-law-is-regressive*, accessed 22 June 2019.

Duncan, J 'The loophole in South Africa's state spying laws' (March 2020) available at *https://www.dailymaverick.co.za/article/2020-03-09-the-loophole-in-south-africas-state-spying-laws/amp/?__twitter_impression=true*, accessed 31 March 2020.

Dunlap, T 'Unsecured IoT: 8 ways hackers exploit firmware vulnerabilities' (2019) available at *https://www.darkreading.com/risk/unsecured-iot-8-ways-hackers-exploit-firmware-vulnerabilities/a/d-id/1335564*, accessed 17 February 2020.

Elliott, DW 'Mechanical aids to evidence' 1958 *Criminal LR* 5.

Fischer-Dieskau, S & D Wilke 'Electronically signed documents: Legal requirements and measures for their long-term conservation' (2006) 3 *Digital Evidence and Electronic Signature Law Review* 38.

Folkinshteyn, B 'A witness against himself: A case for stronger legal protection of encryption' 30 (2013) *Santa Clara High Technology LJ* 375.

Galbally, J & J Fierrez, M Martines-Diaz & J Ortega-Garcia 'Evaluations of brute-force attack to dynamic signature verification system using synthetic samples' (2009) paper presented at 10th International Conference on Document Analysis and Recognition available at *http://atvs.ii.uam.es/atvs/files/2009_ICDAR _Brute Force_Galbally_Published.pdf*, accessed 17 October 2016.

Gallavin, C & D Seng, 'Hearsay' in S Mason & D Seng (eds) *Electronic Evidence* 4ed (2017) University of London, London at 70.

Galves, F 'Where the no-so-wild things are: Computers in the courtroom – The Federal Rules of Evidence and the need for institutional reform and more judicial acceptance' (2000) 12 *Harvard JL Technology* 165.

Garcia, R 'Garbage in, gospel out: Criminal discover, computer reliability and the Constitution' (1991) 38 *UCLA LR* 1043.

Gilbert, P 'SA smartphone penetration now at over 80%, says ICASA' 3 April 2019 available at *https://www.itweb.co.za/content/GxwQDM1AYy8MlPVo*, accessed 9 July 2019.

Gillespie, AA 'Regulation of Internet surveillance' (2009) *European Human Rights LR* 552.

Hackett, Y 'The search for authenticity in electronic records' (2003) 3.2 *The Moving Image* 100.

Hoening, M 'Computer simulations and other weapons' (1993) 2 *New York LJ* 3.

Hofman, J 'Electronic evidence in criminal cases' 3 (2006) *SACJ* 257.

Hofman, J 'South Africa' in S Mason (ed) *Electronic Evidence: Disclosure, Discovery and Admissibility* 1ed (2007) LexisNexis Butterworths, London 459.

Hofman, J & J de Jager 'South Africa' in S Mason (ed) *Electronic Evidence* (2012) Butterworths Law, London.

Hosein, G & CW Palow 'Modern safeguards for modern surveillance: An analysis of innovations in communications surveillance techniques' (2013) 74.6 *Ohio State LJ* 1071.

Hosmer. C 'Proving the integrity of digital evidence with time' (2002) 1.1 *International J of Digital Evidence* 1 available at *https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf*, accessed 22 July 2019.

Huey, L & R Rosenberg 'Watching the web: Thoughts on expanding police surveillance opportunities under the Cyber-Crime Convention' (2004) 46 *Canadian Journal of Criminology and Criminal Justice* 597.

Jacobs, W 'The Electronic Communications and Transactions Act: Consumer protection and Internet contracts' 2004 *SA Merc LJ* 556 at 557.

John, T & M Maguire 'Police surveillance and its regulation in England and Wales' in S Field & C Pelser (eds) *Invading the Private: State Accountability and New Investigative Methods in Europe* (1998) Dartmouth Publishing, London.

Joseph, GP 'A simplified approach to computer-generated evidence and animations' (1999/2000) 43 *New York Law School LR* 875.

Keenan, B 'Contingency and Surveillance: Framing the risk of taking risks' (2014) 2.2 *Birbeck LR* 293.

Kerr, OS 'Internet surveillance law after the USA Patriot Act: The Big Brother that isn't' (2003) 97 *Northwestern University LR* 607.

Kerr, OS 'Ex ante regulation of computer search and seizure' 96 (2010) *Virginia LR* 1241.

Kerr, OS 'An equilibrium-adjustment theory of the Fourth Amendment'125 (2011) *Harvard LR* 476.

Kerr, OS 'Executing warrants for digital evidence: The case for restrictions on nonresponsive data' (2015) 48.1 *Texas Tech LR* 1.

Kerr, OS & B Schneider 'Encryption workarounds' (2018) 106 *Georgetown LR* 989.

Kerr, OS 'Compelled decryption and the privilege against self-incrimination' (2019) 97 *Texas LR* 767.

Kiok, J 'Missing the metaphor: Compulsory decryption and the Fifth Amendment' (2015) 24.53 *Public Interest LJ* 53.

Klare, MT 'Redefining national security' (12 March 2009) The Nation available at *https://www.thenation.com/article/redefining-national-security/*, accessed 22 May 2019.

Koops, B-J ' Should ICT regulation be technology neutral' in B-J Koops et al (eds) *Starting Points for ICT Regulation* (2006) Asser Press, The Hague.

Kunz, T & S Okunick and U Viebeg 'Long-term security for signed documents: Services, protocols and data structures' in AU Schmidt, Me Kreutzer & R Accorsi *Long-term and dynamical aspects of information security: Emerging trends in information and communication security* (2007) Nova Science Publishers, New York.

Losey, RC 'Hash: The new bates stamp' (2007) 12 *Journal of Technology L and Policy* 1 at 12-13 available at *https://ralphlosey.files.wordpress.com/2008/07/hasharticleloseycorrected.pdf*, accessed 21 July 2019.

Lynch, C 'Authenticity and integrity in the digital environment: An exploratory analysis of the central role of trust' (2000) available at *https://www.clir.org/pubs/reports/pub92/lynch/*, accessed 21 July 2019.

Lyon, D 'Bentham's panopticon: from moral architecture to electronic surveillance' (1991) 98.3 *Queen's Quarterly* 596.

Mare, A & J Duncan 'An analysis of the communications surveillance legislative framework in South Africa' (November 2015) available at *https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf*, accessed February 2019.

Mare, A 'A qualitative analysis of how investigative journalists, civic activists, lawyers and academics are adapting to and resisting communications surveillance in South Africa' (March 2016) available at *https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/duncan_2_comm_surveillance.pdf*, accessed February 2019.

Mason, S 'Sources of digital evidence' in S Mason (ed) *Electronic Evidence: Disclosure, Discovery and Admissibility* (2007) LexisNexis Butterworths, London.

Mason, S in 'The characteristics of electronic evidence' in S Mason (ed) *Electronic Evidence: Disclosure, Discovery and Admissibility* 1ed (2007) LexisNexis Butterworths, London.

Mason, S 'Electronic evidence: A proposal to reform the presumption of reliability and hearsay' 30 (2014) *Computer Law and Security Review* 80.

Mason, S 'The presumption that computers are "reliable"' in S Mason & D Seng (eds) *Electronic Evidence* 4ed (2017) 101.

Mason, S & A Stanfield 'Authenticating electronic evidence'in S Mason & D Seng (eds) *Electronic Evidence* 4ed (2017) 193.

May, TC 'The cyphernomicon' (1994) 8.3.4 available at *https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ*, accessed on 20 May 2016.

McKinley, D 'New terrains of privacy in South Africa' December 2016 available at *https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/r2kmpdp_new_terrains_of_privacy_in_south__africa_masterset_small.pdf*, accessed February 2019.

McMullan, T 'What does the panopticon mean in the age of digital surveillance?' (2015) available at *https://www.guardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham*, accessed 26 October 2016.

Meeks, BN 'Is privacy possible in the digital age?' (2000) available at *http://www.nbcnews.com/id/3078854/t/privacy-possible-digital-age/#.WHI2fLFh0fN*, accessed 08 January 2017.

Mendel, T 'Defining the scope of national security' (March 2013) at 9 available at *https://www.right2info.org/resources/publications/mendel-on-defining-national-security*, accessed 22 May 2019.

Mitchell, B 'A list of every IP address used by Google' (19 November 2018) available at *https://www.lifewire.com/what-is-the-ip-address-of-google-818153*, accessed 4 July 2019.

Mokgoro, Justice Y 'Annual report on the interception of private communications' (15 October 2015) available at *http://pmg-assets.s3-website-eu-west-1.amazonaws.com/intelligence.pdf*, accessed 22 June 2019.

Morgan, J 'Privacy is completely and utterly dead, and we killed it' (2014) available at *http://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/#609dae69dfbd*, accessed 11 January 2017.

Pistorius, T 'Monitoring, interception and Big Boss in the workplace: Is the devil in the details?' (2009) 12.1 PER available at *http://www.saflii.org/za/journals/PER/2009 /1.html*, accessed 05 January 2017.

Preston, A 'The death of privacy' (2014) available at *https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston*, accessed 11 January 2016.

Reed, C 'The admissibility and authentication of computer evidence: A confusion of issues' in T Green (ed) *British and Irish Legal Education Technology Association* (1990) Law and Technology Centre of UK Law Schools, London.

Reed, C & L Davis 'Electronic commerce' in C Reed & J Angel (eds) *Computer Law* (2000) Blackstone Press, Oxford.

Redmayne, M 'Rethinking the privilege against self-incrimination' (2007) 27 *Oxford Journal of Legal Studies* 209.

Rice, M 'Surveillance: *Zakharov v Russia* and what it means for the Investigatory Powers Bill available at *https://www.opendemocracy.net/en/zakharov-v-russia-refresher-on-how-far-europe-has-come/*, accessed 16 May 2018.

Richards, MN 'The dangers of surveillance' (2013) 26 *Harvard LR* 1934.

Rivest, R 'The MD5-Message digest algorithm' RFC 1321 (1992) *Internet Engineering Task Force* available at *http://www.ietf.org/rfc/rfc1321.txt*, accessed 22 July 2019.

Robert, AJ 'Privilege against self-incrimination – key to encrypted material' (2009) *Criminal LR* 191.

Roberts, A'Privacy, data retention and domination: *Digital Rights Ireland Ltd v Minister for Communications* (2015) 78.3 *The Modern Law Review* 535.

Rodriguez, K 'Tackling state surveillance and protecting human rights' (2012) available at *https://www.eff.org/deeplinks/2012/12/tackling-state-surveillance-and-human-rights-protecting-universal-freedoms*, accessed 08 January 2017.

Roos, A 'Privacy in the Facebook era: A South African legal perspective' (2012) SALJ 375.

Sandywell, B 'On globalisation of crime: the Internet and new criminality' in Y Jewkes & M Yar *Handbook in Internet Crime* (2010) Willan Publishing, Cullompton 38-66.

Salgado, RP 'Fourth Amendment search and the power of the hash' (2005) 119 *Harvard LR* 38.

Sacharoff, L 'Unlocking the Fifth Amendment: Passwords and encrypted devices' (2018) 87 *Fordham LR* 203.

Sacharoff, L 'What am I really saying when I open my smartphone? A response to Orin S. Kerr' (2019) 97 *Texas LR* 63.

Selyukh, A 'A year after San Bernardino and Apple-FBI, Where are we on encryption?' (Dec 2016) available at *https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on*-encryption, accessed 8 April 2020

Selyukh, A 'Apple Vs. The FBI: The unanswered questions and unsettled issues' (March 2016) available at *https://www.knkx.org/post/apple-vs-fbi-unanswered-questions-and-unsettled-issues*, accessed 8 April 2020.

Seng, DB 'Computer output as evidence' (1997) *Singapore Journal of Legal Studies* 130.

Skeen, A St O 'Evidence and computers' (1984) 101 *SALJ* 675.

Slogobin, C 'Surveillance and the constitution' (2009) 55 *The Wayne LR* 1105.

Solove, DJ 'Digital dossiers and the dissipation of Fourth Amendment privacy (2002) 75 *Southern California LR* 1083.

Smith, JC 'The admissibility of statements by computer' [1981] *Crim LR* 387.

Solove, DJ ' Reconstructing electronic surveillance law' (2004) 72 *The George Washington LR* 1701.

Sommer, P 'Digital footprints: Assessing computer evidence' (1998) *Criminal LR Special Edition: Crime, Criminal Justice and the Internet* 61.

Sommer, P 'Computer forensics: An introduction' (1997) available at *http://www.virtualcity.co.uk/vcaforens.htm*, accessed on 16 May 2016.

Swales, L 'An analysis of the regulatory environment governing hearsay electronic evidence in South Africa: Suggestions for reform – Part One' (2018) 21.1 *PER/PELJ* available at *http://www.scielo.org.za/pdf/pelj/v21n1/17.pdf*, accessed 27 July 2019.

Swales, L ' An analysis of the regulatory environment governing hearsay electronic evidence in South Africa: Suggestions for reform – Part Two' (2018) 21.1 *PER/PELJ* available at *http://www.scielo.org.za/pdf/pelj/v21n1/18.pdf*, accessed 27 July 2019.

Swart, H 'Secret state: How the government spies on you' (14 October 2011) available at *http://mg.co.za/article/2011-10-14-secret-state/*, accessed 17 May 2016.

Swart, H 'Big Brother is listening – on your phone' (November 2015) available at *https://mg.co.za/article/2015-11-12-big-brother-is-listening-on-your-phone*, accessed February 2019.

Swart, H 'How cops and crooks can "grab" your cellphone–and you' (November 2015) available at *https://mg.co.za/article/2015-11-29-how-cops-and-crooks-can-grab-your-cellphone-and-you*, accessed February 2019.

Swart, H 'Say nothing–the spooks are listening' (December 2015) available at *https://mg.co.za/article/2015-12-17-say-nothing-the-spooks-are-listening*, accessed February 2019.

Swart, H 'Communications surveillance by the South African intelligence services' (February 2016) available at *https://www.mediaanddemocracy.com/ uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf*, accessed February 2019.

Swart, H 'You always feel like somebody's watching you? They probably are' Daily Maverick (June 2016) available at *https://www.dailymaverick.co.za/article/2016-06-03-you-always-feel-like-somebodys-watching-you-they-probably-are./*, accessed 16 September 2017.

Swart, H 'Cell phone privacy: Law enforcement pulls 70,000 subscribers' call records each year – and that's a minimum estimate' (23 August 2017) available at *https://www.dailymaverick.co.za/article/2017-08-23-cell-phone-privacy-law-enforcement-pulls70*

000-subscribers-call-records-each-year-and-thats-a-minimum-estimate/, accessed 5 July 2019.

Swart, H 'Missed call: Rica registration 'useless' for crime prevention purposes' (November 2016) available at *https://www.dailymaverick.co.za/article/2016-11-10-missed-call-rica-registration-useless-for-crime-prevention-purposes/*, accessed February 2019.

Swart, H 'Your cellphone records and the law: The legal loophole that lets state spying run rampant' 20 May 2018 available at *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 5 July 2019.

Swire, P & K Ahmad 'Encryption and globalization' 13 (2012) *Columbia. Science & Technology LR* 416.

Tapper, T 'Evanescent evidence' (1993) 1.1 *International Journal of Law and Information Technology* 35.

Terzian, D 'The Fifth Amendment, encryption, and the forgotten state interest' 61 (2014) *UCLA LR Discourse* 298.

Terzian, D 'The micro-hornbook on the Fifth Amendment and encryption' (2015-2016) 104 *Geo LJ Online* 168.

Terzian, D 'Forced decryption as equilibrium – Why it's constitutional and how *Riley* matters' (2014-2015) 109 *Northwestern University LR* Online 56.

Thompson II, RM & C Jaikaran 'Encryption: Selected Legal Issues' (2016) available at *https://fas.org/sgp/crs/m isc/R44407.pdf*, accessed 7 April 2020.

Travis, A 'MPs call communications data bill "honeypot for hackers and criminals"' 31 October 2012 *The Guardian* available at *https://www.theguardian.com/technology/2012/oct/31/communications-data-bill-honeypot-hackers-criminals*, accessed 4 July 2019.

Trottier, D & D Lyon 'Key features of social media surveillance' in C Fuchs, K Boersma, A Albrechtslund and M Sandoval (eds) *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (2012) Routledge, New York.

Van Buskirk, E & VT Liu, 'Digital evidence: Challenging the presumption of reliability' 1.1 (2006) *Journal of Digital Forensic Practice* 19.

Van Diemen, E '"Spying case": 8 times journalists believe they were snooped on, as RICA Act gets challenged in court' 4 June 2019 available at *https://www.news24.com/SouthAfrica/News/spying-case-8-times-journalists-believe-they-were-snooped-on-as-rica-act-gets-challenged-in-court-20190604*, accessed 17 June 2019.

Walden, I 'Computer Crime' in C Reed & J Angel (eds) *Computer Law* (2003) Oxford University Press, Oxford.

Warren, SD & and LD Brandeis 'The right to privacy' (1890) *Harvard LR* 193.

Watney, M 'Admissibility of electronic evidence in criminal proceedings: An outline of the South African legal position' (2009) 1 *JILT* available at *https://warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/watney/watney.pdf*, accessed 27 July 2019.

Weber, AM 'The Council of Europe's Convention on Cybercrime' (2003) 18 *Berkley Technology Law Journal* 425-466.

Westin, AF 'Privacy and freedom' (1968) 25.1 *Washington Lee LR* 166.

Willassen, SY 'Hypothesis-based investigation of digital timestamps' 75 in I Ray and S Shenoi (eds) *Advances in Digital Forensics IV* (2008) Springerlink, New York available at *https://link.springer.com/book/10.1007/978-0-387-84927-0*, accessed 22 July 2019.

Witkowski, J 'Can juries really believe what they see? New foundational requirements for the authentication of digital images' (2002) 10 *Journal of L and Policy* 267.

Wu, H & G Zheng 'Electronic evidence in the blockchain era: New rules on authenticity and integrity' 36 (2020) 105401 *Computer Law & Security Review* 1.

Yar, M 'E-crime 2.0: the criminological landscape of social media' (2012) 21 *Information & Communications Technology Law* 207-219.

Reports / Internet references:

– amaBhungane Centre for Investigative Journalism case number 25979/17 'Notice of motion and founding affidavit' 11 April 2017 available at *https://www.dropbox.com/sh/w6y420sbgll850r/AADvfgsuv9Nda5Qoe9oJX5i6a?dl=0&preview=170411_amaB+notice+of+motion%2C+founding+affidavit.pdf*, accessed 19 June 2019.
– 'Apple v. FBI concerning an order requiring apple to create custom software to assist the FBI in hacking a seized iPhone' available at *https://epic.org/amicus/crypto/apple/*, accessed 8 April 2020.
– Department of the Prime Minister and Cabinet New Zealand 'Defining national security' (September 2017) available at *https://dpmc.govt.nz/sites/default/files/2017-09/fact-sheet-3-defining-national-security_1.pdf*, accessed 22 May 2019.
– Don't Spy on Us 'Don't spy on us: Reforming surveillance in the UK' (September 2014) available at *https://www.dontspyonus.org.uk/assets/files/pdfs/reports/DSOU_Reforming_surveillance.pdf*, accessed 08 August 2019.

- Don't Spy on Us: 'Response to the inquiries into privacy and surveillance' (September 2015) available at *https://www.dontspyonus.org.uk/assets/site/dontspyonus/files/DSOU_ Response_report_WEB.pdf*, accessed 23 February 2018.
- 'End-to-end encryption' available at *https://faq.whatsapp.com/en/android/28030015/*, accessed 13 July 2019.
- Facebook founder M Zuckerberg (2010) available at *https://www.theguardian.com/technology/2010/jan/11/facebook-privacy*, accessed 08 January 2017.
- Former Sun Microsystems CEO Scott McNealy (1999) available at *http://archive.wired.com/politics/law/news/1999/01/17538*, accessed 08 January 2017.
- *Google transparency report* available at *https://transparencyreport.google.com/https/overview?hl=en*, accessed 13 April 2020.
- 'Intelligence: Signals intelligence' available at *https://www.cia.gov/newsinformation/featured-story-archive/2010-featured-story-archive/intelligence-signals-intelligence1.html*, accessed 20 March 2020.
- 'Internet of babies – When baby monitors fail to be smart' (2018) available at *https://sec-consult.com/en/blog/2018/02/internet-of-babies-when-baby-monitors-fail-to-be-smart*, accessed 17 February 2020.
- 'Internet of Things (IoT) and AI self-driving cars' available at *https://www.aitrends.com/ai-insider/internet-of-things-iot-and-ai-self-driving-cars/*, accessed 17 February 2020.
- 'Internet of Things statistics 2020 [The rise of IoT]' available at *https://techjury.net/stats-about/internet-of-things-statistics/#gref*, accessed 17 February 2020.
- InterPARES project 'Requirements for assessing and maintaining the authenticity of electronic records' (2002) available at *http://www.interpares.org/book/interpares_ book _k_ app 02.pdf*, accessed 21 July 2019.
- JUSTICE *Investigatory Powers Bill 2016: Part 8 surveillance oversight briefing for House of Commons committee stage* (April 2016) available at *https://justice.org.uk/wp-content/uploads/2016/04/JUSTICE-Briefing-IP-Bill-HC-CS-Part-8.pdf*, accessed 25 March 2020.
- Liberty Liberty's response to the Home Office consultation *Protecting the public in a changing communications environment* available at *https://www.libertyhumanrights.org.uk/sites/default/files/liberty-s-communications-data-consultation-response.pdf*, accessed 4 July 2019.
- Liberty *Liberty's briefing on the Investigatory Powers Bill for report stage in the House of Commons* (June 2016) available at *https://www.libertyhumanrights.org.uk/sites/default/fil*

es/campaigns/resources/Liberty%27s%20Briefing%20on%20the%20Investigatory%20Powers%20Bill%20for%20Report%20Stage%20in%20the%20House%20of%20Commons.pdf, accessed 22 May 2019.

– Media Policy and Democracy Project 'The surveillance state: Communications surveillance and privacy in South Africa' (March 2016) available at *http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillancestate-web.pdf*, accessed 05 January 2017.
– *Managing discovery of electronic information: A pocket guide for judges* (2012) 2ed Federal Judicial Centre available at *https://www.fjc.gov/sites/default/files/2015/eldscpkt2d_eb_0.pdf*, accessed 02 August 2019.
– Necessary and Proportionate *International principles on the application of human rights law to communications surveillance: Background and supporting international legal analysis* at 19 available at *https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf*, accessed 29 March 2020.
– 'Number of monthly active Facebook users worldwide as of 1st quarter 2019 (in millions)' available at *https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/*, accessed 17 June 2019.
– 'Password recovery speeds: How long with your password stand up' (2016) available at *http://www.lockdown.co.uk/?pg=combi*, accessed 17 October 2016.
– Privacy International *Submission to the joint committee on the draft Investigatory Powers Bill* (21 December 2015) available at *https://privacyinternational.org/advocacy-briefing/720/privacy-international-submission-joint-committee-draft-investigatory-powers*, accessed 2 July 2019.
– Privacy International, Right2Know, and the Association for Progressive Communications 'Submission in advance of the consideration of the periodic report of South Africa, Human Rights Committee, 116th Session, 7-31 March 2016' (March 2016) available at *https://www.apc.org/en/pubs/submission-advance-consideration-periodic-report-s*, accessed 2 July 2019.
– 'Power of minister to appoint Rica judge in spotlight at ConCourt' (February 2020) available at *https://www.timeslive.co.za/news/south-africa/2020-02-25-power-of-minister-to-appoint-rica-judge-in-spotlight-at-concourt/*, accessed 29 March 2020.
– Press release 'AmaB challenges snooping law' (20 April 2017) available at *https://amabhungane.org/advocacy/advocacy-amab-challenges-snooping-law/*, accessed 19 June 2019.

– ‘Ramaphosa proposes a new deal for South Africa’ (November 2017) available at *https://www.fin24.com/Economy/ramaphosa-proposes-a-new-deal-for-south-africa-20171113*, accessed 25 February 2019.
– ‘Ramaphosa: My new deal for SA – and 10-point action plan for jobs, growth, transformation’ (November 2017) available at *https://www.biznews.com/thought-leaders/2017/11/14/ramaphosa-new-deal-for-sa/*, accessed 25 February 2019.
– Right2Know ‘Big Brother exposed: Stories of South Africa’s intelligence structures monitoring and harassing activist movements’ available at *https://www.r2k.org.za/category/publications/*, accessed February 2019.
– Right2Know ‘Stop the surveillance! Activist guide to RICA and state surveillance in SA’ available at *https://www.r2k.org.za/category/publications/*, accessed February 2019.
– Right2Know ‘The surveillance state: Communications surveillance and privacy in South Africa’ available at *https://www.r2k.org.za/category/publications/*, accessed February 2019.
– Right2Know ‘SPOOKED: Surveillance of journalists in SA’ (June 2018) *https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf.*, accessed 17 June 2019.
– Securing an open society: Canada’s national security policy (April 2004) available at *http://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf*, accessed 22 May 2019.
– ‘Signals intelligence’ available at *https://www.globalsecurity.org/intell/library/policy/army/fm/2-0/chap8.htm*, accessed 20 March 2020.
– ‘Some notes on big numbers’ *http://www.quadibloc.com/math/bignum.htm*, accessed 17 October 2016.
– ‘South African population 2019’ available at *https://www.worldometers.info/world-population/south-africa-population/*, accessed 9 July 2019.
– South Africa's written responses to the UN Human Rights Committee following South Africa's review ref 50/2016 (10 March 2016) available at *https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/ZAF/INT_CCPR_AIS_ZAF_23518_E.pdf*, accessed 2 April 2020.
– Top court questions surveillance laws’ (February 2020) available at *https://mg.co.za/article/ 2020-02-28-top-court-questions-surveillance-laws/*, accessed 29 March 2020.
– ‘World Internet user and 2019 population statistics’ available at *https://www.internetworldstats.com/stats.htm*, accessed 17 June 2019.

– 'Youtube statistics' *https://www.youtube.com/yt/press/statistics.html*, accessed 17 June 2019.

South African Law Reform Commission Papers

South African Law Commission (Project 6) Review of the Law of Evidence Report *Admissibility in civil proceedings of evidence generated by computers* (1982).

South African Law Commission (Project 95) Working Paper 60 *Investigation into the Computer Evidence Act 56 of 1983* (1985).

South African Law Commission Discussion Paper 99 (Project 108) *Review of the law of evidence* (1986).

South African Law Commission Issue paper 14 (Project 108) *Computer related crime: Options for reform in respect of unauthorised access to computers, unauthorised modification of computer data, and software applications, related to procedural aspects* (1998).

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

South African Law Commission Discussion Paper 113 (Project 126) *Review of the law of evidence – Hearsay and relevance* (2008).

South African Law Commission Issue Paper 26 (Project 126) *General overview of the rules of evidence and possible areas of reform* (2008).

South African Law Commission Issue Paper 26 (Project 126) *Electronic evidence in criminal and civil proceedings: Admissibility and related issues* (2010).

South African Law Commission Discussion Paper 131 (Project 126) *The review of the law of evidence* (2015).

South Africa – Commissions of Enquiry

Office of the Inspector-General of Intelligence 'Executive summary of the final report on the findings of an investigation into the legality of the surveillance operations carried out by the NIA on Mr S Macozoma. Extended terms of reference report on the authenticity of the allegedly intercepted e-mails', media briefing, 23 March 2006, available at *www.intelligence.gov.za/OversightControl/IG%20Exec%20Summary%2023%20Mar% 2006.doc*, accessed 05 January 2016.

Ministerial Review Commission 'Intelligence in a constitutional democracy 10 September 2008' Final report to the Minster for Intelligence Services, the Honourable Mr Ronnie Kasrils MP available at *http://www.lse.ac.uk/international-development/Assets/Documents/PDFs/csrc-background-papers/Intelligence-In-a-Constitutional-Democracy.pdf*, accessed 05 January 2016.

The European Commission

European Commission *Proposal for a regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters* Strasbourg, 17.4.2018 COM(2018) 225 final available at *https://eclan.eu/files/attachments/.2504/L_Proposal_Regulation_e_evidence_2018.pdf*, accessed 20 April 2020.

United Kingdom / Home Office / Parliamentary Reviews

Anderson, D QC *A question of trust: Report of the investigatory powers review* (2015) Independent Reviewer of Terrorism Legislation available at *www.gov.uk/government/publications*, accessed on 17 May 2016.

Anderson, D QC 'Statement by the Independent Reviewer of terrorism legislation on publication of the report of the investigatory powers review (A question of trust)' (2015) available at *https://terrorismlegislationrevi ewer.independent.gov.uk/w…/IPR-Press-Release.docx*, accessed on 20 May 2016.

Home Office 'Interception of communications in the United Kingdom: A consultation paper' (Cm 4368, 1999).

Home Office 'Guidance Investigatory Powers Bill: Overarching documents' (2015) available at *https://www.gov.uk/government/publications/draft-investigatory-powers-bill-overarching-documents*, accessed 17 May 2016.

Home Office Gov.UK 'Fact sheets and guidance relating to the Investigatory Powers Bill' 4 March 2016 available at *https://www.gov.uk/government/publications/investigatory-powers-bill-fact-sheets*, accessed 21 June 2019.

Home Office Gov.UK 'Fact sheet: equipment interference' 4 March 2016 available at *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/530554/Equipment_Interference_Factsheet.pdf*, accessed 21 June 2019.

Home Office Gov.UK 'Investigatory Powers Bill: Bulk powers' 4 March 2016 available at *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/530549/Bulk_Powers_Factsheet.pdf*, accessed 21 June 2019.

Intelligence and Security Committee of Parliament *Privacy and security: A modern and transparent legal framework* (12 March 2015) available at *https://www.pdpjournals.com/docs/88433.pdf*, accessed 08 August 2019.

Joint Committee on the draft Investigatory Powers Bill Report Draft Investigatory Powers Bill (11 February 2016) available at *https://publications.parliament.uk/pa/jt 201516/jtselect/jtinvpowers/93/93.pdf*, accessed 22 May 2016.

Royal United Services Institute for Defence and Security Studies *A democratic license to operate: Report of the independent surveillance review* (July 2015) *available at https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf*, accessed January 2018.

The United Nations

United Nations Siracusa Principles on the limitation and derogation of provisions in the International Covenant on Civil and Political Rights Annex, UN Doc E/CN.4/1984/4 (1984) available at *https://www.uio.no/studier/emner/jus/humanrights/HUMR5503/h09/undervisningsmateriale/SiracusaPrinciples.pdf*, accessed 22 May 2019.

United Nations Human Rights Committee General Comment No. 27 (1999) CCPR/C/21/Rev.1/Add.9, reproduced in Human Rights Instruments (2008) *Compilation of general comments and general recommendations adopted by Human Rights Treaty Bodies* HRI/GEN/1/Rev.9 (Vol. I).

United Nations Human Rights Council 'The right to privacy in the digital age' A/HRC/27/37 (30 June 2014) available at *http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf*, accessed 04 January 2016.

United Nations Human Rights Council 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank LaRue' A/HRC/23/40 (17 April 2013) available at *https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf*, accessed 4 July 2019.

United Nations Human Rights Committee 'Concluding observations on the initial report of South Africa' CCPR/C/ZAF/CO/1 (27 April 2016) available at *http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2FZAF%2FCO%2F1&Lang=en*, accessed 29 February 2018.

United Nations Educational, Scientific and Cultural Organization *Protecting journalism sources in the digital age* (2017) available at *http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/protecting_journalism_sources_in_digital_age.pdf*, accessed 30 June 2020.

INTRODUCTION

I RESEARCH QUESTION

The research question central to the thesis is stated as follows: what are the implications of new technological phenomena in South African law and its challenges to the existing legal frameworks in relation to investigatory powers of law enforcement and security and intelligence agencies to obtain electronic evidence, and its subsequent admissibility in criminal proceedings? The thesis seeks to investigate how our existing legal frameworks which regulate the use of and access to electronic evidence in criminal proceedings, including its admissibility, integrate and adapt to challenges raised by new and rapidly changing technological developments.

Written with an emphasis on South African law, but also considering certain jurisdictional aspects of international law, the thesis follows the temporal development of an investigation initiated by a suspicion of criminal activity, followed by an investigation, and thereafter by presentation of evidence at trial. Each chapter focuses on a type of investigative power: the investigative power is discussed critically to ascertain whether the law has developed appropriately to advancements in technology or in ways that are cause for concern. The thesis considers the challenges of continued technological advancements and complexity of electronic evidence by concentrating on certain key investigative powers of law enforcement and the security and intelligence agencies to obtain such evidence, whether obtained from third party telecommunication service providers, or from the victim or suspect/target of an investigation.

Following the investigation, and having obtained what appears to be prima facie evidence of criminal activity, the next stage is prosecution and the process of presenting evidence to a court. Evidential issues have been central to many of the debates about the nature and medium of the evidence being presented. The most interesting perhaps is that of evidential exclusions, and the extent to which the nature of the evidence presented, in this instance electronic evidence, impacts on admissibility in criminal proceedings. Complex admissibility rules of evidence have historically existed to govern evidential exclusions, which may occur due to statutory provisions, through judicial determination in case law or through a combination based on statute and case law. In this regard, two separate issues are the focus of research interest: (a) admissibility of electronic evidence and (b) its weight.

A consideration and analysis of these issues could be taken further in terms of understanding what the law could be. Introducing new laws, or amending existing ones, will only work to a certain extent. In the end, the law needs to be enforced in a modern fast-paced environment of technological advancements where, arguably, almost any criminal activity perpetrated today has an electronic element to it. In the final analysis, the thesis considers appropriate and meaningful reform towards a modern and transparent legal framework in South African law.

II THE CHALLENGES OF REGULATING INVESTIGATORY POWERS AND ELECTRONIC EVIDENCE IN AN ERA OF EVOLVING TECHNOLOGICAL PHENOMENA

The last two decades have witnessed rapid developments in technology resulting in extraordinary changes to the physical nature of computers, introduction of smart devices and mobile technology, including the proliferation of a modern global communications system, a range of applications and networked technology. Advancements in technology have revolutionised society and its ability to send, receive and now routinely store information in mostly electronic form. [1] These technological developments have also created new opportunities for crime. Perpetrators are increasingly using sophisticated techniques to evade detection and perpetrate serious and organised crime. Many of the features of modern technology such as low cost, ease of use and the potential of anonymity and pseudonymous activity make new technologies an appealing medium for committing and facilitating crime. With the use of technology in criminal activity, obtaining electronic evidence that can reside almost anywhere of criminal conduct poses different challenges and investigatory concerns when compared to obtaining conventional physical evidence.

The ability of law enforcement and security and intelligence agencies to make progress in investigations in an increasingly internet-based communications environment raises concerns about the erosion of their capabilities by technological change.[2] 'We have to

[1] See F Cairncross *The Death of Distance: How the Communications Revolution will Change our Lives* (1997) and the author's revised and updated version, *The Death of Distance: How the Communications Revolution is Changing our Lives* (2001) wherein '[t]he death of distance' we are told 'will probably be the single most important force in shaping society in the first half of the next century'.

[2] Home Office 'Guidance Investigatory Powers Bill: Overarching documents' (2015) available at *https://www.gov.uk/government/publications/draft-investigatory-powers-bill-overarching-documents*, accessed 17 May 2016.

enter the labyrinth to find them'[3] has been quoted in reference to categories of websites, in particular the 'dark net' which offers sophisticated systems of anonymity beyond the reach of law enforcement:

> '[I]t is quite clear that we have a pressing and, indeed, rising challenge to deal with highly encrypted communications online that are managed through the space of the darknet, which are effectively out of the reach of law enforcement authorities – not in every case, but in an increasing proportion of those cases. It is fair to say that the scope that the police have to monitor communications in the offline world is greater than it is in the online world. Given that a majority of those communications run by these networks are moving online, there is a security gap there. To what extent it should be plugged by the right and balanced legislation is for others to judge but I do think it is one of the most pressing problems that police face across Europe.'[4]

In the era of the information age and a modern fast-paced environment of technological advancements, the nature of criminal threats evolves. This presents new challenges in respect of an appropriate balance between the needs of law enforcement and security and intelligence agencies in the disruption, detection and investigation of criminal activity and rights of individuals.[5] Investigative tools and techniques have to be adapted to keep pace with technology in combatting these criminal threats. The exercise of investigative powers by law enforcement and the state and security agencies are by their very nature intrusive, and interfere with the rights of individuals, whether third parties such as telecommunication service providers, or the suspect/target of an investigation. Any disproportionate, or unfettered, use of such investigative powers can have consequences for individual rights.[6] Invoking May's cypherpunk manifesto of imagery of Internet criminals as the 'four horseman of the apocalypse: drug-dealers, organised crime, terrorists and paedophiles'[7] this thesis provides a critical analysis of existing legal frameworks regulating the investigative powers of law enforcement and security and intelligence agencies in the current modern environment of the information age in which they operate:

---

[3] Attributed to Sir Ian Lobban, then Director of the GCHQ quoted in D Anderson QC *A question of trust: Report of the Investigative Powers Review* (2015) Independent Reviewer of Terrorism Legislation at 48 available at *www.gov.uk/government/publications*, accessed 17 May 2016.
[4] Attributed to R Wainwright, then Director of Europol, quoted in Anderson op cit note 3 at 48.
[5] I Walden *Computer Crimes and Digital Investigations* (2007) at 204.
[6] United Kingdom *Interception of communications in the United Kingdom: A consultation paper* (Cm 4368, 1999) 1.
[7] TC May 'The cyphernomicon' (1994) 8.3.4 available at *https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ*, accessed on 20 May 2016.

> 'Modern communications networks can be used by the unscrupulous for purposes ranging from cyber-attack, terrorism and espionage to fraud, kidnap and child sexual exploitation. A successful response to these threats depends on entrusting public bodies with the powers they need to identify and follow suspects in a borderless online world. But trust requires verification. Each intrusive power must be shown to be necessary, clearly spelled out in law, limited in accordance with international human rights standards and subject to demanding and visible safeguards.'[8]

As new technologies and new capabilities become more prevalent in the information age, new opportunities exist for these new technologies to be exploited by criminal elements. One result of this is that the investigation of many traditional (offline) criminal offences will now involve electronic evidence.[9] This thesis is not about cybercrime offences, now increasingly recognised as a distinct branch of criminal law.[10] The issues of criminal procedure and evidence examined in this thesis are not limited to cybercrimes, but are relevant to almost any type of criminal activity. A number of academic texts have explored core concepts of cybercrime and the numerous ways in which criminal activity could be facilitated by technology.[11] While this is not the place for identifying cybercrimes, albeit a phenomenon that is not easy to define, or for adopting a classification that appropriately determines when a crime is or is not a cybercrime, it is a necessary and useful starting point. Key in the analysis of the core concepts of cybercrimes is the recognition that many cybercrimes are arguably traditional crimes, whereby technology facilitates or is an incidental aspect of the principal traditional crime but in a way that technology may afford evidence of it.[12] In the modern environment of technological advancements that have revolutionised mobile and communication technologies, arguably almost any criminal activity perpetrated has an electronic element to it.[13] Therefore, whilst the principal crime may not be a

[8] D Anderson 'Statement by the independent reviewer of terrorism legislation on publication of the report of the Investigatory Powers Review (A question of trust)' (2015) available at *https://terrorismlegislationreviewer.independent.gov.uk/wp…/IPR-Press-Release.docx*, accessed on 20 May 2016.
[9] AA Gillespie *Cybercrime: Key Issue and Debates* (2019) at 333.
[10] Ibid at vii.
[11] Ibid at 13. See M Wasik *Crime and the Computer* (1991); B Sandywell 'On globalisation of crime: the internet and new criminality' in Y Jewkes & M Yar *Handbook in Internet Crime* (2010) 38-66; D Wall 'Cybercrimes and the Internet' in D Wall (ed) *Crime and the Internet* (2001) 3-7; M Yar 'E-crime 2.0: The criminological landscape of social media' (2012) 21 *Information & Communications Technology Law* 207-219, AM Weber 'The Council of Europe's Convention on Cybercrime' (2003) 18 *Berkley Technology Law Journal* 425-466.
[12] Gillespie op cite note 9 at 9-13. See also J Clough 'Cybercrime' (2011) 37 *Commonwealth Legal Bulletin* 671 at 672.
[13] Ibid.

cybercrime per se, it is likely that most investigations in the information age will involve having access to electronic evidence in what would appear to be 'traditional crimes'.

In the last decade, communications technology have undergone significant advancements and continues to evolve at an unprecedented level. Evolving communications technology is now central to the way we interact, both socially and commercially. Communications technologies, such as the Internet, mobile smartphones and WiFi enabled devices, have become part of daily life with major developments including wireless email, instant messaging and social networking as central modes of communication. Such developments also brings together various and different forms of communication (mobile calls, emails, internet, instant messaging, social media access, banking, shopping, and so forth) to a single device 'that is both mobile and Internet enabled.'[14] There are now in excess of one trillion websites providing instantaneous access to a diverse range of information and services, with more than 4.54 billion Internet users as of January 2020.[15] With almost 2.5 billion monthly active users as of the fourth quarter of 2019, Facebook is the biggest social network worldwide.[16] The video-sharing platform YouTube is just as impressive: 'over 2 billion logged-in users visit YouTube each month and daily users watch over a billion hours of video and generate billions of views.'[17] The extent of content generated is unprecedented in terms of the degree of detailed information that can be gathered and stored. With almost real-time access to information and communications providing instant and 'now' means of interaction,[18] innovations in communications technology is such that modern life is portrayed increasingly online, as the Internet has become both pervasive and increasingly intimate of peoples' lives.[19]

This thesis is deliberately titled 'electronic evidence'. It is necessary to understand the context of the term. When criminal activity is perpetrated, the ability of law enforcement and the state and security agencies to prosecute those involved is guided, to an extent, by the

[14] Media Policy and Democracy Project *The surveillance state: Communications surveillance and privacy in South Africa* (March 2016) available at *http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillancestate-web.pdf*, accessed 05 January 2017.
[15] 'Global digital population as of January 2020' available at *https://www.statista.com/statistics/617136/digital-population-worldwide/*, accessed 11 March 2020.
[16] 'Number of monthly active Facebook users worldwide as of 4th quarter 2019 (in millions)' available at *https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/*, accessed 11 March 2020.
[17] Available at *https://www.youtube.com/yt/press/statistics.html*, accessed 11 March 2020.
[18] T Pistorius 'Monitoring, interception and big boss in the workplace: is the devil in the details?' (2009) 12.1 PER available at *http://www.saflii.org/za/journals/PER/2009/1.html*, accessed 05 January 2017.
[19] Human Rights Council 'The right to privacy in the digital age' A/HRC/27/37 (30 June 2014) available at *http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf*, accessed 04 January 2016.

availability and access to information across a range of contexts, including, the gathering of intelligence, access to obtaining evidence, analysis thereof and subsequent presentation in criminal proceedings.[20] In the investigation process, particular techniques, or use of investigative powers, at different stages in an investigation are generally subdivide into covert (interception and surveillance) or coercive techniques (search and seizure).[21] New and evolving technologies, whether through latest devices or software applications, are capable of creating a trail of electronic evidence that can originate from a variety of sources and geographies. In the event of a criminal investigation, devices and information will need to be accessed and examined. In recent times as ease of Internet connectivity and mobile technologies came to prominence, it was realised that the information accompanying a communication between individuals could be useful to identify persons of interest to be placed under surveillance, or to establish evidential relationships between persons of interest.[22] For example:

> A robbery was perpetrated at the premises of Company X and items of considerable value were stolen. For the purposes of the investigation that is to take place, the disclosure of the information sought, in this instance information from cell towers servicing the area in which the premises is located, may well provide identifying markers or particulars of persons of interest. These include call/messaging information (date, duration and time of all calls or messages made and received) or geolocation information of the device when it was used (by analysing their logs and using triangulation techniques to determine the general location of the device at the time of a call/message) or internet browsing information for a particular device. An examination of this information identifies C and D as suspects/target of the investigation. C and D deny knowing each other and being involved in the robbery. Analysis of information from the cell towers triangulate C and D's location together to early hours of the morning in the vicinity of where the robbery took place, and also reveal that a history of calls/messaging between them.[23]

It is possible to identify some characteristics of electronic evidence and, in particular, the challenges it can pose to the law: (a) *scale*—potential number of victims and suspects/target of an investigation is huge; (b) *quantity*—a particular issue with electronic evidence is volume and likelihood that most individuals use more than one device, with personal storage devices in the terabytes now being considered commonplace;

[20] See Walden op cite note 5 at 203-295.
[21] Ibid at 203-04.
[22] Gillespie op cite note 9 at 337.
[23] Based on *Nampak (Pty) Ltd v Vodacom (Pty) Ltd and Others* 2019 (1) SA 257 (GJ).

(c) *anonymity*—referred to as the 'identity' problem such that anonymous or undetectable communications are becoming more widespread; (d) *accessibility*—technology is making it more difficult to locate the evidence because of the use of encryption/password systems; (e) *deletion and destruction*—electronic information and data is extremely volatile and susceptible to claims to fabrication and manipulation.[24]

In South Africa, legislation governing the use of investigative powers by law enforcement, including security and intelligence agencies, is covered by a number of statutes, key among them is the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.[25] A central premise of the thesis is that evolving technological phenomena can and do present challenges to existing legal concepts on evidence and the powers of law enforcement and the security and intelligence agencies to obtain electronic evidence and its admissibility in criminal proceedings. This is done in the context of understanding whether South African law has developed appropriately in response to advancements in technology.

As to matters of evidence, courts are increasingly presented with evidence that originates from a variety of sources which raises a number of evidential concerns. A particular challenge facing proponents of electronic evidence in court proceedings, as often referenced by the South African courts, relate to concerns with electronic evidence by virtue of the nature of its medium. This is primarily due to the intangible and often transient nature of electronic data, where such data can be created, stored, copied and transmitted with relative ease. It can also be easily modified or tampered without obvious signs of changes made, thereby rendering the process of investigation and recording of evidence extremely vulnerable to claims of errors, accidental alteration, prejudicial interference or fabrication.[26] In *S v Ndiki and Others*, [27] a case that involved admissibility of computer generated printouts, it was stated: 'Finally, in dealing with computer evidence it must be recognised that computers are not infallible and that the dangers inherent in this type of evidence must be acknowledged and the necessary safeguards put in place.' [28] Many of the earlier held

[24] Gillespie op cit note 9 at 14 and 333-35.
[25] Hereafter 'RICA 2002'.
[26] C Tapper 'Evanescent evidence' (1993) 1.1 *International Journal of Law and Information Technology* 35; I Walden 'Computer crime' in C Reed & J Angel (eds) *Computer Law* 5ed (2003) at 295.
[27] 2008 (2) SACR 252 (Ck).
[28] Supra note 27 at 270.

assumptions that a computer is just like a 'compact filing cabinet' or that electronic documents are just like the paper equivalent no longer hold true.[29]

The admissibility of electronic evidence in criminal proceedings is regulated by the provisions of various sources of law, including the Electronic Communications and Transactions Act 25 of 2002,[30] the Criminal Procedure Act 51 of 1977 and the common law. The desirability of the current legal framework in this regard has raised a number of admissibility issues in relation to hearsay and authenticity.[31] Indeed, on matters of evidence and challenges to the admissibility of electronic evidence, should such evidence be exempt from the evidential rules regulating hearsay? Having regard to the nature and characteristics of electronic evidence, including legitimate concerns about its reliability and authenticity, should stricter standards for admissibility, generally, and in the context of evidential weight, apply to electronic evidence as a 'new species of evidence' with a whole new body of evidence law specific to its use?

III THESIS STRUCTURE

The thesis is divided into five main chapters, and the content of each is briefly set out below. Chapter one will place the rest of the thesis into context. In doing so it considers what is meant by the information age and a modern fast-paced environment of technological advancements referred to throughout the thesis and as the setting in which the law operates. Part II introduces the information age and examples in recent advancements in technology that underlie key debates on legislative reform considered in the thesis. Part III presents perspectives on the right to privacy in the information age. Part IV briefly introduces key legislation which will be considered in this thesis, namely RICA 2002 and the ECT Act 25 of 2002 and the issues informing the analysis.

The thesis seeks to understand the implications of new technology and new capabilities in the information age in the context of the investigative powers of law enforcement and the state and security agencies. Chapters 2, 3 and 4 examine the regulatory framework governing the processes for obtaining electronic evidence in criminal

[29] P Sommer 'Computer forensics: An introduction' available at *http://www.virtualcity.co.uk/vcaforens.htm* at 62, accessed on 16 May 2016.
[30] Hereafter 'ECT Act 2002'.
[31] *S v Harper* 1981(1) SA 88 (D); *S v De Villiers* 1993 (1) SACR 574 (Nm); *S v Mashiyi and Another* 2002 (2) SACR 387 (Tk); *Ndlovu v Minister of Correctional Service and Another* [2006] 4 All SA 165 (W); *S v Ndiki and Others* 2008 (2) SACR 252 (Ck).

investigations. They generally divide into three mechanisms: (a) interception of communications; (b) obtaining evidence from third party telecommunication service providers; and (c) obtaining evidence from a suspect/target of an investigation. Each mechanism is governed by legal frameworks that present unique issues to evolving technological phenomena. Understandably, the issues discussed in chapters 2,3 and 4 can overlap. A key argument in the analysis of these mechanisms for obtaining electronic evidence in criminal proceedings is that, despite widespread innovations in policy and technology globally, South African domestic legislation remains out-dated, especially its safeguards as 'technological innovations makes even more new and diverse forms of communication surveillance possible.'[32]

Chapter two is about interception of communications. After the Part 1 introduction, the chapter will explore, in Part II, the legal framework for interception in RICA 2000 including circumstances in which lawful interception can take place, authorisation procedures and the protection of privacy interests through prohibiting unlawful interceptions. Part III deals with existing challenges in the legal framework of RICA 2002. The key challenges identified are twofold: (a) the scope and breadth of investigative powers by law enforcement and the security and intelligence agencies; being (b) unconstrained by out-dated legislative frameworks that have expanded the scope of their activities and the extent of their capabilities in an information age of innovations in technology. The RICA 2002 has been the subject of legal challenge and Part IV considers the future of interception of communications in South Africa. A conclusion is drawn in Part V.

Chapter three is about communications data. Part II begins with an analysis of the obligations of telecommunication service providers in RICA 2002 with regard to mandatory data retention. This is followed by an examination of the investigatory powers of law enforcement and security and intelligence agencies to acquire communications data. The key issues identified relate to the process of authorising the acquisition of communications data, procedures in RICA 2002 for storing, accessing, examining, using and destroying the communications data. Completing the analysis is a consideration of s 205 of the Criminal Procedure Act 25 of 1977 as a parallel process for law enforcement and security and intelligence agencies to obtain communications data from third party telecommunication service providers. Part III concludes the chapter.

[32] Walden op cite note 5 at 179.

Chapter four is about compelled decryption. Part II is an overview of the powers of law enforcement and security and intelligence agencies to compel decryption. RICA 2002 compels (a) disclosure of the decryption key; or (b) provision of decryption assistance to obtain access to the encrypted information or to put that encrypted information in an intelligible form. Part III considers certain legal issues that may arise in relation to compelled decryption. These powers anticipate, at the very least, that the potential disclosure of information may incriminate the suspect/target to whom a compelled decryption order is directed. Applying the constitutional law framework on the right against self-incrimination, two distinct issues arise with regard to compelled disclosure and modern technology: (a) compelled disclosure of a user's passcode (reveal/enter the passcode); and (b) compelled entry of a biometric based information (by placing a finger on a device or by facial recognition). In the analysis, a nuanced understanding of the interaction between modern technology and legal doctrine will be integral in the development of doctrinal principles that involve 'reveal-the-passcode', 'use-a-fingerprint-or-facial-recognition', 'enter-the-passcode' or 'produce-the- decrypted-data' scenarios. Part IV considers the development of a doctrinal approach in South African law. Part V is the conclusion.

Chapter five shifts focus to the evidentiary aspects in relation to the admissibility of electronic evidence. The introduction of electronic evidence in criminal legal proceedings raises unique challenges in the South African law on evidence. This chapter identifies two separate issues in this regard: (i) admissibility of electronic evidence and (ii) its weight. In doing so an analysis of relevant provisions the ECT Act 25 2002 are considered. Part II is about the ECT Act 2002 and its provisions on admissibility and evidential weight of electronic evidence. Part III considers electronic evidence in the context of the exclusionary rule on hearsay and real evidence. Part IV considers the evidential weight of electronic evidence and new rules on the business records exception, including authenticity and integrity. Part V completes the chapter with concluding remarks on rethinking admissibility and evidential weight of electronic evidence in the information era.

In the final analysis, the conclusion chapter of the thesis considers appropriate and significant proposals for change towards a modern and transparent legal framework in South African law. In doing so, it is hoped that my contribution to the legal landscape and debates about far-reaching and long term developments in the law of criminal procedure and evidence in the outcomes of the thesis research, is a better understanding of the challenges and

complexities of regulating investigatory powers and electronic evidence in an era of evolving technological phenomena.

IV RESEARCH METHODOLOGY

In terms of methodology, the thesis is primarily concerned with the law of criminal evidence and procedure in South Africa from a theoretical perspective. While it is beyond the scope of the thesis to conduct a comprehensive comparative study of electronic evidence in criminal proceedings and subsidiary research areas, reference will be made to other jurisdictions where relevant to the analysis undertaken, either as a basis for critically assessing the approach in South African law or as a starting point for discussion on issues where South African law has yet to develop. Various legal sources will be used to critically consider the South African position including, case law, books, journal articles, white papers, legislation, and the common law. Where applicable, the thesis shall refer to comparative jurisprudence, to draw on key lessons, especially where such jurisprudence demonstrates a very different approach to the position in South Africa law.

CHAPTER ONE

THE WORLD IN AN INFORMATION AGE

I INTRODUCTION

This chapter will place the rest of the thesis into context. It is necessary to consider what is meant by the information age and a modern fast-paced environment of technological advancements referred to throughout the thesis, and as the setting in which the law operates. Part II introduces the information age and provides examples of recent advancements in technology that underlie key debates on legislative reform considered in the thesis. Part III presents perspectives on the right to privacy in the information age. Part IV briefly introduces key legislation which will be considered in this thesis, namely the: (a) Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, and (b) Electronic Communications and Transactions Act 25 of 2002.

II THE INFORMATION AGE

(a) New technology, new capabilities: connectivity, devices and data

We live in the information age.[1] This refers to a period in human history beginning in the 20th century characterised by the rapid shift from traditional industrial production to one primarily based upon information technology, computerisation and an era marked by rapid adoption of new technologies.[2] A recently expressed view is that when the history of the information age is written, 2019 will be heralded as a 'landmark year where innovation was rife.'[3] This is undoubtedly true. The world as we live in has experienced in recent years new technologies from artificial intelligence (AI) and machine learning to blockchain and the Internet of Things (IoT). New digital technologies are having a major impact on our lives and transforming the way we live and work – and that impact will only grow in 2020 and beyond. After all, new technology, albeit in different forms, have preceded almost every generation just 'as the

[1] Also known as the 'computer age', 'digital age' or 'new media age'.
[2] See 'Information age' available at *https://en.wikipedia.org/wiki/Information_Age*, accessed 17 February 2020.
[3] 'The top five trends for digital transformation in 2020' available at *https://www.information-age.com/top-5-trends-digital-transformation-2020-123469909/*, accessed 17 February 2020.

telegraph gave way to the telephone, the stagecoach gave way to the automobile, and the typewriter gave way to the wordprocessor.'[4]

A significant example of the result of a combination of continued advanced technologies in the information age is IoT. In its simplest sense, IoT is a concept that is about *connectivity, devices and data*. IoT refers to a system of interrelated computing devices connecting to the Internet, with the ability to gather and share information without human-computer intervention. The combination of technologies that IoT contains and make it work is often referred to as 'smart' technologies. These smart technologies include new platforms such as advanced analytics, 5G networks, sensor tech devices and edge computing. Examples of IoT in the form of sensor tech devices (smart devices) range from the simplest consumer centric to industrial based devices that provide (a) real-time insights and the ability to store reams of data that is being recorded, and (b) the ability to efficiently and quickly process that stored data in order to create actionable insights out of it. Common examples of IoT technology for the consumer include smart speakers, the most popular of which is the Amazon Alexa[5] capable of home automation (lighting/heating controls), voice interaction, ordering take-out food, streaming services, delivering messages and making calls, playing audiobooks, and providing real-time information such as weather, traffic news and sports. A popular IoT technology in the midst of energy challenges resulting in almost daily electricity blackouts in South Africa, is the smart sense energy monitor.[6] The device provides in-depth insight into how energy is being used in a home, automatically tracks electricity usage and lets the user know which appliances are hogging up power.

IoT and connectivity are growing rapidly. Statistics reveal that there are 26.6 billion IoT devices in the world as at August 2019, and there are expected to be over 65 billion IoT devices worldwide by 2025, with consumers now connected more than ever, such that 127 IoT devices connect to the Internet every second.[7] A perusal of IoT technology on the market now makes the most mundane of home chores exciting and automated. In the year 2020 information age, advanced applications IoT technology are being tested in the automotive industry and are

[4] F Galves 'Where the not-so-wild things are: Computers in the courtroom – The Federal Rules of Evidence and the need for institutional reform and more judicial acceptance' (2000) 12 *Harvard JL Technology* 165 at 300.
[5] Available at *https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b?ie=UTF8&node=9818047011*, accessed 17 February 2020.
[6] Available at *https://www.amazon.com/Sense-Energy-Monitor-Electricity-Usage/dp/B075K6PHJ9*, accessed 17 February 2020.
[7] 'Internet of Things statistics 2020 [The rise of IoT] available at *https://techjury.net/stats-about/internet-of-things-statistics/#gref*, accessed 17 February 2020.

likely to soon lead us into the future of automatous driving in the form of fully capable, IoT-intelligent self-driving autonomous cars.[8]

Technology promises an exciting journey in the information age. Are there any serious concerns? There are security and privacy challenges and concerns about how potential vulnerabilities might allow cybercrime to take place. If no security, such as anti-hacking software, was applied in the design stage of IoT devices could these devices be hacked and used to facilitate criminal activity? Potentially, yes. Arguably IoT technology could provide greater opportunities for technology facilitated criminal activity.[9] Dunlap suggests that hackers actively exploit weaknesses in IoT security not to attack the devices themselves, but as an entry point to a network for all kinds of malicious behaviour, such as distributed denial-of-service attacks, malware distribution, spamming and phishing, click fraud, and credit card information theft.[10] IoT technology can potentially be used to perpetrate more traditional (offline) offences, such as robbery or burglary. Examples relate to smart surveillance devices or smart automation technology popular in many homes. Smart thermostats (for controlling heat/cooling and automatically turn off when occupants are away), smart baby monitors[11] and smart wireless cameras, which if hacked could potentially reveal occupant movements, allowing perpetrators to watch for when a house is empty and the opportunity to burgle the premises. It is clear that as the IoT ecosystem expands, new levels of security and privacy provisions will be needed.

(b) Evolving methods of communication

A particular issue with electronic evidence in the information age is the sheer volume of electronic information and data. The information age quite literally is about 'information' in the form of zeros and ones, which has 'become a commodity that is quickly and widely disseminated and easily available especially through the use of computer technology.'[12] In the information age, the growth of wireless connectivity, communication and mobile technologies have revolutionised the way to connect to the Internet, with an almost instantaneous ability to

[8] 'Internet of Things (IoT) and AI self-driving cars' available at *https://www.aitrends.com/ai-insider/internet-of-things-iot-and-ai-self-driving-cars/*, accessed 17 February 2020.
[9] AA Gillespie *Cybercrime: Key issues and debates* (2019) at 8.
[10] T Dunlap 'Unsecured IoT: 8 ways hackers exploit firmware vulnerabilities' (2019) available at *https://www.darkreading.com/risk/unsecured-iot-8-ways-hackers-exploit-firmware-vulnerabilities/a/d-id/1335564*, accessed 17 February 2020.
[11] 'Internet of babies–When baby monitors fail to be smart' (2018) available at *https://sec-consult.com/en/blog/2018/02/ internet-of-babies-when-baby-monitors-fail-to-be-smart*, accessed 17 February 2020.
[12] Available at *https://www.merriam-webster.com/dictionary/Information%20Age*, accessed 17 February 2020.

send, receive and now routinely store information in mostly electronic form. Mobile technology and associated devices have evolved as rapidly as computers in the last two decades. In today's information age, mobile phones, now often referred to as smart phones, no longer lead with their traditional feature of being able make/receive telephone calls with short message services. With the development of touch screen technology, mobile technologies have revolutionised connectivity and communication. Mobile technology now means the ability to access the Internet, almost anywhere, and in public places such as malls, airports, and hotels. Mobile phone contracts by telecommunication service providers are now dominated, not by call minutes and short message service (SMS) bundles, but by data bundles and smart phone devices where for many the ability to make/receive telephone calls is perhaps one of the least used functions of the device.[13] User interaction is now predominantly through software applications and social media platforms. In the year 2020 information age, the landline telephone has given way to smartphone devices, postal letters to email communications, instant messaging, video calls and social networking sites. Voice calls and traditional methods of SMS texts have now been overtaken by instant messaging applications, social network communication, all of which allow both voice and video calls.

In terms of a recent compilation of the latest global social media statistics of consumer adoption and usage in 2019, the number of internet users worldwide in 2019 was 4.388 billion, the number of social media users worldwide in 2019 was 3.484 billion, the number of mobile phone users in 2019 was 5.112 billion.[14] Similarly for instant messaging applications, there are 1.6 billion active users, 'WhatsApp' is number one among instant messaging applications, followed closely by 'Facebook Messenger' with 1.3 billion users and the Chinese instant messaging application 'WeChat' with 1.1 billion users. This is followed by 'Instagram' with one billion users and the Chinese 'QQ' with over 800 million active users.[15] Many of these applications are accessed through smartphone devices, which as standalone devices are also capable of providing detailed information on user movements and geographic locations:

> 'Mobile application software on a cell phone, or "apps," offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for

[13] Gillespie op cit note 9 at 4-6.
[14] D Chaffey 'Global social media research summary 2019' available at *https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/*, accessed 04 August 2019.
[15] B Bucher 'WhatsApp, WeChat and Facebook messenger apps – Global messenger usage, penetration and statistics' available at *https://www.messengerpeople.com/global-messenger-usage-statistics/*, accessed 04 August 2019.

> sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase "there's an app for that" is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life.'[16]

New technology has not only increased opportunities for criminal activity, it has also created opportunities for law enforcement and security and intelligence agencies to have access to more sophisticated and new capabilities.[17] The range of intrusive capabilities now available to law enforcement and security and intelligence agencies triggers a range of issues and challenges for individual rights, including how those capabilities are used in investigation activities, the scale of their use, the extent to which such capabilities intrude on privacy rights, legislative authority for their use and safeguards that constrain and regulate such new technological capabilities.[18] These include intrusive capabilities known as 'IMSI catchers', a device that enables interception capabilities in relation to mobile phone devices. There are also applications that reveal location history and allow the tracking of mobile phone devices. Beyond these intrusive capabilities, a simple search of information and digital contents on a smartphone device can in itself be quite revealing. Different technologies, whether through devices or software applications, are capable of creating a trail of electronic evidence that can originate from a variety of sources and geographies:

> '[This] means that almost everything anybody does on a device that is connected to a network is capable of being distributed and duplicated with ease. As a result, the same item of digital data can reside almost anywhere. The ramifications for lawyers and police officers are obvious: the relevant document may be available, but it might not be clear where it resides. This affects how a criminal investigation is conducted….'[19]

Riley v California (US) [20] provides useful insights into evolving methods of communication in the information era, and has been described as a 'helpful reminder' of

---

[16] *Riley v California* 573 U.S. ___ (more) 134 S. Ct. 2473; 189 L. Ed. 2d 430 at 20.
[17] D Anderson QC *A question of trust report of the Investigative Powers Review* (2015) Independent Reviewer of Terrorism Legislation available at *www.gov.uk/government/publications*, accessed 17 May 2016 at 68-70.
[18] Intelligence and Security Committee of Parliament *Privacy and security: A modern and transparent legal framework* (12 March 2015) at 11 available at *https://www.pdpjournals.com/docs/88433.pdf*, accessed 08 August 2019.
[19] S Mason 'The characteristics of electronic evidence' in S Mason (ed) *Electronic Evidence: Disclosure, Discovery and Admissibility* 1ed (2007) 21 at 33.
[20] Supra note 16.

technology as it now exists and the need for the law to keep pace 'both in the interests of national security and the protection of the public, and in the interests of the civil liberties of individuals.'[21] Riley was stopped by police for a traffic violation, which subsequently led to his arrest on charges of possession of concealed and loaded firearms. Incident to his arrest on weapons charges, police searched Riley's and seized a smartphone device from his trousers' pocket. The police accessed the device's information and digital contents. As a result thereof, based in part on videos and photographs on the smartphone, Riley was charged in connection with a shooting incident that had taken place a few weeks earlier. In the second case consolidated for review, another petitioner Wurie, was arrested by police after being involved in an apparent drug sale. Following Wurie's arrest, two mobile phones were seized from his person. The police accessed the mobile phone and, from call logs of repeated calls to the mobile phone, traced the phone number to an address suspected to be Wurie's apartment. In the execution of a search warrant, police found drugs, a firearm and ammunition. Wurie was subsequently charged with drugs and firearm related offences. The United States Supreme Court was presented with a Fourth Amendment issue of whether the police may, without a warrant, search information and digital contents on a mobile phone that was seized during the course of an arrest.

In a unanimous decision, the Supreme Court held that police generally require a warrant in order to search mobile phones, even when it occurs during an otherwise lawful arrest. Debunking earlier held assumptions and analogies between physical records and digital data as being 'materially indistinguishable', Roberts CJ explained that analogising the search of data on a mobile phone to a search of physical items is akin to 'saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from Point A to Point B but little else justified lumping them together.'[22] Roberts CJ observed that mobile phone devices 'differ in both a quantitative and a qualitative sense' from other types of objects kept on an arrested person. Such a device, he noted, 'is itself misleading' because they effectively operate as 'minicomputers that also happen to have the capacity to be used as a telephone' with 'one of the most notable distinguishing features' being 'their immense storage

[21] *The Queen (on Application of National Council for Civil Liberties (Liberty) v Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs* [2019] EWHC 2057 (Admin) para 200.
[22] Supra note 16 at 16-17.

capacity.'[23] He continued that the storage capacity of modern cell phones have a number of consequences for privacy:

> 'First, a cell phone collects in one place many distinct types of information – an address, a note, a prescription, a bank statement, a video – that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier.'[24]

Later, Roberts CJ expounded on the qualitative differences between physical records and stored digital data on a mobile phone by reference to examples such as an 'Internet search and browsing history' which 'could reveal an individual's private interests or concerns' and 'historic location information' which 'can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.'[25]

These challenges raised in *Riley* demonstrate the complexities of electronic evidence and technology. Similarly, in South Africa, the pace of technological change is a challenge for those responsible for policy, legislation and regulation.[26] The last two decades have witnessed rapid developments in technology resulting in extraordinary changes to the physical nature of computers, introduction of smart devices and mobile technology, including the proliferation of a modern global communications system, range of applications and networked technology. The existence of adequate safeguards against misuse of these devices and applications under the guise of investigation activity cannot be understated. Limits and safeguards are therefore essential in an information age no longer limited by 'physical realities' which 'generally constituted only a narrow intrusion on privacy.'[27]

---

[23] Supra note 16 at 17.
[24] Supra note 16 at 18.
[25] Supra note 16 at 19-20. The Chief Justice referred to *United States v Jones* 565 U. S. ___, ___ (2012) (Sotomayor, J., concurring) (slip op., at 3): 'GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.'
[26] See Royal United Services Institute for Defence and Security Studies *A democratic license to operate: Report of the independent surveillance review* (July 2015) at 7 available at *https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf*, accessed January 2018 (hereafter 'RUSI').
[27] *Riley's* case supra note 16 at 3.

III A PERSPECTIVE ON PRIVACY IN THE INFORMATION AGE

(a) *'Electronic surveillance is the greatest level[l]er of human privacy ever known'*[28]

It has been rightly stated that 'antiquated laws will neither keep the public safe nor ensure individual privacy.'[29] The concept of privacy has been much debated, especially in recent times. Following the constructs of a law, that was developed before the unprecedented rise of innovations in technology that have enabled a technology-dependent and data-based society, the right to privacy, both online and offline, poses new dilemmas for privacy protection and what constitutes a justifiable level of intrusion in law.[30] There are two imperatives in the underlying analysis for a change in law: (a) innovations in communications technology enabling greater capabilities of our law enforcement and security and intelligence agencies, and (b) the privacy interests they implicate.

New techniques and technologies of surveillance capabilities emphasise the cautionary statements of Justice Brandeis when he said that '[s]ubtler and more far-reaching means of invading privacy have become available to the Government', and that '[d]iscovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.'[31] In the information era, communications technologies have enhanced the capacity to conduct electronic surveillance and data collection. Technological advancements mean declining costs of surveillance technology and data storage. This means that the ability and effectiveness of the state in conducting surveillance is no longer limited by scale or duration, or any of the financial or practical disincentives often associated with conducting surveillance, allowing the state to have 'a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before.'[32]

---

[28] *United States v White* 401 U.S. 745 (1971) at 756, Douglas J dissenting.
[29] RUSI op cit note 26 at x.
[30] Ibid.
[31] *Olmstead v United States* 277 U.S. 438, 473 (1928) (Brandeis J, dissenting). See also SD Warren and LD Brandeis 'The right to privacy' (1890) Harvard LR 193 at 195: 'Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meets the demands of society … Recent inventions and business methods call attention to the next step which must be taken for protection of the person, and for securing to the individual … the right to be let alone.'
[32] Human Rights Council 'The right to privacy in the digital age' A/HRC/27/37 (30 June 2014) at 3 available at *http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf*, accessed 04 January 2016.

Any disproportionate, or unfettered, use of interception powers can have consequences for individual rights.[33] The volume of communications data now being generated has the potential to give law enforcement, including security and intelligence agencies, unprecedented access to personal information unless privacy protections and safeguards are robust in the modern communications environment.[34] The regulation of electronic surveillance and the need to protect us from a 'much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words' has been articulated by Supreme Court of Canada court as 'the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance.'[35] The court went further:

> 'A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. … If the state may arbitrarily record and transmit our private communications, it is no longer possible to strike an appropriate balance between the right of the individual to be left alone and the right of the state to intrude on privacy in the furtherance of its goals, notably the need to investigate and combat crime.[36]

As the court recognised, the regulation in doing so 'is not to deny that it is of vital importance that law enforcement agencies be able to employ electronic surveillance in their investigation of crime.'[37] After all, electronic surveillance plays 'an indispensable role in the detection of sophisticated criminal enterprises.'[38] The threat that such conduct would pose to privacy rights, and deemed 'wholly unacceptable' by the court, is if 'in a free society that the agencies of the state be free to use this technology at their sole discretion.'[39] It therefore becomes important, and necessary to 'strike a reasonable balance between the right of individuals to be left alone and the right of the state to intrude on privacy in furtherance of its responsibilities for law enforcement.'[40]

---

[33] United Kingdom *Interception of communications in the United Kingdom: A consultation paper* (Cm 4368, 1999) 1.
[34] J Clough 'A world of difference: The Budapest convention on cybercrime and the challenges of harmonisation' (2014) 40.3 *Monash University LR* 698 at 712. See also L Huey and R Rosenberg 'Watching the web: Thoughts on expanding police surveillance opportunities under the Cyber-Crime Convention' (2004) 46 *Canadian Journal of Criminology and Criminal Justice* 597.
[35] *R v Duarte* [1990] 1 SCR 30 at 44.
[36] Supra note 35 at 44.
[37] Supra note 35 at 44.
[38] Supra note 35 at 44.
[39] Supra note 35 at 45.
[40] Supra note 35 at 45.

Section 14 of the Constitution of the Republic of South Act 108 of 1996[41] guarantees everyone the right to privacy, including the right not to have their person or home searched, their property searched, their possessions seized, or the privacy of their communications infringed. The right to privacy has been discussed in a number of Constitutional Court judgments.[42] In *Bernstein and Others v Bester and Others NNO*,[43] Ackermann J characterised the right to privacy as 'a continuum of privacy rights which may be regarded as starting with a wholly inviolable inner self, moving to a relatively impervious sanctum of the home and personal life and ending in a public realm where privacy would only remotely be implicated, if at all.'[44] He stated:

> 'A very high level of protection is given to the individual's intimate personal sphere of life and the maintenance of its basic preconditions and there is a final untouchable sphere of human freedom that is beyond interference from any public authority. So much so that, in regard to this most intimate core of privacy, no justifiable limitation thereof can take place. But this most intimate core is narrowly construed. This inviolable core is left behind once an individual enters into relationships with persons outside this closest intimate sphere; the individual's activities then acquire a social dimension and the right of privacy in this context becomes subject to limitation.'[45]

---

[41] Hereafter 'the Constitution'.

[42] *National Coalition For Gay and Lesbian Equality and Another v Minister of Justice and Others* 1999 (1) SA 6 (CC) paras 29-32; *Mistry v Interim Medical and Dental Council of South Africa and Others* 1998 (4) SA 1127 (CC) paras 22-23, 25, 27-30; *Case and Another v Minister of Safety and Security and Others, Curtis v Minister of Safety and Security and Others* 1996 (3) SA 617 (CC) para 91. See also *Investigating Directorate: 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 2001* (1) SA 545 (CC) (25 August 2000) para 18: 'As we have seen, privacy is a right which becomes more intense the closer it moves to the intimate personal sphere of the life of human beings, and less intense as it moves away from that core.' See also *Thint (Pty) Ltd v National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others* 2009 (1) SA 1 (CC) para 77: 'Although a search and seizure operation will inevitably infringe a person's right to privacy, the Act provides considerable safeguards which ensure that the infringement goes no further than reasonably necessary in the circumstances. Furthermore, the requirement of judicial authorisation for search warrants is only one aspect of a broader scheme which ensures that the right to privacy is protected.'

[43] 1996 (2) SA 751 (27 March 1996). The most pertinent passage in his judgment merits quotation in full, para 67: 'The truism that no right is to be considered absolute implies that from the outset of interpretation each right is always already limited by every other right accruing to another citizen. In the context of privacy this would mean that it is only the inner sanctum of a person, such as his/her family life, sexual preference and home environment, which is shielded from erosion by conflicting rights of the community. This implies that community rights and the rights of fellow members place a corresponding obligation on a citizen, thereby shaping the abstract notion of individualism towards identifying a concrete member of civil society. Privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly.'

[44] *S v Jordan and Others (Sex Workers Education and Advocacy Task Force and Others as Amici Curiae* (CCT31/01 2002 (6) SA 642 para 76. *Bernstein's* case supra note 43 para 75.

[45] Supra note 43 para 75.

Notably the right to privacy extends beyond 'the inner sanctum', a principle firmly established in *Bernstein's* case. The Court stated that 'the scope of a person's privacy extends *a fortiori* only to those aspects in regard to which a legitimate expectation of privacy can be harboured.'[46] In *Magajane v Chairperson, North West Gambling Board*,[47] the court sought to interpret the right to privacy with reference to *Bernstein's* case: 'Ackermann J described what can be seen as a series of concentric circles ranging from the core most protected realms of privacy to the outer rings that would yield more readily to the rights of other citizens and the public interest.'[48] It is possible to identify two forms which an invasion of the right to privacy may take: (i) an unlawful intrusion upon the personal privacy of another and (ii) the unlawful publication of private facts about a person.[49] The right to privacy covers certain private facts about which there is a reasonable expectation of privacy. The reasonable expectation of privacy test comprises two questions. Firstly, there must at least be a subjective expectation of privacy and, secondly, the expectation must be recognised as reasonable by society.[50]

Central to the debate and delicate legislative balance is a consideration of whether privacy is possible,[51] and still matters in this era of innovations in communications technology.[52] Is it the case that 'privacy is no longer the social norm',[53] and should we simply accept that in this information age 'you have zero privacy anyway, get over it?'[54] As such is it inevitable that privacy can no longer be protected? That any attempt to regulate the powers of law enforcement and security and intelligence agencies, should thus be abandoned?[55] Therefore any intrusion by law enforcement and security and intelligence agencies remains

[46] Supra note 43 para 77.
[47] (CCT49/05) 2006 (5) SA 250 (8 June 2006).
[48] Supra note 47 para 77.
[49] *Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and Another* (612/90) [1993] 2 All SA 109 (A) (18 February 1993) para 29. At para 31, the court stated: 'The telephone-tapping which occurred was manifestly an unlawful invasion of the privacy of Sage and its corporate executives and appellants did not seek to justify the tapping; nor is there any acceptable evidence on record which would possibly provide such justification.'
[50] *Bernstein's* case supra note 43 paras 75-76.
[51] BN Meeks 'Is privacy possible in the digital age?' (2000) available at *http://www.nbcnews.com/id/3078854/t/privacy-possible-digital-age/#.WHI2fLFh0fN*, accessed 08 January 2017.
[52] A Roos 'Privacy in the Facebook era: A South African legal perspective' (2012) 129 *SALJ* 375.
[53] Facebook founder M Zuckerberg (2010) available at *https://www.theguardian.com/technology/2010/jan/11/facebook-privacy*, accessed 08 January 2017.
[54] Former Sun Microsystems CEO Scott McNealy (1999) available at *http://archive.wired.com/politics/law/news/1999/01/17538*, accessed 08 January 2017. See also J Morgan 'Privacy is completely and utterly dead, and we killed it' (2014) available at *http://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/#609dae69dfbd*, accessed 11 January 2017.
[55] Anderson op cit note 17.

'justified by a calculated and often persuasive narrative that holds the goals of national security above all else?'[56] As noted by Preston:

> 'We have come to the end of privacy; our private lives, as our grandparents would have recognised them, have been winnowed away to the realm of the shameful and the secret. … Insidiously, through small concessions that mounted up over time, we have signed away rights and privileges that other generations fought for, undermining the very cornerstones of our personalities in the process. While outposts of civilisation fight pyrrhic battles, unplugging themselves from the web – *"going dark"* – the rest of us have come to accept that the majority of our social, financial and even sexual interactions take place over the internet and that someone, somewhere, whether state, press or corporation, is watching.'[57]

Notwithstanding the developments in communications technologies in the information age, in my view, it does not mean that individual privacy should no longer be protected, or that attempts to regulate the exercise of investigative powers should be abandoned without ado.[58] It is within this context that the exercise of investigative powers by law enforcement and security and intelligence agencies in chapters 2, 3 and 4 are explored. Undoubtedly, the investigative powers analysed in chapters 2-4 implicate the right to privacy. A number of cases in the Constitutional Court dealing with warrants for search and seizures provide guidance in this regard. In *Mistry v Interim Medical and Dental Council of South Africa and Others*, the Constitutional Court held that '[t]he existence of safeguards to regulate the way in which state officials may enter the private domains of ordinary citizens is one of the features that distinguish a constitutional democracy from a police state.'[59] In *Magajane's* case, with regard to all regulatory inspections 'searches' for the purpose of the threshold question of whether the inspection falls within the scope of the privacy interest, Van Der Westhuizen J in writing the judgment of the court held that it would be 'undesirable' to 'impose' an 'arbitrary demarcation line between degrees of intrusion' that would 'invoke' the right to privacy.[60] Doing so, he held, 'would have the negative effect of placing certain administrative inspections beyond the reach of judicial review.'[61] It was concluded that the relevant provision governing regulatory

---

[56] K Rodriguez 'Tackling state surveillance and protecting human rights' (2012) available at *https://www.eff.org/deeplinks/2012/12/tackling-state-surveillance-and-human-rights-protecting-universal-freedoms*, accessed 08 January 2017.
[57] A Preston 'The death of privacy' (2014) available at *https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston*, accessed 11 January 2016.
[58] Ibid at 37-38.
[59] Supra note 42 para 25. See also *Gaertner and Others v Minister of Finance and Others* 2014 (1) SA 442 (CC) para 47: 'the right to privacy embraces the right to be free from intrusions and interference by the state and others in one's personal life.'
[60] Supra note 47 para 59.
[61] Supra note 47 para 59.

inspections limited the constitutional right to privacy and Van Der Westhuizen J went further to consider whether the limitation of the right passed 'constitutional muster.'[62] Van Der Westhuizen J importantly referred to a proportionality analysis in relation to legislation that limited the right to privacy, including an applicant's expectation of privacy and the breadth of the legislation:

> 'Legislation may not be so broad as to have the real potential to reach into private homes. In assessing whether legislation could have achieved its desired ends through less damaging means, a court will determine whether the legislation could have required a warrant, and a court will consider whether a warrant requirement would frustrate the state's regulatory objectives and whether in the absence of a warrant the legislation provides sufficient guidance to inspectors as to the limits of the inspections.'[63]

It is not intended in the thesis to provide detailed analysis on the legal protections of the right to privacy in South African law.[64] Suffice to add the following: the right to privacy is a qualified right. Its interpretation in the context of a world in a year 2020 information age raises challenges as regards our understanding in terms of the dichotomy of notions and boundaries between what constitutes public interest and what constitutes private interest.[65] Notions of privacy have significantly changed in the last decade to the extent that innovations in digital communications technologies have resulted in an 'unprecedented willingness' to share 'once-private information with online contacts, service providers and the general public.'[66] At the press of 'accept' on a touchscreen device, large volumes of personal information are now created as a result of day-to-day online activities, seemingly without any guarantee of whom can access that information once the digital record has been created.[67] Changes to privacy notions as coined in the description 'modern attitudes to privacy' are therefore not without relevance.[68] This may for example have a bearing on (diminished) reasonable expectations of privacy in a particular type of data at a particular time, or perhaps a sort of argument for dispensing with the constraints on the state's retention or use of such data?

---

[62] Supra note 47 para 59.
[63] Supra note 47 para 50.
[64] Helpful texts in this regard include I Currie & J de Waal *The Bill of Rights Handbook* 6ed (2013) at 294-313; H Davis *Human Rights and Civil Liberties* (2003) and R Stone *Textbook on Civil Liberties and Human Rights* 5ed (2004).
[65] Human Rights Council op cit note 32.
[66] Anderson op cit note 17 at 37.
[67] Rodriguez op cit note 56.
[68] Ibid at 37-38. See also D Bilchitz 'Privacy, surveillance and the duties of corporations' (2016) *TSAR* 45 and McKinley, D 'New terrains of privacy in South Africa' December 2016 available at *https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/r2kmpdp_new_terrains_of_privacy_in_south__africa_masterset_small.pdf*, accessed February 2019.

To the contrary however, I am of the view that as more of our lives are lived online, and as more of our personal information is bound by a system of interrelated *connectivity, devices and data*, with the ability to gather and share our detailed information, the arguments for strict legal regulation on the powers of the state become, if anything, more compelling.[69]

IV KEY LEGISLATIVE INSTRUMENTS

The final part of this chapter will introduce the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002[70] and Electronic Communications and Transactions Act 25 of 2002[71] as key legislation in respect of the investigative powers of law enforcement and the security and intelligence agencies to obtain electronic evidence and subsequent admissibility of such evidence in criminal proceedings. Whilst there are criticisms, and more recently legal challenges to the constitutionality of certain provisions, RICA 2002 and the ECT Act 2002 are arguably the most important legislative instruments to consider the issue of electronic evidence. One of the criticisms levelled against this key legislation, enacted almost two decades ago, is the rigid application of its provisions such that the current era of the information age and a modern fast-paced environment of technological advancements, is treated as not making a difference, when they clearly do. This section is intended as a brief introduction to challenges for the law, and not to discuss in depth the full contents of the legislative provisions as these will considered (where relevant) in the chapters to follow.

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

(i) Background: The Interception and Monitoring Prohibition Act 127 of 1992

In South African law during the 1990s the period between the adoption of the interim Constitution of the Republic of South Africa Act 200 of 1993, and ultimately the new democratic constitutional dispensation with the adoption of a Bill of Rights in the final Constitution of the Republic of South Act 108 of 1996, led to a repeal of legislation dealing with safety and security that sustained apartheid as a political and social system of

[69] Anderson op cit note 17 at 38.
[70] Hereafter 'RICA 2002'.
[71] Hereafter 'ECT Act 2002'.

institutionalised racial segregation.[72] Many were clearly inconsistent with the Constitution as the supreme law of the land.[73] The Interception and Monitoring Prohibition Act 127 of 1992[74] was enacted on 1 February 1993. It was drafted before the interim Constitution (1993), and remained operative for a number of years following the adoption of final Constitution and Bill of Rights (1996). While the IMP Act 1992 was drafted without the framework of the final Constitution and Bills of Rights, it was recognised in the drafting stages that the Act would have to withstand legal challenges on the constitutionality of its provisions. The following observation was made in *S v Naidoo and Another*,[75] a case regarding the constitutionality of the IMP Act 1992 in relation to the limitation clause contained in s 33(1) of the interim Constitution:

> '[T]he Monitoring Act was a law of general application, the provisions of which complied with the requirements of s 33 of the interim Constitution. …What is clear is that, probably after the experience of police methods during the apartheid era, … the Legislature saw fit to repeal the old provisions relating to interception of personal articles, telephone communications, etc in terms of which various Ministers could authorise such actions and to replace those provisions with the obviously extremely stringent and limited provisions of the Monitoring Act. Such provisions are, as I have already indicated, in line with similar provisions in other countries.'[76]

Although the IMP Act 1992 passed a constitutional legal challenge in *Naidoo's* case, consideration had to be given for a review of an Act drafted before the new constitutional and democratic dispensation in South Africa by implication of the court's observation of the legacy of apartheid and objectionable police methods used. The South African Law Reform

---

[72] See N Mandela *Long Walk to Freedom* (1994), A Sparks *Tomorrow is Another Country* (1994), F Welsh *A History of South Africa* (1998) , M Shaik *The ANC Spy Bible* (2020), H Dousmetzis *The Man Who Killed Apartheid: The Life of Dimitri Tsafendas* (2019), S Venter *A Free Mind: Ahmed Kathrada's Notebook from Robben Island* (2005) and A Kathrada *No Bread for Mandela: Memoirs of Ahmed Kathrada, Prisoner No. 568/64* (2010).

[73] This included the Riotous Assemblies Act 17 of 1956; the Explosives Act 26 of 1956; the Intimidation Act 72 of 1982; the Internal Security Act 74 of 1982; and the Regulation of Gatherings Act 205 of 1993.

[74] Hereafter ' IMP Act 1992'.

[75] 1998 1 SACR 479 (N). The case involved a law enforcement authority that furnished false and misleading affidavits to a judge in order to obtain judge's direction, in terms of the IMP Act 1992, permitting law enforcement to monitor certain telephones. The question before the court: 'was the evidence obtained as a result of the issue of the [Judge's] direction based on the false information furnished to him, evidence obtained in a manner that violates any right, of the accused, in the Bill of Rights?' (at 522). The Court expounded on two schools of thought that had emerged, after the enactment of the interim Constitution, with regard to the admissibility of evidence obtained by unlawful means, 'namely (a) that the Courts had a wide general discretion to exclude unlawfully or improperly obtained evidence on grounds of fairness and public policy, and (b) that the exercise of a judicial discretion was no longer permissible, and that if evidence had been obtained in breach of a constitutional right it had to be excluded unless the breach could be justified in terms of the constitutional 'limitation' clause (namely s 33(1) of the interim Constitution, which corresponded with s 36(1) of the new Constitution)' (at 491).

[76] Supra note 75 at 505.

Commission[77] reviewed the IMP Act 1992 in a comprehensive legislative reform project titled 'Review of Security Legislation'.[78] The IMP Act 1992 was reviewed 'with reference to, and in comparison with, the legal position in France, the Netherlands, Belgium, Germany, Britain, the United States of America, Hong Kong and Canada.'[79] The compelling reasons for a review of the IMP Act 1992 related to the impact of new technologies on the regulation of surveillance and interception of communications. The Law Reform Commission proposed a draft Bill, that sought to augment the legal provisions of the IMP Act 1992.[80] Telecommunication service providers vehemently opposed the recommended proposals. The Mobile Telephone Networks (Pty) Ltd [MTN] was of the opinion that the Bill's proposals were 'grossly unreasonable, not only towards Service Providers or Network Operators but also to the general public.'[81] Three

[77] The South African Law Reform Commission (prior to 2002 known as the South African Law Commission) is established by the South African Law Reform Commission Act 19 of 1973. The Law Reform Commission makes 'recommendations to Government for the development, improvement, modernisation or reform of the law.' The Law Reform Commission is accountable to the Minister of Justice and Constitutional Development.
[78] See South African Law Commission (Project 105) Review of Security Legislation Discussion Paper *The Interception and Monitoring Prohibition Act 127 of 1992* (1998) and South African Law Commission (Project 105) Review of Security Legislation Report *The Interception and Monitoring Prohibition Act 127 of 1992* (1999).
[79] South African Law Commission (Project 105) Review of Security Legislation Report *The Interception and Monitoring Prohibition Act 127 of 1992* (1999) at xiii. The Law Reform Commission observed that 'in general', the IMP Act 2002 compared favourably with the legislation of the list countries (at xiii).
[80] The Interception and Monitoring Prohibition Amendment Bill 1999. Specific recommendations included: insertion of a definition of 'call-related information' service' (clause 1*(a)*); the definition of 'judge' (clause 1*(b)*); definition of 'communication' (clause 1*(b)*); expansion of the definition of 'serious offence' to include inter alia 'planned or premeditated' and offenses relating to: trafficking in firearms, ammunitions and explosives, death or serious bodily harm of any person, organised crime, money-laundering or the proceeds of crime (clause 1*(c)*); the definition of 'telecommunication service' (clause 1*(d)*); no person shall intercept or monitor any conversation or communication (clause 2(1)*(b)*); designation of judges and application for interception directives(clause 3(1)*(a)*); client/legal representative privilege (clause 3(7)); the remuneration of direct costs (clause 4(5)); ensuring capacity to intercept (clause 5A); acquiring of facilities and devices (clause 5A(2)); the investment, technical maintenance and operating cost in enabling interception to be carried out by service providers (clause 5A(3)), routing of duplicate signals to relevant central monitoring centre (clause 5A(4)); central monitoring centres to be equipped and maintained at State's expense (clause 5A(5)); the Minister may issue a directive to comply with his or her directive specifying the security, technical and functional requirements of facilities and devices (clause 5A(6)); capacity, systems used and connectivity, etc (clause 5A(7)); period of three months to comply with directive (clause 5A(8)); provision of call-related information on an ongoing basis for a specified duration (clause 5B(1); routing the information to a designated central monitoring centre (clause 5B(2)); the judge may direct the provision of call-related information on an ongoing basis (clause 5B(3)); the provisions of the Act on the provision of call-related information excludes the use of any power in any other Act to obtain evidence or information in respect of a person, body or organisation (clause 5B(4)); telecommunication service providers to keep proper records of client identities and addresses in respect of whom a service is provided (clause 5B(4)); provision of information regarding identity (clause 5B(6)); provision of name, identity number and address of person contracted for the use of a specified telecommunications number (clause 5B(7)); urgent applications (clause 6); evidence is subject to the decision of a Director of Public Prosecutions or an Investigating Director (clause 6A(1)); admissibility of evidence obtained as a result of monitoring/interception (clause 6A(2)); penalties (clause 8); and revocation of license (clause 8A).
[81] South African Law Commission (Project 105) Review of Security Legislation Report *The Interception and Monitoring Prohibition Act 127 of 1992* (1999) at 133. Telkom expressed similar sentiments: 'the proposals give rise to a plethora of problems' in relation to obligations placed on telecommunication service providers (at 128) and will need to be 're-examined' and re-defined' (at 130). M-Web responded that it remained 'unconvinced by the proposed amendments and stated that it 'may not pass constitutional muster as there may

key issues came to the fore during the consultation process: (a) the circumstances in which it will be appropriate (and lawful) for law enforcement and security and intelligence agencies to undertake surveillance and interception of communications which was recognised as 'essential to effective police work';[82] (b) the protection of individual rights, in particular, the right to privacy in view of 'increasingly powerful and revealing technology'; and (c) the adoption of a legal framework that avoids a negative impact on development of innovation and new technologies.[83] Twenty-one years later, the tension between these three issues remain as important in the analysis of the current legal frameworks regulating the investigative powers of surveillance and interception of communications by law enforcement and security and intelligence agencies in South Africa. These are issues that need to be addressed and lie at the heart of analysis in the thesis.

Although the Interception and Monitoring Prohibition Amendment Bill 1999 in the form proposed by the Law Reform Commission did not become law, many of its proposals came to be reflected in new legislation in the form of RICA 2002.[84] There is no other legislation in South Africa specifically regulating the interception of communications. Similar to models adopted worldwide, RICA 2002 bans interception of communications content, creates exceptions for government agencies, permits access to information about the communications (metadata), establishes authorisation and oversight regimes, and compels communication service providers to provide intercept capabilities and/or access to data, including prescriptions on data retention and compelled decryption measures.[85] The RICA 2002 regulates the interception of certain communications relating to serious crimes, the provision of certain communication-related information, applications to a designated judge for the issuing of directions and entry warrants, the execution of directions and entry warrants by law enforcement officers and the prohibition of telecommunication services which do not have the capability of being intercepted. The Act also creates offences and prescribes penalties for any contravention of its provisions. It also prescribes that certain information of clients must be

be no rational basis for the imposition of potentially overbroad obligations on a telecommunications [service provider] (at 135).

[82] *Naidoo's* case supra note 75 at 505.

[83] South African Law Commission (Project 105) Review of Security Legislation Report *The Interception and Monitoring Prohibition Act 127 of 1992* (1999) at 134-35.

[84] The Interception and Monitoring Prohibition Amendment Act 77 of 1995, assented to on 28 September 1995, was limited by its only provision for the amendment of s 1 of the IMP Act 1992 'so as to redefine "judge" to 'mean any judge of any provincial or local division of the Supreme Court of South Africa including…any retired judge.' The IMP Act 1992 and the Amendment Act 1995 was subsequently repealed by RICA 2002.

[85] See G Hosein and CW Palow 'Modern safeguards for modern surveillance: An analysis of innovations in communications surveillance techniques' (2013) 74.6 *Ohio State LJ* 1071 at 1072.

obtained and kept by telecommunication service providers should it be required for detecting or investigating serious crime.[86]

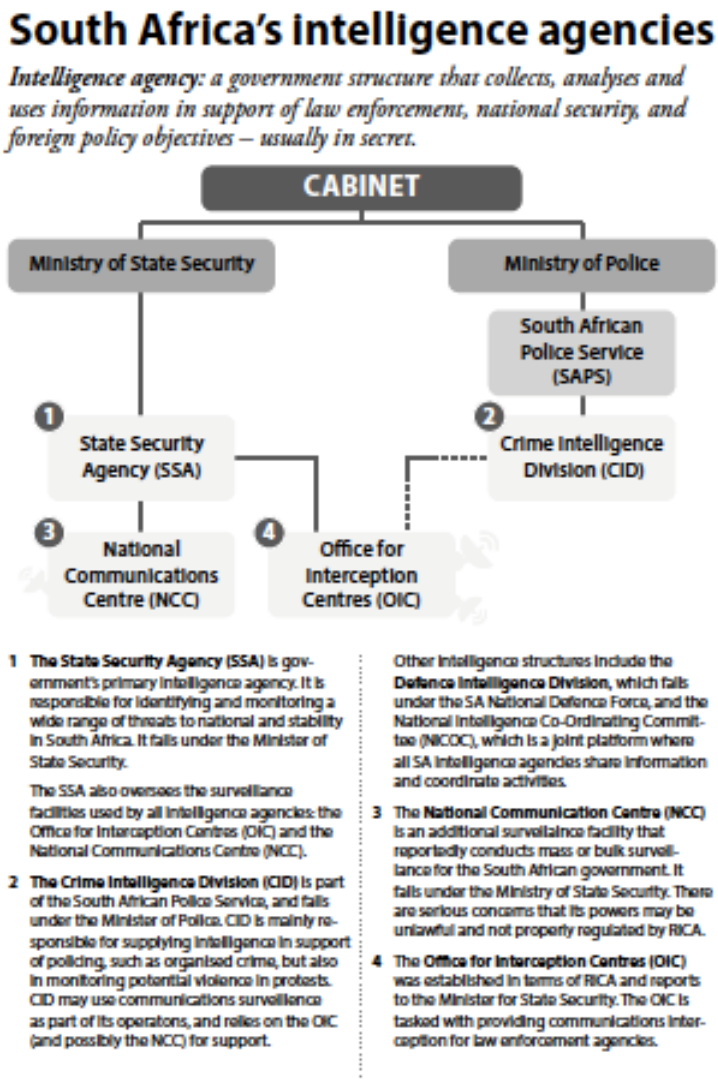
(ii) Interception of communications

The use of interception in South Africa is currently governed by RICA 2002. Interception involves making available the contents of any communication to someone other than the sender or intended to a person other than then sender, recipient or intended recipient. As an intelligence gathering and investigative capability available to law enforcement and security and intelligence agencies, access to such information and communications by interception can be essential in the disruption, prevention and detection of criminal activities, including providing operational support leadings to arrests and prosecutions. At the time of its enactment into law, interception commonly related to telephony, such as intercepting voicemail messages. Technically, RICA 2002 refers to 'communications' and insofar as they relate to the 'contents of communications.' In the context of technological advancements this could include emails and other forms of communications such as VoIP services, such as Skype or Facetime.[87] Does it matter? Arguably yes. Given that such investigative power is potentially a significant intrusion into privacy rights in a year 2020 information age, effective safeguards, transparency and oversight become of vital importance.

Interception conducted under a lawful warranted process can only be used for specified purposes, including for prevention and detection of serious offences, or for matters related to national security or national economic interests. Interception is limited to the following structures of the state, collectively referred to in the thesis as law enforcement and security and intelligence agencies:[88] (a) the South African Police Services; (b) the South African National Defence Force; (c) the National Intelligence Agency; (d) the South African Secret Service; (e) Directorate of Special Operations (now Head of an Investigating Directorate); (e) the National Prosecuting Authority; and (f) the Independent Complaints Directorate. The Right2Know

[86] Memorandum on the objects of the Regulation of Interception of Communications and Provision of Communication-Related Information Amendment Bill, 2006, Background of Bill clause 1. The Act was assented to on 30 December 2002,86 however, it only came into operation on 30 September 2005. See Proclamation R55 in Government Gazette 28075: '30 September 2005 as the date on which the said Act, with the exception of sections 40 and 62 of the Act, shall come into operation.' Further in terms of Proclamation R23 in Government Gazette 31189, ss 62(1) and (5) of the Act came into operation on 30 June 2008. In its latest amendment, RICA 2002 has been amended by the General Intelligence Laws Act 11 of 2013.
[87] AA Gillespie *Cybercrime: Key Issues and Debates* (2019) at 337.
[88] Having regard to the definition of 'applicant', including 'directorate', 'law enforcement agency' and 'law enforcement officer' in s 1 of RICA 2002.

campaign diagrammatically presents an overview of the role of South Africa's intelligence agencies as follows:[89]



The investigative powers in relation to interception is controversial and has attracted attention in recent years, mostly because of allegations levelled against law enforcement and the security and intelligence agencies. The allegations include reports of unlawful surveillance practices, abuse of power, inadequate safeguards and remedies against unlawful interference with the right to privacy. In April 2017, the amaBhungane Centre for Investigative Journalism launched a legal challenge to the constitutionality of RICA 2002 following surveillance measures by the National Intelligence Agency[90] against its director, SP Sole.[91] The incidents

[89] Source: Right2Know 'SPOOKED: Surveillance of journalists in SA' June 2018 *https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf.*, accessed 17 June 2019.
[90] Now the State Security Agency (hereafter 'SSA').
[91] Press release 'AmaB challenges snooping law' 20 April 2017 available at *https://amabhungane.org/advocacy/advocacy-amab-challenges-snooping-law/*, accessed 19 June 2019.

cited in its papers included the illegal tapping of a journalists phones, deliberate lying to judges in order to get electronic surveillance authorisation; using improperly obtained information to harass journalists investigating members of the police crime intelligence unit; security and intelligence surveillance of journalists investigating corruption; monitoring of private communications of journalists who challenged the censorship policies of the state broadcaster and bribery of telecommunication service providers to obtain phone records of media editors.[92]

The legal challenge by amaBhungane Centre for Investigative Journalism has now also forced the state to address the constitutionality of the legal provisions of RICA 2002. The technicalities of how a communication is intercepted is likely to change as technology develops and as such it is important that the outcome of legislative reform remains dynamic, whether in the form of amendments to existing law or new legislation.[93] The thesis will examine the 'concrete question' of how the use of emerging surveillance technologies, as an intelligence gathering and investigative capability, should be regulated in South African law with sufficient safeguards against risk of abuse.[94] This will be explored in the context of the regulatory framework in the RICA 2002 governing the investigative powers of law enforcement and the security and intelligence agencies, specifically, interception of communications (chapter 2), retention and acquisition of communications data (chapter 3), and access to electronic data protected by encryption (chapter 4).

(iii) Retention and acquisition of communications data

Arguably the most controversial investigative power, and one which poses challenges for the law in recent times, relates to the mandatory retention and acquisition of communications data. To law enforcement and the security and intelligence agencies 'communications data is simply using the by-product of communications devices as evidence' and is regarded as significant in criminal investigations, particularly serious offences.[95] By 2017, it was reported that the yearly

[92] In a report, *Protecting journalism sources in the digital* age, published in 2017 by the United Nations Educational, Scientific and Cultural Organization, it was found that that the legal frameworks that protect the confidential sources of journalism are under significant strain in the digital age by the challenges of mass surveillance, mandatory data retention, and disclosure by third party intermediaries. Available at *http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/protecting_journalism_sources_in_digital_age.pdf*, accessed 30 June 2020. See also E van Diemen '"Spying case": 8 times journalists believe they were snooped on, as RICA Act gets challenged in court' 4 June 2019 available at *https://www.news24.com/South Africa/News/spying-case-8-times-journalists-believe-they-were-snooped-on-as-rica-act-gets-challenged-in-court-20190604*, accessed 17 June 2019.
[93] Gillespie op cit note 9 at 80.
[94] Hosein and Palow op cit note 85 at 1089.
[95] Gillespie op cit note 9 at 4-6.

average of requests to the four major telecommunication service providers in South Africa for communications data estimated about 51,286. Although it is difficult to gauge the increase in requests over the years,[96] it appears that accessing communications data has quickly become mainstream, and almost routine for law enforcement and the security and intelligence agencies.[97] Communications data has always been likened to 'who', 'when' and 'where' of a communication, but not the content of what was said or written.[98] Differing authorisation procedures in RICA 2002 between interception (content) and communications data ('envelope' information, not its contents), reflect a legal construct that distinguishes between what kinds of information implicate greater or lesser privacy interests. This distinction is based on the fact that because the content of the communication cannot be accessed, it is therefore not as intrusive.

The counter-argument is that technological advancements have arguably blurred this distinction. RICA 2002 lags behind the pace in an era of innovations in communications technology such that law enforcement and security and intelligence agencies are able to capture more information than previously possible, some reportedly by unlawful surveillance practices, raising significant concerns for individual rights. Having regard to a modern communications environment in which RICA 2002 operates in the year 2020 information age, and its implications for surveillance measures, the position in RICA 2002 based on underlying assumptions that communications data is less intrusive and not as revealing as the content of communications is no longer sustainable. Indeed, it has been noted that monitoring communications data over a period of time could reveal sensitive content and detailed understanding of a person's life. Roberts notes that analysis and collation of this information could reveal 'the number and nature of a person's relationships, the state of his finances; his

[96] Section 42 of RICA 2002 prohibits the disclosure of any information received pursuant to the Act. This includes, by virtue of s 42(3), the disclosure of the fact that any demand for lawful interception or communications data has been issued under the Act. Telecommunication service providers in South Africa also take the view that to publish aggregate statistics would be to disclose the existence of one or more lawful interception or communications data demands. See Vodafone Group Plc *Law Enforcement Disclosure Report 2015* available at *https://www.vodafone.com/content/dam/vodcom/sustainability/pdfs/vodafone_law_enforcement_disclosure_report_2015-4.pdf*, accessed 10 March 2020.

[97] Gillespie op cit note 9 at 38-39 quoting Theresa May MP (*Hansard*, HC Deb 10 July 2014, vol 584, col 456.): 'Communications data has played a significant role in every Security Service counter-terrorism operation over the last decade. It has been used as evidence in 95 per cent of all serious organised crime cases handled by the Crown Prosecution Service. And it has played a significant role in the investigation of many of the most serious crimes in recent time, including the Oxford and Rochdale child grooming cases, the murder of Holly Wells and Jessica Chapman and the murder of Rhys Jones. It can prove or disprove alibis, it can identify associations between potential criminals, and it can tie suspects and victims to a crime scene.'

[98] Home Office Acquisition and disclosure of communications data – Code of Practice (TSO 2007) available at *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf*, accessed 4 July 2019.

political views, religion, sexual orientation, life plans and other aspirations; what opinions he might hold about others; his fears, predilections and foibles.'[99]

This has implications for retention of communications data by telecommunication service providers so that it can be later acquired by law enforcement and the security and intelligence agencies. RICA 2002 makes provision for both retention and acquisition of communications data. As will be seen, the acquisition of communications data can only be for specified purposes, including for the prevention and detection of 'serious offences' or in the interests of 'national security or compelling national economic interests' if the reasonable grounds to believe' threshold has been met.[100] RICA 2002 also sets out a core provision in relation to mandatory retention of communications data.[101] What does this mean for our privacy interests, in context of a year 2020 information age, when telecommunication service providers are legally required to retain information about the way we use their services such as whom we called on a particular date and from a particular location, websites we visited and how often, our purchasing habits, our geolocation movements – all of which if collated and analysed can be quite revealing.

There are differing views between those (a) who believe that the mandatory retention of our communications data is 'inappropriate' and constitutes a serious interference with our privacy rights[102] and those (b) who doubt whether the 'mere retention' of communications data amounts to any interference with privacy rights, and if it does, 'it ought to be considered a relatively trivial interference.'[103] The state is likely to argue that even if in principle there is an interference with privacy rights, the interference is 'reasonable and justifiable in an open and democratic society'[104] for the prevention and detection of serious offences. Roberts further expands on the differing views as regards weight to be attached to privacy rights on this issue of communications data:

---

[99] A Roberts 'Privacy, data retention and domination: *Digital Rights Ireland Ltd v Minister for Communications* (2015) 78.3 *The Modern Law Review* 535 at 544.
[100] Section 17, 19.
[101] Section 30.
[102] Gillespie op cit note 9 at 340. See Roberts op cit note 99 at 535 and J Duncan, 'Spies are all set to grab your metadata' (11 September 2015) available at *https://mg.co.z /article/ 2015-09-10-spies-are-all-set-to-grab-your-metadata*, accessed 30 June 2019. See also Liberty *Liberty's response to the Home Office consultation: "Protecting the public in a changing communications environment"* at 19 available at *https://www.libertyhum anrights. org.uk/sites/default/files/liber ty-s-communications-data-consultation-response.pdf*, accessed 4 July 2019, suggesting, with reference to *S and Marper v United Kingdom* EctHR 30562/04 and 30566/04 (4 December 2008), that a similarity could be drawn to retention databases of DNA taken from suspects, victims and witnesses alike.
[103] Roberts op cit note 99 at 535.
[104] Section 36, Constitution of the Republic of South Africa Act 108 of 1996.

> 'It might be said that mere retention of communications data will have no obvious effect on the lives of the great majority of those in respect of whom data is retained. Views on what ought to be required by way of justification for the retention of data are likely to vary in a way that corresponds roughly with divergence of views on the value of privacy and gravity of the interference that individuals suffer where communications data are retained. We might expect those who believe that retention constitutes a particularly serious interference with privacy to say that data retention ought to be predicated on some degree of individualised suspicion, and that even where such suspicion exists, not every piece of communications data should be retained. Those who attach less weight to privacy interests, on the other hand, are more likely to accept the 'needle in a haystack argument'; mass data retention will ensure that a few vital pieces of information are available to the state for the purposes of detecting and investigating serious crime, but in order to find the needle in the haystack, one has to first secure the haystack.'[105]

Following from the above recognition that mandatory retention of communications data 'will have no obvious effect' on the 'great majority', Roberts argues that '[t]he mere fact that there has been a loss of privacy' does not necessarily lead 'to the conclusion that those who have suffered the loss are thereafter subject' to exercise of arbitrary power. [106] He argues that the central issue is 'the extent that the loss of privacy leads to the acquisition of power to interfere on an *arbitrary* basis.'[107] This is an important point. Having regard to the regulatory framework in RICA 2002 for mandatory retention and acquisition of communications data, we should be concerned with the exercise of arbitrary power by law enforcement and the security and intelligence agencies. The right to privacy is not absolute. Any interference is measured against whether it is 'reasonable and justifiable in an open and democratic society' and for legitimate reasons, in this instance for the prevention and detection of 'serious offences' or in the interests of 'national security or compelling national economic interests', and could trump privacy rights. Revelations by the *amaBhungane* case referred above suggests that the scope for arbitrary interference by law enforcement and the security and intelligence agencies is not speculative. As the analysis will demonstrate, the concerns about retention and acquisition of communications data in South Africa is not merely academic or abstract. These are key issues to be explored and central to analysis in chapter 3.

[105] Roberts op cit note 99 at 535.
[106] Ibid at 545.
[107] Ibid (emphasis in original text).

(iv) Electronic data protected by encryption

As if these challenges are not formidable enough, they are in turn compounded by the increasingly accessibility and use of encryption technology.[108] Encryption is considered to be one of the most effective ways of achieving data security and is now commonly used in protecting electronic data that is either 'at rest' such as files on a computer or storage devices (e.g. USB flash drives), or 'in transit' such as data being transferred via networks (e.g. the Internet or e-commence transactions). Messaging services such as 'WhatsApp' as a matter of course encrypt messages end-to-end, whereby its encryption technology 'ensures only you and the person you're communicating with can read what's sent, and nobody in between, not even WhatsApp.'[109]

While encryption is a powerful tool for safeguarding sensitive information, especially in response to increased levels of privacy awareness, data breaches and identity theft, the use of robust digital encryption technologies have also presented opportunities for criminals to encrypt data, whether stored on a device or in transit, in order to conceal their criminal activities and so evade detection and prosecution. With encryption being so widespread, access to data protected by encryption poses challenges for law enforcement and security and intelligence agencies. Even when such electronic evidence has been lawfully obtained, a challenge faced is that seized data may be protected by some form of security measure, such as a password or other form of encryption thereby rendering the data inaccessible or unintelligible.

The concept of 'practically uncrackable' encryption is important to the process of encryption.[110] Without the key or password, criminal investigations involving access to potential evidence that is protected by encryption can require an extraordinary amount of time and resources to bypass encryption. An activity commonly known as 'brute-force attack'[111] could be used, that is guessing every possible iteration of the key until the key is discovered. The type and complexity of the system and key length used in the encryption often determine the practical feasibility of performing a brute-force attack with longer keys exponentially more difficult to break than shorter ones. A measure of the strength of the encryption software is

[108] PN Grabosky & RG Smith *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities* (1998) at 206.
[109] 'End-to-end encryption' available at *https://faq.whatsapp.com/en/android/28030015/*, accessed 13 July 2019.
[110] RM Thompson II & C Jaikaran 'Encryption: Selected legal issues' (2016) at 4 available at *https://fas.org/sgp/crs/misc/R44407.pdf*, accessed 7 April 2020.
[111] J Galbally, J Fierrez, M Martines-Diaz and J Ortega-Garcia 'Evaluations of brute-force attack to dynamic signature verification system using synthetic samples' (2009) paper presented at 10th International Conference on Document Analysis and Recognition available at *http://atvs.ii.uam.es/atvs/files/2009_ICDAR_BruteForce_Galbally_Published.pdf*, accessed 17 October 2016.

how long it would theoretically take an unauthorised user to launch a successful brute-force attack to break the code.[112] It has been noted that a thirteen digit passcode configuration on an iPhone would take about 25,000 years 'to run every possibility.'[113] Some options for law enforcement and security and intelligence agencies include: 'find the key, guess the key, compel the key, exploit a flaw in the encryption software, access plaintext while the device is in use, and locate another plaintext copy,'[114] each option however presents different practical, technological and legal hurdles.[115]

A recourse for law enforcement and security and intelligence agencies in South African law is to 'compel the key'.[116] RICA 2002 provides a legal framework for compelled decryption by (a) disclosure of the decryption key; or (b) provision of decryption assistance[117] to obtain access to the encrypted information or to put that encrypted information in an intelligible form.[118] These powers anticipate, at the very least, that the potential disclosure of information may incriminate the suspect/target to whom a compelled decryption order is directed. As such, compelled decryption directions inevitably engages the constitutional right against self-incrimination, and the difficult legal question of when would enforcement of such decryption direction violate such right.

The issues are complex. Where a suspect/target refuses or fails to comply with compelled decryption, does subsequent prosecution and conviction violate the constitutional right against self-incrimination? Where a suspect/target complies with compelled decryption for access to information that may be incriminating, does subsequent use of that information in criminal proceedings violate the right against self-incrimination? These are keys issues addressed in chapter 4.

---

[112] 'Password recovery speeds: How long with your password stand up' (2016) available at *http://www.lock down.co.uk/?pg=combi*, accessed 17 October 2016 and 'Some notes on big numbers' *http://www.quadibloc. com/math/bignum.htm*, accessed 17 October 2016. For example, a 15-character, all lower-case password has 1.6 sextillion combinations and would take in excess of 50,000 years of brute-force to decipher. An 8-character complex password has 7.2 quadrillion combinations and will likely be cracked in less than 84 days.
[113] OS Kerr & B Schneider 'Encryption workarounds' (2018) 106 *Georgetown LR* 989 at 1000.
[114] Ibid at 991.
[115] Ibid at 996-1011.
[116] Although, the South African Law Reform Commission identified encryption as a key challenge of new technologies in its review of the IMP Act 1992, no proposals addressed this issue in its final recommendations in the proposed Interception and Monitoring Prohibition Amendment Bill 1999. See South African Law Commission (Project 105) Review of Security Legislation Discussion Paper *The Interception and Monitoring Prohibition Act 127 of 1992* (1998) and South African Law Commission (Project 105) Review of Security Legislation Report *The Interception and Monitoring Prohibition Act 127 of 1992* (1999).
[117] Section 29(1)*(a)* and *(b)*.
[118] Section 29(2).

(b) Electronic Communications and Transactions Act 25 of 2002

An assessment of the treatment of electronic evidence in South African law gives weight to the statement that 'electronic evidence is undeniably problematic.'[119] In one South African work on the law of evidence, the authors remarked: 'In leaving paper, we have also left almost all guarantees of authenticity and reliability ….'[120] The concerns of electronic evidence as with other types of evidence, relate to concerns about authenticity and integrity such as ease of manipulation, destruction, deletion, alteration or fabrication (accidental or otherwise). With electronic evidence, there are added concerns that the evidence can also be modified without obvious signs of changes made.[121] Sometimes the simplest act of switching on/off a computer or device can result in loss of information.[122] The treatment of electronic evidence in South African law can be traced to 1976, and has since tested both the judiciary and the process of legislative reform, in particular in the South African law of evidence.

(i) Background: Computer Evidence Act 57 of 1983

The first reported case, a civil matter, in which the Appellate Division held that printouts of bank records generated by a computer would not be admissible, is our starting point. Prior to the ECT Act 2002, electronic evidence in South African law was regulated by Computer Evidence Act 57 of 1983.[123] The Act was enacted in response to the difficulty created by *Narlis v South African Bank of Athens*.[124] Notably twenty-six years before the ECT Act 2002 was enacted, *Narlis* is regarded as the one of the first cases in South African law demonstrating the need for legislative reform in view of technological advancements.

The Appellate Division held that a computer printout cannot be received as evidence under the provisions of section 34 of the Civil Proceedings Act 25 of 1965.[125] The application of the CPA 1965, drafted before the emergence of computers became widespread, raised questions about whether the definition of 'document' in the Act was wide enough to include computer generated documents. Section 33 of the CPA 1965 defined 'document' to include

[119] J Hofman 'South Africa' in S Mason (ed) *Electronic Evidence: Disclosure, Discovery and Admissibility* (2007) 459 at 459.
[120] Attributed to CWH Schmidt & DT Zeffertt *Evidence* para 133 as quoted in Hofman op cit note 119 at 459.
[121] South African Law Commission Issue Paper 26 (Project 126) *Electronic evidence in criminal and civil proceedings: Admissibility and related issues* (2010) at 9.
[122] Gillespie op cit note 9 at 339.
[123] Hereafter 'CEA 1983'. In addition to the Civil Proceedings Evidence Act 25 of 1965 and the Criminal Procedure Act 51 of 1977.
[124] 1976 (2) SA 573 (A).
[125] Hereafter 'CPA 1965'.

'any book, map, plan, drawing or photograph' and on a literal reading too restrictive to encompass computer generated documents. Section 34(1) of the CPA 1965 provides that 'in any civil proceedings where direct or oral evidence of a fact would be admissible, *any statement made by a person in a document* intending to establish the fact, shall on production of the original document be admissible as evidence of that fact' provided that certain conditions are present.[126] With specific reference to ss (1) of 'any statement made by a person in a document', the Appellate Division held that the computerised bank statements could not be admitted in terms of this section as the statements were not made 'by a person' as contemplated by the Act. Holmes JA stated: 'it is essential to note that sec. 34(2) deals only with such a statement, as referred to in sub-sec. (1). And straightaway ones finds that sub-sec. (1) refers only to "any statement made by a *person* in a document" (my italics). Well, a computer, perhaps, fortunately, is not a person.'[127] Foreseeing the challenging nature of the outcome, Holmes JA rightly remarked '[t]his is perhaps a matter which might well engage the attention of the Legislature in South Africa.'[128]

The decision of the Appellate Division caused 'much consternation', particularly in the banking industry at the time which placed extensive reliance on usage of computers.[129] Following the outcome of *Narlis*, the Clearing Bankers Association of South Africa requested the South African Law Reform Commission to investigate the need for specific legislation regulating the admissibility of computer-generated evidence in civil proceedings. In April 1982, the Law Reform Commission's report on '*Admissibility in civil proceedings of evidence generated by computers*' was presented to the Minister of Justice.[130] During 1983 the CEA 1983 was passed, largely based on the draft Bill proposed by the Law Reform Commission. At the time of its enactment, the CEA 1983 was recognised as going 'some way in overcoming the restrictions that the hearsay rule of evidence [placed] on the admissibility of computer print-outs as evidence.'[131] However, in terms of application, the CEA 1983 did not apply to criminal proceedings,[132] evident from the preamble which read: 'to provide for the admissibility in civil

[126] As set out in s 34(1)*(b)*. Two conditions are stipulated: (a)the person who made the statement either had personal knowledge of the matters dealt with in the statement; or (b) where the document in question is or forms part of a record purporting to be a continuous record, made the statement (in so far as the matters dealt with therein are not within his personal knowledge) in the performance of a duty to record information supplied to him by a person who had or might reasonably have been supposed to have personal knowledge of those matters.
[127] Supra note 124 at 577.
[128] Supra note 124 at 578.
[129] *S v Mashiyi and Another* 2002 (2) SACR 387 (Tk) at 390.
[130] South African Law Commission (Project 6) Review of the Law of Evidence (1982).
[131] *Mashiyi's* case supra note 129 at 390.
[132] In a 1986 report, the South African Law Commission considered whether scope of the CEA 1983 should be extended to criminal proceeding, however deferred any outcome pending further work (see South African Law

proceedings of evidence generated by computers and for matters connected therewith.' By its application only in civil proceedings, the CEA 1983 therefore did not overcome problems faced by the courts relating to the admissibility of computer printouts in terms of s 34 of the CPA 1965, as held in *Narlis*, insofar as criminal proceedings were concerned.[133]

The CEA 1983 also caused numerous difficulties, specifically due its overly cumbersome technical requirements in relation to printouts. Section 3(1) of the Act provided that an 'authenticated computer printout [was] admissible on its production as evidence of any fact recorded in it of which direct oral evidence would be admissible.' Collier provides a succinct summary on the impact of the requirements of the Act:

> '"Authenticated" meant that the printout must be accompanied by an authenticating affidavit and other supplementary affidavits necessary to establish the reliability of the information contained in the printout. The court could attach as much or as little evidential weight to the printout as the circumstances of the case dictated (s 4). The Act required that the deponent to the authenticating affidavit had to be a person qualified to depose thereto in two respects (s 2(3)). First, by reason of his knowledge and experience of computers and the particular system in question; and, secondly, in respect of his examination of all relevant records and facts concerning the operation of the computer and the data and instructions supplied to it. The records and facts had to be verified by him if he had control of or access to them in the ordinary course of his business, employment, duties or activities (s 2(4)(a)). If not, then a supplementary affidavit was required from a person who had control of or access to them (s 2(4)(b)). Records and facts were sufficiently verified if the deponent stated that, to the best of his knowledge and belief, they comprised all the relevant records and facts.'[134]

In *Ex Parte Rosche*,[135] the CEA 1983 was heralded as a 'facilitating Act not a restricting one.'[136] The relevant evidence was a telephone company's computer printouts which were automatically generated recording details of telephone calls, in this case the printouts reflected information of telephone calls made from a hotel in Mozambique to a guest house in South Africa. Although the provisions of the CEA 1983 were not met, the court accepted the printouts

---

Commission Discussion Paper 99 (Project 108) *Review of the law of evidence* (1986)). The Law Commission published a discussion paper dealing with computer-related crime in 2001 (see South African Law Commission Discussion Paper 99 (Project 108) *Computer related crime: preliminary proposals for reform in respect of unauthorised access to computer, unauthorised modification of computer data and software applications and related procedural aspects* (2001)). Further legislative reform proposals by the Law Commission were subsequently superseded by the enactment of the ECT Act 2002.

[133] *Mashiyi's* case supra note 129 at 390.

[134] DW Collier 'Electronic evidence and related matters' in PJ Schwikkard & SE van der Merwe *Principles of Evidence* 3ed (2009) at 412.

[135] [1988] 1 All ER 318 (W).

[136] Supra note 135 at 328.

as real evidence and held them admissible[137] 'in the sense that it came about automatically and not as a result of any input of information by a human being' and with 'no room for dishonesty or human error.'[138]

(ii) Law of Evidence Amendment Act 45 of 1988

Could the provisions of the Law of Evidence Amendment Act 45 of 1988[139] offer any potential assistance to admissibility of computer generated documents? Although the provisions of the Act 'radically impacted on the application of the common law of hearsay'[140] a view expressed at the time was that the LEA Act 45 of 1988 was 'of little or of no assistance in regard to the acceptance of computer print-outs which contain processed information as evidence.'[141] The reasoning was based on the provision of s 3(4) which defined 'hearsay evidence' to mean 'evidence, whether oral or in writing, the probative value of which depends upon the credibility of any person other than the person giving such evidence.' This referred to the rationale in *Narlis* that 'a computer is not a person and the logic expressed in that case in excluding computer print-outs as evidence for reason of them not being statements made by a person applies equally to s 3(4) of Act 45 of 1988.'[142]

The only possible vehicle which could allow the admissibility of computer generated documents as evidence in criminal proceeding is s 221 of the Criminal Procedure Act 51 of 1977.[143]

---

[137] The trustworthiness and reliability of the printouts was established with the following evidence: (a) the information in handwritten records of the calls—they were carbon copies of the chits prepared by the telephone operator on duty at the hotel on the day in question, reflected the same information as in the printouts (although the operator could not be traced to give evidence) (at 326); (b) evidence of the functional workings of the telephone recording equipment was adduced (at 328); (c) evidence of the reliability of the information contained in the printout and similar printouts as being "accepted by both the telephone company and its subscribers as being correct over a number of years" (at 328); (d) information concerning the software qualities, namely (i) the software in this case did not generate random impulses as in the case of games; and (ii) it did not do creative interpretation of input as when virtual reality is created from an architect's plan (at 329).

[138] *Ex parte Rosche* supra note 135 at 326. The court likened the printout in the present case as similar to the radar diagram produced in the English case of *The Statue of Liberty: Owners of the Motorship Sapporo Maro v Owner of Steam Tanker, Statue of Liberty* [1968] 2 All ER 195 (PDA) where such a document was admitted as evidence.

[139] Hereafter 'CPA 1965'.

[140] *Mashiyi's* case supra note 129 at 390.

[141] Supra note 129 at 390.

[142] Supra note 131 at 390-91.

[143] Hereafter 'CPA 1977'.

(iii) Criminal Procedure Act 51 of 1977

Admissibility of computer printouts in criminal proceedings is based on s 221 (business records) and s 236 (banking records) of the CPA 1977. Section 236 allows for the admissibility of accounting records and documents in the possession of a bank, including a computer printout or device that recorded or stored the document,[144] subject to the requisite supporting affidavits,[145] including an affidavit by a person stating that (a) they are in the service of the bank; (b) such accounting records and documents are the records of the bank; (c) the said entries or documents have been made compiled, printed or obtained in the usual and ordinary course of the business of the bank; and (d) such accounting records or documents are in the custody or under the control of such bank. Specifically, s 221 which provides that 'in criminal proceedings in which direct oral evidence of a fact would be admissible, *any statement contained in a document* and tending to establish that fact shall, upon production of the document, be admissible as evidence' provided that certain conditions are present.[146] The definition of 'document' in s 221(5) 'includes any device by which information is recorded or stored' and '"statement" includes any representation of fact whether made in words or otherwise.' The CPA 1977 does not provide a definition of record.

In *S v Harper*,[147] the scope and meaning of s 221 was considered in relation to admissibility of computer printouts. The court considered the question as to whether a computer printout is a document within the ordinary grammatical meaning of 'document' in s 221(5). Milne J held that 'the computer printouts consist of typed words and figures and would, prima facie, clearly fall within the ordinary meaning of the word "document".'[148] On the question of whether the computer itself, as a device or machine, would fall under the extended meaning of the definition of 'document' in s 221(5), Milne J stated:

> 'In my view, if the computer print-outs [in dispute] are 'documents' within the ordinary grammatical meaning of that word, then they are admissible. If they are not, then, in my view, they are inadmissible. … Computers do record and store information but they do a great deal else. … *The extended definition of "document" is clearly not wide enough to cover a computer, at any rate where the operations carried out by it are more than the mere storage or recording of information.* Quite apart from that, however, how would the document, that is in this case

[144] In terms of s 236(6), '"document" includes a recording or transcribed computer printout produced by any device by means of which information is recorded or stored.'
[145] Section 236(1) and (2).
[146] As set out in s 221(1)*(a)* and *(b)* (emphasis added).
[147] 1981 (1) SA 88 (D).
[148] Supra note 147 at 96.

the computer, be produced? Even if the section could be interpreted to mean that what must be produced is that part of the computer on which information is recorded or stored, that would mean the tape or disc on which it was stored, and this would be meaningless unless the electronic impulses on that tape or disc were to be translated or transcribed into a representation or statement intelligible to the ordinary human eye - or perhaps ear.'[149]

Milne J continued:

'The section does not refer to the product of the device, nor does it refer to any document produced by the device, it refers to the document itself being produced. The section does not refer to the product of the device, nor does it refer to any document produced by the device, it refers to the document itself being produced. The wording of the section, read with the extended definition contained in ss (5), is entirely appropriate to the production of microfilm as evidence since the microfilm itself can be produced. Furthermore microfilm is a means by which information is stored, and recorded. No process other than storage and recording is involved so far as I am aware.'[150]

It is not surprising that the above dictum in *Harper* was interpreted to mean that if a computer performed 'operations' beyond 'the mere storage or recording of information' then the output of those operations, such as a computer printout of information sorted and collated, would be inadmissible.[151] In principle, this meant the admissibility of computer generated information under s 221 of the CPA 1977 was only applicable in instances where the computer was merely recording or storing information. As such certain statements in the *Harper* case, were based on a misreading of the judgment of the court. This interpretation was relied on by the defence in *S v De Villiers*,[152] arguing for the inadmissibility computer printouts of bank statements. In addition, the defence arguments strongly relied on academic commentary at the time where the learned authors in Hoffmann and Zeffertt,[153] based on *Harper* stated: 'a computer printout will not be admissible in terms of s 221.'[154] Supported by the dictum, the authors further stated: 'In other words, a computer printout produced by a computer that sorted and collated information would be inadmissible.[155] This interpretation was rejected by O'Linn J, who held the computer printouts of bank statements admissible:

[149] *Harper's* case supra note 147 at 95 (emphasis added).
[150] Supra note 147 at 95.
[151] See commentary in A St O Skeen 'Evidence and computers' (1984) 101 *SALJ* 675 and LH Hoffmann & DT Zeffertt *South African Law of Evidence* 4ed (1988) at 142.
[152] 1993 (1) SACR 574 Nm.
[153] Hoffmann and Zeffertt op cit note 151 at 142.
[154] *De Villiers'* case supra note 152 at 577.
[155] Supra note 152 at 577.

> 'In my respectful view, the learned authors misread the dictum of Milne J. The learned Judge never held that "a computer print-out will not be admissible in terms of s 221" and that a computer print-out produced by a computer that sorted and collated information would be "inadmissible". The words of Milne J quoted supra and relied on by the learned authors, dealt with the question whether the computer itself, the machine, would fall under the extended definition of "document" in ss (5) of s 221 of the Criminal Procedure Act, which includes in the definition of document – "any device by means of which information is recorded or stored". Milne J in fact held that computer print-outs were 'documents' as contemplated by s 221 and were admissible.'[156]

As correctly pointed out by O' Linn J, the dictum of Milne J was misread and that a general statement based on *Harper's* case, to the effect that 'in other words a computer print-out produced by a computer that sorted and collated information would be inadmissible' was incorrect. As a Namibian case and therefore not binding on South African courts, Miller J in *S v Mashiyi and Another*[157] took a different view to O' Linn J in *De Villiers'* and held that the 'decision in *Harper's* case was at the time of its making clearly correct' and was 'accepted as being so.'[158] The case concerned the admissibility of documents 'which were generated or compiled by the Medscheme computer system which were retrieved from the Medscheme computer system for purposes of this trial.'[159] The business of Medscheme in the procedure it followed in respect of claims received, processed and paid, was in two ways, electronically or written or printed on paper. In the matter before trial, the court was only concerned with 'so-called' paper claims received by mail and processed by clerks in the assessing department, which depending on the claim, which also involved an assessor who captured information on the computer, and the computer then made the calculations regarding the amount to be paid to the service provider:

> 'The documents in dispute are all computer print-outs. Unlike the documents which are not in dispute, which documents are also computer print-outs, but which merely contained information which has been obtained from original paper documents and stored in the computer system, the disputed documents contain information which has been processed by the computer. The information contained in the disputed documents has been obtained after

[156] Supra note 152 at 577.
[157] *Mashiyi's* case supra note 129.
[158] Supra note 129 at 392.
[159] Supra note 129 at 388.

> treatment by arrangement, sorting, synthesis and calculation by the computer. It is not only information that has been retrieved and stored from other documents or any other source.'[160]

With the acknowledgement that 'there have been no statutory developments relating to the admissibility as evidence of computer generated information, in criminal proceedings since *Harper's* case'[161] Miller J concluded that he was 'therefore unable, in terms of the prevailing law to admit as evidence the disputed documents which contain information that has been processed and generated by a computer.'[162] The ruling on the admissibility of computer generated documents as evidence during a criminal trial exposed a serious lacunae in the South African law. Miller J further added his 'voice to the call that this lacunae in our law be filled and for new legislation relating specifically to computer evidence in criminal cases be considered and promulgated.'[163]

The court in *S v Ndiki and Others*[164] observed that '[t]his resulted in the issue regarding the admissibility of computer generated documents being approached from the wrong premises.' On a reading of the *Harper* judgment, this is the correct interpretation. With reference 'to the question as to whether or not a computer print-out is a document within the ordinary grammatical meaning of that word', Milne J in *Ndiki* concluded that the computer printouts are documents within the meaning of 'document' in s 221(5)[165] and proceeded to establish whether the conditions set out in s 221(1)*(a)* and *(b)* were met:

> 'It seems to me necessarily envisaged that, because of the development of modern commerce and the necessity to store records relating to large sums of money and large numbers of people, special provisions would have to be made making evidence admissible that would not be able to be subject to the ordinary rigorous test of cross-examination. In so doing the Legislature has, in addition to stipulating compliance with the above pre-requisites [in terms of s 221(1)*(a)(b)*], also enjoined the matters which are to be taken into account in estimating the weight to be attached to the statements, and I refer to the provisions of ss (3).'[166]

---

[160] Supra note 129 at 388-90.
[161] Supra note 129 at 393.
[162] Supra note 129 at 393.
[163] Supra note 129 at 393.
[164] 2008 (2) SACR 252 (Ck) at 260.
[165] *Harper's* case supra note 147 at 97: 'It seems to me, therefore, that it is correct to interpret the word "document" in its ordinary grammatical sense, and that once one does so the computer print-outs themselves are admissible in terms of s 221. Once that situation has been achieved, then it seems to me that the main thrust of the attack upon the admissibility of these documents disappears.'
[166] Supra note 147 at 97. The narrow interpretation of *Harper* was applied by Miller J in the earlier case *Mashiyi* case supra note 129, such that s 221 of the CPA 1977 was 'misread' to exclude computer printouts on the reasoning that the disputed documents contained information which had been processed by the computer.

These challenging issues, in addition the overly cumbersome technical requirements of the CEA 1983 led to growing calls for legislative reform.[167] Although initially in 1987 the South African Law Reform Commission expressed contentment with the CEA 1983, [168] in 1995 the Commission recommended its repeal.[169] Despite the recommendations of the Law Reform Commission, no new legislation on electronic evidence was forthcoming. [170] Legislative intervention eventually came, seven years later, in the form of the ECT Act 2002. The CEA 1983 was repealed in its entirety and replaced with the ECT Act 25 of 2002.[171] Notably, the ECT Act 2002 was led through parliamentary processes by the Department of Communications. Although the Department of Justice and Constitutional Development[172] took part in the consultation process preceding the Act, it appears that neither the DoJCD nor the Law Reform Commission contributed to the evidential provisions contained in the Act.[173]

[167] Hoffmann & Zeffertt op cit note 151 at 142: '(B)ecause of what has been held in *S v Harper and Another* as regards the non-admissibility of computer print-outs in terms of s 221 of the Criminal Procedure Act 1977 (at least when the computer has processed data) there is a need for legislation that relates specifically to computer evidence in criminal cases.'

[168] South African Law Commission (Project 6) *review of the law of evidence report* (1987). At 28: 'For the present the Commission is not convinced of an immediate need for a general investigation into the effectiveness of Act 57 of 1983.'

[169] South African Law Commission (Project 95) Working Paper 60 *Investigation into the Computer Evidence Act 56 of 1983* (1985) at iv.

[170] The Law Reform Commission later turned its attention to legislative reform proposals in respect of computer crime in two papers issues: (a) South African Law Commission Issue paper 14 (Project 108) *Computer related crime: Options for reform in respect of unauthorised access to computers, unauthorised modification of computer data, and software applications, related to procedural aspects* (1998); and (b)South African Law Commission Discussion Paper 99 (Project 108) *Computer-related crime: Preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects* (2001).

[171] In terms of s 92 of the ECT 2002 the provisions of the CEA1983 are repealed in its entirety. The provisions of the Civil Proceedings Evidence Act 25 of 1965 and the CPA 1977 remain relevant and may be used to assist with the admissibility of particular types of electronic evidence, such as trade or business records

[172] Hereafter 'DoJCD'

[173] Hofman op cit note 119 at 460. For details of the consultation phase, see *A Green Paper on Electronic Commerce for South Africa* (November 2000) co-ordinated and compiled by the Department of Communications, Republic of South Africa.

(iv) Chapter III of the ECT Act 2002 and corresponding Model Law on Electronic Commerce

The ECT Act 2002 is based on a resolution adopted by the General Assembly of the United Nations Commission on International Trade Law regarding electronic commerce,[174] referred to as *UNCITRAL Model Law on Electronic Commerce*.[175] Its purpose is stated as follows:

> 'The Model Law on Electronic Commerce (MLEC) purports to enable and facilitate commerce conducted using electronic means by providing national legislators with a set of internationally acceptable rules aimed at removing legal obstacles and increasing legal predictability for electronic commerce. In particular, it is intended to overcome obstacles arising from statutory provisions that may not be varied contractually by providing equal treatment to paper-based and electronic information. Such equal treatment is essential for enabling the use of paperless communication, thus fostering efficiency in international trade.'[176]

As one of sixty member states of UNCITRAL, South Africa together with other 'implementing states' sought to give effect to the MLEC by the enactment of the ECT Act 2002, which is based on the provisions of the MLEC. In terms of its preamble, the ECT Act 2002 endeavours inter alia 'to provide for the facilitation and regulation of electronic communications and transactions' and 'to promote universal access to electronic communications and transactions and the use of electronic transactions.' A key object of the ECT Act 2002 is to 'promote legal certainty and confidence in respect of electronic communications and transactions.'[177] Section 3 further provides that the Act 'must not be interpreted so as to exclude any statutory law or the common law from being applied to, recognising or accommodating electronic transactions, data messages or any other matter provided for in this Act.'

The ECT Act 2002 creates legal certainty on issues such as the validity and enforceability of electronic contracts, the time and place of contract information, and

---

[174] Hereafter referred to as 'UNICTRAL'. See United Nations Commission on International Trade Law *Model Law on Electronic Commerce with Guide to Enactment* (1996) with additional art 5bis adopted by resolution of General Assembly 51/162 of 6 December 1996 available at *https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf*, accessed 3 March 2020 (hereafter MLEC Guide to Enactment).

[175] UNCITRAL was established by the General Assembly in 1966 (Resolution 2205 (XXI) of 17 December 1966). In the establishment of the Commission, the General Assembly recognised that disparities in national laws governing international trade created obstacles to the flow of trade, and it regarded the Commission as the vehicle by which the United Nations could play a more active role in reducing or removing these obstacles. See *https://uncitral.un.org/en/about*, accessed 1 August 2019.

[176] *UNCITRAL Model Law on Electronic Commerce* (1996) available at *http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html*, accessed 1 August 2019.

[177] Section 2*(e)*.

formalities such as 'writing', 'signature' and 'original'.[178] In doing so, it promotes the objectives of the MLEC, which include enabling or facilitating the use of electronic commerce and providing equal treatment between paper-based documentation and computer-based information.[179] This is referred to as a 'functional equivalence' approach.[180] In a lucid approach, functional equivalence recognises differences in use of traditional paper-based documentation and its computer-based equivalent. In doing so, the functional equivalence approach regulates the 'functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques.'[181] Specifically, the functional equivalent approach has been taken in articles 6 to 8 of the MLEC with respect to the concepts of 'writing', 'signature' and 'original', which correspond similarly in ss 12, 13 and 14 of the ECT Act 2002.

Chapter III of the ECT Act 2002 explicitly deals with the law of evidence, specifically s 15 under the heading 'admissibility and evidential weight of data messages'. The term 'electronic evidence' is not referred to in any law governing the admissibility of evidence. As with the MLEC, the ECT Act 2002, refers to the output of information by/in an electronic medium as 'data message' or 'electronic transaction'. To the extent appropriate these terms will be used interchangeably with the preferred term 'electronic evidence' as an all-encompassing term, broad enough to reflect information in its electronic form or medium as being generated or stored by a computer or other device.[182] The corresponding equivalent of s 15 of the ECT Act 2002 in the MLEC is article 9. The functional equivalence approach, we are told, does not apply to s 15/article 9: 'A data message, in and of itself, cannot be regarded as an equivalent of a paper document in that it is of a different nature and does not necessarily perform all conceivable functions of a paper document.'[183] Does this make the ECT Act 2002 less effective in its treatment of electronic evidence? If the conclusion to be drawn is that

[178] The long title of the ECT Act 2002 provides: 'To provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy for the Republic; to promote universal access to electronic communications and transactions and the use of electronic transactions by SMME's [small, medium and micro-enterprises]; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-government services; and to provide for matters connected therewith.'
[179] MLEC Guide to Enactment op cit note 174 at 17.
[180] Ibid at 20-21.
[181] Ibid at 20.
[182] Adapted from Mason's definition of 'electronic evidence' as 'data (compromising the output of analogue devices or data in digital format) that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system that is relevant to the process of adjudication. See S Mason 'Sources of digital evidence' in S Mason (ed) *Electronic Evidence: Disclosure, Discovery and Admissibility* (2007) para 2.03.
[183] MLEC Guide to Enactment op cit note 174 at 21.

electronic evidence with specific reference to the admissibility and evidential weight provisions in s 15 of the ECT Act 2002 'cannot be regarded as an equivalent of a paper document *in that it is of a different nature*',[184] should stricter standards for admissibility, generally, and in the context of authenticity and integrity apply to electronic evidence in contrast to traditional paper-based documentation?

In an alternative consideration, if the objective is to create a 'media-neutral environment'[185] such that there is no discrimination or disparity in the treatment of traditional paper-based documentation and its computer-based equivalent,[186] then surely the functional equivalence approach should apply to the s 15 evidential provisions with reference to 'data messages' as electronic evidence? Hofman observes: '[t]here is little point in making a data message legally effective in the same way as a document if the data message cannot be used as evidence in the same way.'[187] The need for a more balanced approach is reflected in s 4(2)*(a)* of the ECT Act 2002 which reads[188]: '[t]his Act must not be construed as requiring any person to generate, communicate, produce, process, send, receive, record, retain, store or display any information, document or signature by or in electronic form.' The MLEC is explicit in its objective and approach. The legal recognition of those situations where parties opt to use electronic means 'merely indicates that the form in which certain information is presented or retained cannot be used as the only reason for which that information would be denied legal effectiveness, validity or enforceability [and] should not be misinterpreted as establishing the legal validity of any given data message or of any information contained therein.'[189] In terms of implications for the South African courts interpreting the provisions of the ECT Act 2002, specifically chapter III on evidence, potentially a court should interpret the Act such that its provisions on electronic evidence is the functional equivalent of laws governing other forms of evidence, such as traditional paper-based documentation.[190]

In terms of its application and its provisions for general admissibility does the ECT Act 2002 make all data messages, and therefore all electronic evidence, admissible? If so, does this mean that electronic evidence is exempt from the exclusionary rules of evidence? If the ECT Act 2002 does not make all electronic evidence admissible, then establishing the relationship

[184] Ibid (emphasis added).
[185] Ibid at 17.
[186] Ibid at 31.
[187] Hofman op cit note 119 at 461-2.
[188] Ibid.
[189] MLEC Guide to Enactment op cit note 174 at 31.
[190] Hofman op cit note 119 at 462.

between chapter III of the ECT Act 2002 and other laws governing the admissibility of evidence is therefore important for understanding the provisions s 15 of the ECT Act 2002. Further, the ECT Act 2002 does not make a distinction between records of a computer that simply stored or recorded information, and records of 'operations' performed by a computer beyond 'the mere storage or recording of information.' Does this distinction fall away as means of facilitating the admissibility of electronic evidence because – arguably, s 15 makes all electronic evidence admissible? These are key issues considered in chapter five of the thesis.

CHAPTER TWO

INTERCEPTION OF COMMUNICATIONS

I INTRODUCTION

This chapter is about interception of communications. The chapter will explore in Part II the legal framework for interception in the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2000,[1] including circumstances in which lawful interception can take place, authorisation procedures and the protection of privacy interests through prohibiting unlawful interceptions. Part III deals with existing challenges in the legal framework of RICA 2002. The key challenges identified are twofold: (a) the scope and breadth of investigative powers by law enforcement and the security and intelligence agencies; being (b) unconstrained by out-dated legislative frameworks that have expanded the scope of their activities and the extent of their capabilities in an information age of innovations in technology. The RICA 2002 has been the subject of legal challenge and Part IV considers the future of interception of communications in South Africa. A conclusion is drawn in Part V.

II REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT 70 OF 2002

(a) The meaning of interception

RICA 2002 describes the process of interception as one by which a person monitors, views or diverts a communication in the course of its transmission 'so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication.'[2] The meaning of 'intercept' is important. It includes the 'acquisition of the contents of any communication' through the 'monitoring' of a communication, the 'viewing' of the contents and the 'diversion' of an 'indirect communication from its intended destination to any other destination.'[3] Central to the definition of intercept is the acquisition of the *content* of the communication and to make *all*

[1] Hereafter 'RICA 2002'.
[2] Section 1.
[3] Ibid.

or some of the content available to a person other than the intended recipient or sender. Therefore, it is not necessary that the entire contents of a communication is intercepted, and partial disclosure will also be covered by the legal provisions of RICA 2002. It is important to note that core to the relevant provisions regulating interception is the *contents* of the communication. The definition of 'contents' is stated as 'when used with respect to any communication, includes any information concerning the substance, purport or meaning of that communication.'[4] Information about the communication, known as communications data, such as the IP address of geolocation data can assist to identify or provide the location of the sender/recipient. The acquisition of this type of data by law enforcement and the security and intelligence agencies is considered in chapter 3. It is important to note that use of this type of data is not an interception as envisaged by ss 2-11.

(b) Unlawful interception

Any interception of communications outside of RICA 2002 would be unlawful, and the Act specifically criminalises unlawful interception.[5] It prohibits the intentional interception or authorisation of an interception of any communication in the course of its occurrence or transmission. Section 2 constitutes the key provision in this regard and prescribes prohibition of unlawful interceptions. This means that no person may intentionally intercept or attempt to interception any communication in occurrence or transmission by using interception or monitoring devices. All activity that monitors the traffic on a telecommunication system is covered by s 2 in terms of prohibition of interception. To monitor means to record communications, including the mere fact that a communication was sent or a site visited.[6] The definition of 'communication' is stated to 'include both a direct communication and an indirect communication.' Indirect communications include a message or a part thereof in the form of data, text, visual images (text or symbols) in the subject line, text or symbols in filling in recipient's address and any other form or combination of forms.[7]

[4] The term 'contents' in relation to any communication 'includes any information concerning the substance, purport or meaning of that communication.' The term 'communication' is defined to include 'both a direct communication and an indirect communication'.
[5] Chapter 9, s 47-57.
[6] Section 1.
[7] Section 1. This definition is adopted directly from the Interception and Monitoring Prohibition Amendment Bill 1999, referred earlier in chapter 1 as proposed by the South African Law Reform Commission. Whereas the Law Reform Commission proposed this as the definition of 'communication' (clause 1*(b)*), RICA 2002 has adopted verbatim the definition of 'communication' as 'indirect communications'. See South African Law

The prohibition in s 2 refers to the interception of communications 'in the course of its occurrence or transmission.' This is the key part of the offence. On the issue of 'in the course of its occurrence or transmission' in what circumstances is it considered an interception? If law enforcement and security and intelligence agencies 'view or hear' the content of a communication after it has reached the intended recipient, or even at the same time as the recipient, does this amount to interception?[8] By reference to the wording in s 2 'in the course of its occurrence or transmission' the answer is that it is not an interception.[9] Is it the case that interception is only when the communication is 'moving' or transient, that is, literally listening during a call or intercepting as a voice message was being left for the recipient or reading an email after the sender has 'hit send' as the communications are 'in the course of its occurrence or transmission?' In other words, once a voice message has reached a recipients' voicemail or an email has reached the recipients' inbox (but not yet accessed), there can be no interception because the course of 'occurrence or transmission' of the communication has been completed?[10] RICA 2002 addresses such situations where a communication is awaiting in a stored space until it accessed by the intended recipient. For example, a voice message or email communication that is awaiting in a stored system for the intended recipient to access is considered to be 'in the course of its occurrence or transmission' and thus capable of being intercepted.

The offence of unlawful interception in s 2 must be read in conjunction with s 1(2)*(a)* of RICA 2002 which extends the meaning of interception 'if and only if' the interception is effected in the case of – (i) a direct communication, in the course if its occurrence; or (ii) an indirect communication, in the course of its transmission; and s 1(2)*(b)* that the time which an indirect communication is being transmitted includes '*any time* when the telecommunication system *by means* of which such indirect communication is being, or has been, transmitted is used *for storing it in a manner than enables the intended recipient to collect it or otherwise have access to it*.'[11] In other words, specifically s 1(2)*(b)* has the effect of applying to messages, such as voice messages, stored and awaiting to be accessed by the intended recipient. The

Commission (Project 105) Review of Security Legislation Report *The Interception and Monitoring Prohibition Act 127 of 1992* (1999).

[8] AA Gillespie *Cybercrime: Key Issues and Debates* (2019) at 81.

[9] See *R (on the application of NTL) v Crown Court at Ipswich* [2003] QB 131 (UK).

[10] See *R v Coulson et al* [2014] EWCA Crim 1119 (UK) at 1133 where the Court of Appeal rejected arguments that there could not be interception, and noted that the applicable legislation did not have a time limit on interception, or that any storage of the communications had to be transient for interception to apply or have any restrictions that such communications could only be read or heard once.

[11] Emphasis added.

section expressly mentions communications stored on a telecommunication system, including those made after transmission. Therefore, accessing those stored communications that have not yet been accessed by the intended recipient amounts to interception within the prescripts of RICA 2002 where they are accessed by someone else.

Reference to 'by means of a postal service or telecommunication system' reflects the technicalities of interception at the time RICA 2002 was enacted into law, when postal services were the commonly used means of communication, and telephones used mainly for calls and voice messages. The technicalities of how law enforcement and security and intelligence agencies, in the era of the information age, intercept communications have changed significantly since the early 2000s. Interception is no longer limited to letters via postal services, landline telephones, voice messages on answering machines or basic mobile phone technology. Emails, instant messaging applications such as WhatsApp, and social networking sites, which allow both voice and video calls, are now mainstream and dominant means of communication. Much has been made of the concept of 'technology neutrality' and recognition of the fact that technology advancements, now in the information age evolves far too rapidly for technology-specific legislation. It is for this reason, probably, that parliament deliberately did not define 'electronic' or 'computer' or other technology-specific definitions in RICA 2002, and why the Act has remained in operation for more than eighteen years.[12]

The risk that the law would always fall behind the pace of technology because of the time required to amend existing legislation, or introduce new legislation, is undoubtedly a constant challenge for lawmakers, especially in the context of electronic evidence in criminal proceedings. The time for law reform and review of RICA 2002, eighteen years since coming into law, is now long overdue. In choosing the most appropriate and effective solutions in law to technological advancements in the information age, it is important that the legislation remains dynamic, and in leaving it to the courts, could be applied dynamically.[13] Walden proposes two variants of the principle of technology neutrality that will need to be considered: (a) to the extent 'that which is regulated offline should be regulated online'; and (b) the need to treat different types of technologies in a similar manner to the extent that they perform to

[12] See EURIM submission to the APIG Report on Communications Data (January 2003) as quoted in I Walden *Computer Crimes and Digital Investigations* (2007) at 60: '[t]he moment you try and do definitions which rely on some kind of implicit technology model, then you know that those definitions are doomed, certainly within ten years and probably within five.'
[13] Gillespie op cit note 8 at 3, 80-81.

the same effect.[14] As regards the former, this could potentially be the 'functional equivalent'[15] approach in the use of traditional paper-based documentation and its computer-based equivalent referred to in chapter 1 earlier.

However, a criticism of a technology neutral approach in terms of criminal procedure and evidence is that traditional notions of content (interception) and communications data, such that the latter is considered less intrusive than the former, is problematic and no longer sustainable in a year 2020 information age. The technology neutral approach of RICA 2002 now means that law enforcement and the security and intelligence agencies have access to significant amounts of sensitive and revealing information, but under less protection than that of accessing the contents of information. This is a worrying trend. A failure to recognise the unique features of advancements in technology by applying historical distinctions have been noted by Hosein and Pascal: '[a]ttempts to be technology-neutral should be interrogated, lest in our blindness we reduce democratic protections and oversight under the deterministic veil of progress.'[16] The RICA 2002 has been the subject of a successful constitutional legal challenge.[17] If South African lawmakers in updating the legislative frameworks in RICA 2002, insist on applying traditional investigative powers to new technologies through the continued adoption of technology-neutrality principles, it is important they recognise that state access to significant amounts of information is now the norm and stronger protections of privacy interests should be applied.[18]

(c) Lawful authority for interception

In terms of s 49(1) of RICA 2002: 'Any person who intentionally intercepts or attempts to intercept, or authorises or procures any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission, is guilty of an offence.' Sections 3-11 of RICA 2002 provide exceptions to the prohibition on

[14] Walden op cit note 12 at 60. See also B-J Koops ' Should ICT regulation be technology neutral' in B-J Koops et al (eds) *Starting Points for ICT Regulation* (2006) 77-108.
[15] *UNCITRAL Model Law on Electronic Commerce* (1996) available at *http://www.uncitral.org/uncitral/en/ uncitral_texts/electronic_commerce/1996Model.html*, accessed 1 August 2019.
[16] I Hosein and A Pascual 'Understanding traffic data and deconstructing technology-neutral regulations (2002) at available at 8 *http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=55CB1A20C3B31F16872328C4273EED 75?doi=10.1.1.475.5291&rep=rep1&type=pdf*, accessed 12 March 2020.
[17] Press release 'AmaB challenges snooping law' 20 April 2017 available at *https://amabhungane.org/advocacy/advocacy-amab-challenges-snooping-law/*, accessed 19 June 2019.
[18] This issue is also considered further in chapter 3 analysis of communications data under the heading 'the envelope is the content'.

interception and monitoring of communications, whereby in certain instances, interception of communication is: (a) permitted under an interception direction (s 3); (b) by an individual/law enforcement officer who is a party to the communication (s 4); (c) by prior consent of the party to the communication (s 5); (d) in the course of carrying on with business (ss 6 and 10); (e) to prevent serious bodily harm (s 7); (f) to determine a location in the event of emergency (s 8); (g) authorised by other legislation (s 9); and (h) for the purposes of managing radio frequency spectrum (s 11). Lawful authority for interception is through a warrant, referred to in RICA 2002 as an interception direction. The interception direction must be approved by a designated judge. Application to a designated judge for the issuing of an interception direction is set out in s 16-25 of RICA 2002. In terms of s 16(1) 'an applicant may apply to a designated judge for the issuing of an interception direction' which in terms of 16(5) may only be issued for specified purposes, including for the prevention and detection of 'serious offences' or in the interests of 'national security or compelling national economic interests' if the 'reasonable grounds to believe' threshold have been met.

In terms of s 1 'interception direction' is stated to mean 'a direction issued under s 16(3) or 18(3)*(a)* and which authorises the interception, at any place in the Republic, of any communication in the course of its occurrence or transmission, and includes an oral interception direction issued under s 23(7).' This is a key prescription of the legislation. The interception of communications in South African law as regulated by RICA 2002 is applicable only to domestic signal interception by express reference to '*at any place in the Republic*.' In other words, the conduct of interception is only lawful if the interception is effected solely for communications 'in the course of its occurrence or transmission' within South Africa, approved by a designated judge and for certain specified purposes. In effect, the type of interception regulated by RICA 2002 is specifically for 'targeted' interceptions.

Technological advancements have arguably blurred the distinction between domestic and foreign signals, and the technicalities of signal interception potentially mean that interception of foreign signals would capture the communications of persons sending and receiving communications within the borders of South Africa.[19] An important distinction between domestic and foreign signals could be information collected from systems such as

[19] See 'Signals intelligence' available at *https://www.globalsecurity.org/intell/library/policy/army/fm/2-0/chap8.htm*, accessed 20 March 2020. For example, 'communications intelligence' (COMINT) that involves technical and intelligence information derived from intercept of foreign communications.

radars and other weapons systems, [20] or signals detected from weapons under testing and development.[21] The key issue is the basis of lawful authority for foreign signal interception. This is because RICA 2002 only applies to domestic signal interception. If the communication to be intercepted originates outside South Africa, or passes through systems and services located outside South Africa (such as Facebook, WhatsApp or Gmail), or terminates within the borders of South Africa, even if sender and recipient are in South Africa, is there a law in South Africa regulating foreign signal interception if this is not regulated by RICA 2002?

Further, if RICA 2002 is the lawful authority for 'targeted' interceptions as approved by a designated judge and for certain specified purposes, what is the lawful authority for 'bulk' interceptions in South Africa? The position of privacy and civil liberties groups is that there are no laws regulating foreign signal interception and bulk interception in South Africa. The counter argument by the state is that lawful authority for the conduct of interception of foreign signals and communications in bulk is the National Strategic Intelligence Act 39 of 1994.[22] These key issues are considered in detail further below.

III WHY SHOULD WE BE CONCERNED ABOUT THE INTERCEPTION OF COMMUNICATIONS IN SOUTH AFRICA?

RICA 2002 has been subject to significant criticisms, and recently the subject of legal challenge.[23] Underlying majority of the criticisms is a fundamental concern regarding the scope and breadth of these investigatory powers. RICA 2002 was written before the onset of a modern fast-paced environment of technological advancements in the information age dominated by connectivity, data and devices. As an inherently backward looking piece of legislation, a key challenge is that RICA 2002 has not kept pace with the gamut of technological change, and concerns identified below are intensified such that the powers of law enforcement

[20] Referred as 'electronic intelligence (ELINT). See 'Intelligence: Signals intelligence' available at *https://www.cia.gov/new s-information/featured-story-archive/2010-featured-story-archive/intelligence-signals-intelligence-1.html*, accessed 20 March 2020.
[21] Referred as 'foreign instrumentation signals intelligence' (FISINT). See 'Intelligence: Signals intelligence' op cit note 20.
[22] Hereafter 'NSI Act 1994'. See 'Interception of communication and the NCC' in Ministerial Review Commission *Intelligence in a Constitutional Democracy* 10 September 2008 Final Report to the Minster for Intelligence Services, the Honourable Mr Ronnie Kasrils MP (hereafter 'The Matthews Commission') at 180 available at *http://www.lse.ac.uk/international-development/Assets/Documents/PDFs/csrc-background-papers/Intelligence-In-a-Constitutional-Democracy.pdf*, accessed 05 January 2016.
[23] *amaBhungane Centre for Investigative Journalism NPC and SP Sole v Minister of Justice and Correctional Services and Others* Case No: 25978/2017 (16 September 2019), subject to confirmation by the Constitutional Court. See applicants' heads of argument available at *https://amabhungane.org/wp-content/uploads/2019/06/190212_amaB-heads-of-argument.pdf*, accessed 24 March 2020. See also op cit note 77 below.

and the security and intelligence agencies are 'left virtually unconstrained and unsupervised by out-dated legislative frameworks' and 'have unilaterally expanded the scope of their activities and the extent of their capabilities.'[24] In a report dated 27 April 2016, the United Nations Human Rights Committee expressed hard-hitting criticisms of South Africa's interception of communications practices under RICA 2002.[25] The Committee specifically raised concerns about 'relatively weak safeguards, oversight and remedies against unlawful interference with the right to privacy,[26] and 'reports of unlawful surveillance practices, including mass interception of communications carried out by the National Communications Centre.'[27] It was also concerned about the wide scope of the data retention regime under RICA 2002.[28] The Committee recommended that the South African government 'should take all measures necessary to ensure that its surveillance activities conform to its obligations under the Covenant, including article 17'[29] and that any interference by the state with the right to privacy comply with the principles of legality, necessity and proportionality.[30] The Committee further expressly recommended that the South African government should cease 'engaging in mass surveillance of private communications without prior judicial authorization…and consider revoking or limiting the requirement for mandatory retention of data by third parties.'[31] It was also emphasised that the state should also ensure that interception is carried out 'only according to the law and under judicial supervision.'[32] It was recommended that the state 'should increase the transparency'[33] of its legal regime and policies governing surveillance practice. Further, that it should 'speedily establish independent oversight mechanisms to prevent abuses and ensure that individuals have access to effective remedies.'[34]

---

[24] Don't Spy on Us 'Don't spy on us: Reforming surveillance in the UK' September 2014 at 10 available at *https://www.dontspyonus.org.uk/assets/files/pdfs/reports/DSOU_Reforming_surveillance.pdf*, accessed 23 February 2018. See also 'Don't Spy on Us: Response to the Inquiries into Privacy and Surveillance' September 2015 available at h*ttps://www.dontspyonus.org.uk/assets/site/dontspyonus/files/DSOU_Response _report_ WE B.pdf*, accessed 23 February 2018.

[25] United Nations Human Rights Committee 'Concluding observations on the initial report of South Africa' CCPR/C/ZAF/CO/1 27 April 2016 available at *http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Down load.aspx?symbolno=CCPR% 2FC% 2FZAF%2FCO%2F1&Lang=en*, accessed 29 February 2018.

[26] Ibid at 8 para 42.

[27] Ibid.

[28] Ibid.

[29] Article 17 of the International Covenant on Civil and Political Rights reads: '1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks' available at *http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx*, accessed 02 March 2018.

[30] United Nations Human Rights Committee op cit note 25 para 43.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Ibid.

The current framework of RICA 2002 on the investigative powers of interception is explored in this section. In the analysis, the concerns are identified as requiring essential reform necessary in South African law to protect against unlawful and arbitrary interference with the right to privacy balanced against the need to protect the capabilities of law enforcement and the security and intelligence agencies, particularly as these competing interests struggle under 'the strain of technological evolution on society.'[35] The bulk of concerns, in general, fall into the following categories: (a) interception of communications carried out by the National Communications Centre; (b) notification of interception; (c) threshold for conducting interception of communications; (d) lack of any adversarial processes; and (e) appointment of designated judges and independence.

(a) Interception of communications carried out by the National Communications Centre

The RICA 2002 provides for the establishment of interception centres, including the Office for Interception Centres.[36] The OIC is responsible for executing interception directions issued by the designated judge. The OIC operate under the prescripts of RICA 2002 'for the interception of communications in terms of this Act.'[37] This means that in terms of its operations, the OIC focuses on the interception of domestic signals within the lawful authority of RICA 2002 to be approved by a designated judge and for certain specified purposes.

A separate entity, the National Communications Centre,[38] is the state's national facility for intercepting and collecting electronic signals. The NCC, as the state's main interception facility, 'monitors the signals of 'targets' being known persons or organisations that have been identified for intelligence monitoring.'[39] It also undertakes '"environmental scanning" which entails random monitoring of signals through the Centre's bulk monitoring capability.'[40] Its capabilities thus include interception of communications, both *targeted* and in *bulk*. The NCC is currently part of the State Security Agency,[41] and by its nature operates under high levels of secrecy. The operational activities of the NCC, although not transparent or in any way or

[35] Royal United Services Institute for Defence and Security Studies *A democratic license to operate: Report of the independent surveillance review* (July 2015) available at *https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf*, accessed January 2018 at ix (hereafter 'RUSI').
[36] Hereafter 'OIC'. See RICA 2002, s 32-37.
[37] Section 32(1)*(a)*.
[38] Hereafter 'NCC'.
[39] The Matthews Commission op cit note 22 at 180.
[40] Ibid.
[41] Hereafter 'SSA', previously known as the National Intelligence Agency (hereafter 'NIA').

accountable to the public, are subject to the oversight of the Inspector-General of Intelligence.[42] What is known through oversight by the I-GI, a commission of inquiry, independent research and reports by civil liberties groups, is that bulk interception facilities located at the NCC and operated by the SSA do exist in South Africa and focus on foreign signal interception. The clients of the NCC include the South African Secret Service, the South African Police Services and the Financial Intelligence Centre.

The term 'bulk interception' commonly refers to a process of obtaining large volumes of untargeted information from a wide range of people, most of whom are unlikely to be of interest to enforcement and security and intelligence agencies. An understanding of what this means to the state was recently presented in its response to a legal challenge to RICA 2002:

> 'Bulk surveillance in an internationally accepted method of strategically monitoring transnational signals, in order to screen them for certain cue words or key phrases. The national security objective is to ensure that the State is secured against transnational threats. It is basically done through the tapping of transnational signals, including, in some case, undersea fibre optic cables. … intelligence obtained from the interception of electromagnetic, acoustic and other signals, including the equipment that produces such signals. It includes any communication that emanates from outside the borders of [South Africa] and passes through or ends in [South Africa].[43]

The investigative power of bulk interception is controversial. It is recognised that interception of communications in bulk is a vital tool to detect and contribute to the prevention of criminal activity, for intelligence and evidence gathering purposes to be able to identify threats and/or speedily establish links in criminal investigations. The associated technical process involves the use of 'equipment interference' and 'bulk equipment interference.'[44] The use of such techniques varies in complexity and scale. Equipment interference is a term used to gain covert access to information relating to a number of devices linked to 'thematic' investigations or operations.[45] 'Bulk equipment interference' is similar to 'equipment interference' but on a larger scale and performed without any known links between the

[42] Hereafter 'I-GI'. The I-GI is a state entity tasked with the oversight of intelligence services.
[43] *amaBhungane* case supra note 23 para 143, the state's response to concerns related to bulk interception in South Africa.
[44] Ibid.
[45] Home Office Gov.UK 'Fact sheet: equipment interference' 4 March 2016 available at *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/530554/Equipment_Interference_Factsheet.pdf*, accessed 21 June 2019.

targets/suspects.[46] For example, this may involve the access to information from devices in a particular location in order to identify persons of interest. Therefore, this means that most information caught by such means will be irrelevant to any criminal or national security investigation and will contain significant details about innocent individuals whom are in no way implicated in an investigation or operation. Given the intrusive nature of the acquisition of the content of communications in bulk, especially at the stage that data is selected for examination, it is imperative that any regulation of bulk interception ensure constraints on a process that would effectively allow a 'limitless number of unidentified individuals' to have their communications intercepted.[47] Regulation should also ensure that state can continue to acquire content data of communications in bulk, only when it is necessary and proportionate to do so and in full compliance with the law and under judicial supervision.

The investigative power of bulk interception therefore cannot take place without lawful authority for doing so.[48] If the 'targeted' interception of communications in South African law is regulated by RICA 2002 and is applicable only to domestic signal interception by express reference to '*at any place in the Republic*' in terms of s 16(3) or 18(3)*(a)*, what is the lawful authority for foreign signal interception and bulk interception by the NCC?

In August 2006, the then Minister for Intelligence Services, Mr Ronnie Kasrils MP established the Ministerial Review Commission on Intelligence,[49] with the aim of the review being 'to strengthen mechanisms of control of the civilian intelligence structures in order to ensure full compliance and alignment with the Constitution, constitutional principles and the rule of law, and particularly to minimise the potential for illegal conduct and abuse of power.'[50] At the time, the catalyst for the establishment of the Commission was the intelligence crisis of 2005 and 2006 involving the National Intelligence Agency[51] and indications of possible

[46] Home Office Gov.UK 'Investigatory Powers Bill: Bulk powers' 4 March 2016 available at *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/530549/Bulk_Powers_Fact sheet.pdf*, accessed 21 June 2019.
[47] See Home Office Gov.UK 'Fact sheets and guidance relating to the Investigatory Powers Bill' 4 March 2016 available at *https://www.gov.uk/government/publications/investigatory-powers-bill-fact-sheets*, accessed 21 June 2019.
[48] *Pharmaceutical Manufacturers Association of SA and Another: In Re Ex Parte President of The Republic of South Africa and Others* 2000 (2) Sa 674 (CC) para 20: 'The exercise of all public power must comply with the Constitution, which is the supreme law, and the doctrine of legality, which is part of that law.'
[49] The Matthews Commission op cit note 22.
[50] Ibid at 27 and Appendix A at 286.
[51] Hereafter 'NIA'.

misconduct and illegality of surveillance operations against a prominent businessman and political figure.[52]

The following, inter alia, was presented to the Commission on the activities of the NCC: (a) the NCC collects signals intelligence and the mandate to do so derives from s 2 of the NSI Act 1994;[53] (b) the formation of the NCC flowed from a recommendation by the Pikoli Commission in 1996 that government should establish a single, national signals intelligence facility; (c) Cabinet accepted the Pikoli Commission's recommendation to establish the NCC as a separate entity but declined to introduce legislation governing its activities; (d) in June 2008, the then Minister for Intelligence Services, Mr Ronnie Kasrils MP tabled the Intelligence Services Amendment Bill and the National Strategic Intelligence Amendment Bill,[54] which sought to provide for the establishment of the NCC and intended to ensure the legality and constitutionality of the NCC's operations.[55]

Preceding the findings of the Matthews Commission, the illegality and abuse of bulk interception powers by the NCC was documented by the I-GI:

> 'The targeting of South African individuals through the interception of their voice communications by means of the bulk scanning facilities of the National Communications Centre (NCC) was not in keeping with the practice and culture of bulk interceptions, the normal focus of which is the targeted bulk interception of foreign communications. These facilities were used in a way that constituted a gross abuse of the bulk interception facilities of the NCC and constituted a circumvention of the legal interceptions regime provided….'[56]

In its submission to the Matthews Commission, the I-GI found the following in relation to the NCC: (a) '[t]here is no legislative mandate for the NCC and electronic collection of signals; (b) [t]he regulatory framework governing the NCC's special powers is incomplete; (c) bulk interceptions are not usually subject to judicial control; and (d) [t]here is a lack of internal compliance mechanisms for operational activities.'[57] The I-GI recommended that there should

---

[52] The Matthews Commission op cit note 22 at 26, 27. See footnote 2: Office of the Inspector-General of Intelligence 'Executive summary of the final report on the findings of an investigation into the legality of the surveillance operations carried out by the NIA on Mr S Macozoma: Extended terms of reference report on the authenticity of the allegedly intercepted e-mails' media briefing, 23 March 2006, available at *www.intelligence.gov.za/OversightControl/IG%20Exec%20Summary%2023%20Mar%2006.doc*, accessed 05 January 2016.

[53] Referring to 'functions relating to intelligence' in the Act.

[54] Hereafter 'NCC Bill'.

[55] The Matthews Commission op cit note 22 at 182-84. In 2002 and 2008, Cabinet declined the opportunity to introduce legislation regulating NCC and its operational activities.

[56] Office of the Inspector-General of Intelligence op cit note 52 at 18.

[57] Submissions of the Inspector-General of Intelligence op cit note 52 referred in the final report of the Matthews Commission op cit note 22 at 184-185.

be 'clearly defined parameters' and 'a statutory mandate and proper regulations' regarding the operation activities of the NCC in order to minimise the risks of abuse and illegality.[58]

The Commission's report dated 10 September 2008, was addressed as the 'Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP.'[59] The main findings of the Commission noted that the mandate of South Africa's intelligence agencies had become hopelessly politicised by being 'drawn into the realm of party politics'[60] and thus engaged in 'unlawful and unconstitutional'[61] monitoring and investigation of 'legal political activity' [62] and in doing so 'undermined political rights that are entrenched in the Constitution.'[63] The Commission stated that the 'the politicisation of the intelligence process and product [had] a high risk of impairing the Agency's command and control, oversight, accountability and ability to serve the national interest.'[64] The Commission further found that accountability of the intelligence agencies to the public was weak, a 'consequence of excessive secrecy'[65] and that the mandate of the intelligence agencies was overly broad such that the agencies had come to see themselves as the main watchdog of society, almost separate to, and above the constitutional and democratic order.[66]

Concerned that 'intelligence organisations have not shed sufficiently the apartheid-era security obsession with secrecy'[67] the Commission made 'concrete recommendations' in relation to transparency and oversight that included: (a) parliamentary consultation and debate,[68] (b) promulgation of ministerial regulations on intelligence in the *Government Gazette*,[69] (c) that 'executive policy on intelligence and the operations of the intelligence

[58] Ibid.
[59] According to reports by the Right2Know campaign: 'Though its findings were explosive, the Commission's report has been officially sidelined on a technicality – it was 'leaked' to the media before being tabled before Cabinet. This has allowed state officials to refuse to recognise the report, saying it has "no status" because it was not properly processed.' See Right2Know 'Big Brother Exposed: Stories of South Africa's intelligence structures monitoring and harassing activist movements' at 14 available at *https://www.r2k.org.za/category/publications/*, accessed February 2019.
[60] The Matthews Commission op cit note 22 at 180 at 10.
[61] Ibid at 18. At 180: 'the NCC appears to be engaged in signals monitoring that is unlawful and unconstitutional because it does not comply with the relevant legislation [RICA 2002 which prohibits the interception without judicial authorisation]. Similarly, the NIA policy on interception of communication is inconsistent with the Constitution and legislation.'
[62] Ibid at 10.
[63] Ibid.
[64] Ibid.
[65] Ibid at 11.
[66] Ibid at 71-76.
[67] Ibid at 22 and 229.
[68] Ibid at 277.
[69] Ibid at 278.

services should be in the public domain[70] (d) publication of annual reports of the intelligence services;[71] and (e) endorsing the recommendation of the Auditor-General that 'audit reports on the intelligence services be presented to Parliament as public documents, subject to the withholding of sensitive information as permitted by law.'[72]

The Commission's final report also made a number of important recommendations that the intelligence mandate of the key agencies should be 'narrowed' to focus primarily on serious crimes such as terrorism, organised crime, large-scale violence and systemic corruption, and not be 'acting as a secret watchdog over political activity, political parties and government.' [73] Importantly, the Commission recommended the 'NCC may not intercept the communication of a targeted person unless it has obtained an interception direction issued by the designated judge as provided for in RICA.'[74] Further, that immediate steps should be taken to ensure that its policies and procedures on the interception provide for ministerial approval and judicial authorisation, and are in alignment with the Constitution and legislation.[75]

All of this however was, and continued to be ignored with impunity by the state. In many ways, twelve years after the Matthews Commission, South Africa's intelligence agencies appear to remain hopelessly politicised.[76] Evidence of abuse and 'inappropriate' interest in 'lawful political and social activities' by law enforcement and security and intelligence agencies in South Africa have been widely documented by the Right2Know campaign and the Media Policy and Democracy Project,[77] revealing for example that the political intelligence

---

[70] Ibid.
[71] Ibid.
[72] Ibid at 142-43.
[73] Ibid.
[74] Ibid at 300.
[75] Ibid.
[76] See earlier chapter 1 at 32 for incidents cited by amaBhungane Centre for Investigative Journalism in its legal challenge to the constitutionality of RICA 2002.
[77] Right2Know 'SPOOKED: Surveillance of journalists in SA' (June 2018) available at *https://www.sanef.org.za/wp-content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf.*, accessed 17 June 2019; Right2Know 'Big Brother exposed: Stories of South Africa's intelligence structures monitoring and harassing activist movements' available at *https://www.r2k.org.za/category/publications/*, accessed February 2019; Right2Know 'Stop the surveillance! Activist guide to RICA and state surveillance in SA' available at *https://www.r2k.org.za/category/publications/*, accessed February 2019; Right2Know 'The Surveillance State: Communications surveillance and privacy in South Africa' available at *https://www.r2k.org.za/category/publications/*, accessed February 2019; H Swart 'Communications surveillance by the South African intelligence services' (February 2016) available at *https://www.mediaanddemocracy.com/ uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf*, accessed February 2019; A Mare 'An analysis of the communications surveillance legislative framework in South Africa' (November 2015) available at *https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf*, accessed February 2019; A Mare 'A qualitative analysis of how investigative journalists, civic activists, lawyers and academics are adapting to and resisting communications surveillance in South Africa' (March 2016) available at *https://www.mediaand democracy.com/uploads/1/6/5/7/16577624/duncan_2_comm_surveillance.pdf*, accessed February 2019.

focus on 'state spying' have targeted journalists whom have uncovered corruption, state capture, and abuse of power by the intelligence and prosecuting agencies in South Africa.[78]

It is important to note that the Matthews Commission brought to the fore arguments by the state in 2008 that the interception of communications by the NCC lies beyond the prescripts of RICA 2002, and again in 2019 when RICA 2002 was the subject of legal challenge.[79] RICA 2002 prohibits interception of communications without lawful authority of a designated judge, which may only be approved for specified purposes. It was argued by the state that the signals operations by the NCC did not fall within the definition of 'intercept'.[80] Having regard to the definition of 'intercept' and 'communication' referred to earlier, which includes both direct and indirect communications, it is clear that the NCC's signals operations are covered by the prescripts of RICA 2002.[81] A further argument by the state in defence of the operational activities of the NCC being outside the prescripts of RICA 2002 is that RICA 2002 regulates the investigative activities of law enforcement, whereas interception of communications by the NCC is concerned with intelligence.[82] This is an erroneous position. The RICA 2002 applies to law enforcement and the security and intelligence agencies, specifically by reference to s 1 in which 'applicant' in the warrantry processes, includes inter alia officers of South African police and members of the intelligence services.[83]

Another concern is that RICA 2002 does not provide a statutory basis for the use of equipment interference, targeted or in bulk. With no legal framework, it is not clear where, when, how and on what basis these sensitive techniques may be exercised. Further, there is also no legal framework for how data from bulk datasets is selected for examination. The lack of a statutory footing means that there is no constraint that ensures that the collection of data would be limited to only that which would be relevant to an investigation or operation.[84] Reports of unlawful activities by the intelligence agencies are indicative that gaps and weaknesses in the legislative framework of RICA 2002 appear to have been exploited to gather more information than was previously available, including significant details and movements about individuals whom are in no way implicated in any criminal or national security investigations. This was a key finding in the legal challenge to the constitutionality of RICA

[78] Right2Know 'SPOOKED' op cit note 77 at 2.
[79] *amaBhungane* case supra note 23 paras 147-166.
[80] The Matthews Commission op cit note 22 at 188.
[81] Ibid.
[82] Ibid at 188.
[83] Ibid at 188. See also RICA 2002, s 16(3) and (5).
[84] G Hosein and CW Palow 'Modern safeguards for modern surveillance: An analysis of innovations in communications surveillance techniques' (2013) 74.6 *Ohio State LJ* 1071 at 1090.

2002 by amaBhungane Centre for Investigative Journalism.[85] The state contended that the NSI Act 1994 authorised bulk interceptions and relied specifically on s 2, as a function of the Agency,[86] stated throughout as its operative provision: 'to gather, correlate, evaluate and analyse domestic and foreign intelligence (excluding foreign military intelligence).'[87] The state also referred to s 2A(5) dealing with the role of the SSA to vet relevant members of the national intelligence structures for security clearances, which on a plain reading however does not contain any lawful authority for bulk interceptions.[88] Section 2A(5) refers to 'in the prescribed manner, gather information' relating to (a) criminal records; (b) financial records; (c) personal information; or (d) any other personal information relevant to determine the security clearance of a person. Neither (a) nor (b) apply to interception. With regard to (c) personal information (which is not defined in the Act) and (d) any other personal information, arguably, this may apply to targeted interception for vetting purposes, and if so, RICA 2002 would apply.[89] However, there is no reference in the NSI Act 1994 regulating the investigative power of interception, targeted or in bulk. The court rejected contentions by the state that s 2 authorises such investigative powers of interception by reference to 'to gather, correlate, evaluate and analyse domestic and foreign intelligence.' The court noted such phrase is not supported by any authorisation processes, nor sets out where, when, how and on what basis these sensitive investigative powers may be used.[90] Sutherland J held that to read any of the provisions of the NSI Act 1994 to include, by implication of lawful authority for interception both target and in bulk would be an 'extravagance' and 'impermissible in terms of conventional techniques of statutory interpretation.'[91] Accordingly the court found 'no lawful authority' for bulk interception by law enforcement and the security and intelligence agencies. As such the court declared: 'bulk surveillance activities and foreign signals interception undertaken by the National Communications Centre are unlawful and invalid.'[92]

Therefore, until such time as the operational activities are brought within legislative prescripts, the NCC's signals operations fall within the provisions of RICA 2002 in relation to interception of communications. This means that for its signals operations, the NCC must in

[85] *amaBhungane* case supra note 23 paras 143-166.
[86] The structures contemplated include the National Intelligence Coordinating Committee, the SSA and the intelligence units within the Defence Force and the Police.
[87] *amaBhungane* case supra note 23 paras 149-150.
[88] Supra note 23 paras 151-154.
[89] Supra note 23 paras 151-154.
[90] Supra note 23 paras 150 and 155.
[91] Supra note 23 paras 151-162.
[92] Supra note 23 para 165, more than a decade after the Matthews Commission found the NCC 'engaged in signals monitoring that is unlawful and unconstitutional'.

terms of s 16(1) 'apply to a designated judge for the issuing of an interception direction' which in terms of 16(5) may only be issued for specified purposes, including for the prevention and detection of 'serious offences' or in the interests of 'national security or compelling national economic interests' if the reasonable grounds to believe' threshold has been met. To do so otherwise, would be to act without lawful authority and be unconstitutional.

(b) Notification of interception

RICA 2002 prohibits any notification to the suspect/target concerned about interception. In s 16(7)(*a*) of RICA 2002 '[a]n application [for an interception direction] must be considered and an interception direction issued *without any notice* to the person or customer to whom the application applies and *without hearing* such person or customer.'[93] This means that the application for an interception direction is made *ex parte*, without any notification to the suspect/target and without their presence in court. The Act goes so far as to prohibit disclosure of information in terms of the provisions of s 42(1): '[n]o person may disclose any information which he or she obtained in the exercising of his or her powers or the performance of his or her duties in terms of this Act.' The suspect/target of an interception is not notified about the interception even after the conclusion of the investigation or the end of the period of the interception direction, unless the information obtained by means of any interception is admissible as evidence in criminal proceedings against the suspect/target.[94]

This default position of blanket secrecy is argued as normal for investigation purposes, after all notification to the suspect/target may defeat the very purpose of the surveillance operation where there are risks than an investigation might be compromised, for example by witness intimidation or evidence being destroyed. The state vehemently maintains its position 'that absolute and invariable secrecy is required' and that any notification of interception, whether pre- or post-surveillance, would effectively defeat the purpose of RICA 2002 as the very essence of the investigative power of interception is secrecy.[95] This argument is extremely controversial, not least because the permanent position of blanket and invariable secrecy in the

[93] Emphasis added. Section 16(7) applies to the issuing of an entry warrant (ss 22(7)) except for ss 16(3)); a direction in respect of real-time (s 17(6)) and archived meta-data (s 19(6)), including combined applications under ss 18(3); decryption directions (ss 21(6)); and any amendments or extensions (ss 20(6)).
[94] Section 47.
[95] Attributed to South Africa's Minister of Police, Bheki Cele in 'Cele heads to ConCourt to fight surveillance ruling' available at *https://www.iol.co.za/news/politics/cele-heads-to-concourt-to-fight-surveillance-ruling-37690897*, accessed 24 March 2020. See also *amaBhungane* case applicants' heads of argument supra note 23 paras 85-91 for the state's arguments on notification of interception.

legal provisions of RICA 2002 cannot be justified with regard to the right to privacy, which in this context must be understood together with the right of access to courts in the Constitution of the Republic of South Act 108 of 1996.[96] The counter argument is that the right to privacy and the right of access to courts are not absolute rights, and any infringement can be justified in terms of s 36 of the Constitution, in that it is reasonable and justifiable in an open and democratic society, having regard to the factors specified in s 36.[97]

While the state appears willing to accept that there are unlawful surveillance practices by 'rogue elements' within law enforcement and security and intelligence agencies, it also argues that any evidence obtained in contravention of RICA 2002 'is tainted in legal proceedings.'[98] In theory this might be a sound argument. The argument by the state is that the constitutionality of RICA 2002 'must not be decided on the basis that some unscrupulous individual acting outside of the scope of legislation may abuse it or can abuse it.'[99] However, reports of incidents and allegations of unlawful surveillance practices by law enforcement and security and intelligence agencies cannot be ignored. Civil rights campaigns and investigative journalism in South Africa indicate that unlawful surveillance practices are only revealed by accident, or by information leaks, public interest litigation or whistleblowing. One such example abuse by law enforcement and security and intelligence agencies is the 'undisputed first-hand experience of the deponent' in the *amaBhungane* case:[100]

> 'No rebuttal or explanation or effort to justify the interception is attempted [by the state]. No good reason exists not to hear the matter on the facts alleged by Sole alone. Because Sole has not right to demand disclosure, he, being forbidden by RICA from being informed, the fact of

[96] Hereafter 'the Constitution'. Section 14 of the Constitution provides '[e]veryone 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' and provides that "[e]veryone has the right to have any dispute that can be resolved by the application of law decided in a fair public hearing before a court or, where appropriate, another independent and impartial tribunal or forum.' See *amaBhungane* case applicants' heads of argument supra note 23 paras 85-91.

[97] Including '(a) the nature of the right; (b) the importance of the purpose of the limitation; (c) the nature and extent of the limitation; (d) the relation between the limitation and its purpose; and (e) less restrictive means to achieve the purpose.'

[98] See *amaBhungane* case applicants' heads of argument supra note 23 paras 85-91 for the state's arguments on notification of interception.

[99] *amaBhungane* case applicants' heads of argument supra note 23 para 93.

[100] Supra note 23. In 2015, in a case involving the decision to drop corruption charges against then-President of South Africa, Jacob Zuma, it was inadvertently revealed that the communications of an investigative journalist, Sam Sole, and a state prosecutor, Billy Downer, had been intercepted in 2008. This was discovered when Zuma's attorney attached to court papers extracts from official interception conversations between Sole and Downer. Sole had been investigating the decision to drop the charges against Zuma, considered to an extremely controversial prosecutorial decision in South Africa at the time. Sole is an executive director of amaBhungane Centre for Investigative Journalism, an independent and non-profit investigative journalism newsroom in South Africa which aims to 'develop investigative journalism to promote free, capable media and open, accountable and just democracy.' Available at *https://amabhungane.org*, accessed 29 March 2020.

> the spying only became public knowledge fortuitously. Sole's efforts to obtain details, plainly fruitless in the light of the prohibition on disclosure, was furthermore met with contemptuous responses and unsubstantiated allegations that no irregularities occurred.'[101]

In this regard a 'fundamental reorientation'[102] is required in South African law in relation to notification of interception. The default position of blanket secrecy in RICA 2002 means that complaints are unlikely to be made, thereby annulling any ability to challenge the legality of the interception measure retrospectively.[103] Therefore, any safeguards and guarantees against abuse or arbitrariness would escape scrutiny because the suspect/target of the surveillance has the right to challenge the validity of the interception direction and the admissibility of evidence *if* criminal proceedings are instituted.[104] Where there is no criminal proceedings, directly or indirectly involving the subject/target of the interception, there is no recourse because disclosure is prohibited under 'absolute and invariable secrecy' under the RICA 2002. The key issue is that of secrecy, in this instance blanket secrecy, and the unwillingness of the state of concede at least on the possibility of post-surveillance notification to the suspect/target, if not on notification pre-surveillance. Twelve years earlier, the Matthews Commission expressed its concerns with the dangers associated with a culture of secrecy within law enforcement and security and intelligence agencies:

> 'The secrecy surrounding the intelligence organisations is not consistent with the Constitution. …The high level of secrecy is contrary to the spirit of the Constitution. …The Constitution is binding on all organs of state and the dangers associated with secrecy – lack of accountability, abuse of power, infringements of rights and a culture of impunity – apply to the intelligence organisations no less than to other sectors of the state. A fundamental reorientation is therefore required. Secrecy should not dominate and engulf the intelligence community but should be confined mainly to those areas where disclosure of information would cause significant harm to the lives of individuals, the intelligence organisations, the state or the country as a whole. The emphasis on secrecy with some exceptions should be replaced by an emphasis on openness with some exceptions.'[105]

---

[101] Supra note 23 para 19.
[102] The Matthews Commission op cit note 22 at 263.
[103] Liberty 'Liberty's briefing on the Investigatory Powers Bill for report stage in the House of Commons (June 2016) at 64 available at *https://www.libertyhumanrights.org.uk/sites/default/files/campaigns/ resources/Liberty%27s%20Briefing%20on%20the%20Investigatory%20Powers%20Bill%20for%20Report%20Stage%20in%20the%20House%20of%20Commons.pdf*, accessed 22 May 2019.
[104] See *amaBhungane* case applicants' heads of argument supra note 23 paras 85-91 for the state's arguments on notification of interception.
[105] Ibid at 263.

A brief analysis of comparative jurisprudence demonstrates a very different approach to the position in South Africa law. For example in the United States of America, procedure for interception of communications provides for notification to the suspect/target '[w]ithin a reasonable time but not later than ninety days', unless the authorities can show there is 'good cause' to withhold that information.[106] A similar model operates in Canada, where the suspect/target of an interception warrant for the purposes of law enforcement must be given notice within ninety days of an interception warrant expiring. This may be extended up to three years in terrorism cases, subject to judicial oversight, if in the 'interests of justice.'[107] Similar notification provisions apply in Germany and the Netherlands, with exemptions to protect (if required) the integrity of ongoing investigations.

In terms of the German Code of Criminal Procedure,[108] the suspect/target under telecommunication surveillance shall be notified of surveillance measures. The notification should mention the suspect/target's option of court relief and the applicable time limits and should be given as soon as possible without 'endangering the purpose of the investigation, the life, physical integrity and personal liberty of another or significant assets including the possibility of continued use of the undercover investigator.' However, notification will be 'dispensed with where overriding interests of an affected person that merit protection constitute an obstacle.' In the Netherlands, the provisions of the Code of Criminal Procedure[109] state that the public prosecutor must notify in writing the suspect/target of telecommunications or other technical devices of the surveillance 'as soon as the interest of the investigation permits' but not if it is not reasonably possible to do so. If the suspect/target learns of the exercise of surveillance power through means described in 126aa(1) or (4) of the Code, notification is not required. If the investigation relates to terrorist offences or another serious offence, information pertaining to the suspect/target's name, address, postal code, town, number, and type of service of a user of a communication service may be requested, and the notice provisions of 126bb will not apply.

In South Africa the state contends that secrecy is 'inimical to the efficacy of the interception of a communication' and the fact that suspect/target is not notified, whether pre- or post-surveillance, does not necessarily mean that the exercise of such investigative power

[106] 18 U.S. Code § 2518(8)(d).
[107] Canadian Criminal Code, s 188, 195-196.
[108] Section 101(4)(3).
[109] Part VD, Chapter One, s126bb.

was not 'reasonable and justifiable in an open and democratic society.'[110] While it is recognised that in some circumstances it is necessary to protect the integrity of investigations, working methods and field operations by law enforcement and security and intelligence agencies, the position of the state that 'absolute and invariable secrecy is required – forever, regardless of the circumstances'[111] is not sustainable nor justifiable in terms of the s 36 limitation provision in the Constitution. It is possible for the suspect/target who has been made the subject of surveillance to be informed of that interception, when the operation is completed, and where no investigation, working methods or field operations by law enforcement and security and intelligence agencies might be prejudiced as a result. While pre-surveillance notification may be justified, the requirement of continued secrecy after termination of the surveillance operation 'is not rationally linked to any legitimate purpose.'[112]

The requirement of notification to the suspect/target of surveillance as soon as possible is identified by the European Court of Human Rights as an important safeguard against abuse, and positioned that 'as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned.'[113] In a number of cases including, *Klass v Germany*,[114] *Weber and Savaria v Germany*[115] and *Roman Zakharov v Russia*,[116] the European Court of Human Rights referred to the importance of the target/suspect having access to an effective remedy before the courts as 'inextricably linked' to user notification.[117] In *Klass v Germany*, the Court stated:

> 'Inextricably linked to this issue is the question of subsequent notification, since there is in principle little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality.'[118]

---

[110] *amaBhungane* case applicants' heads of argument supra note 23 paras 85.
[111] Supra note 23 paras 85.
[112] Supra note 23 para 93.
[113] *Association for European Integration and Human Rights and Ekimhzhiev* EctHR 62540/00 (28 June 2007) paras 90-91.
[114] EctHR 5029/71 (6 September 1978).
[115] EctHR 54934/00 (29 June 2006).
[116] EctHR 47143/06 (4 December 2015). The ECtHR found that that judicial remedies for those the subject/target of interception in Russia were generally ineffective, particularly in light of the total absence of any notification requirement to the interception subject/target, and without any meaningful ability of retrospective challenges to surveillance measures.
[117] See also *Malone v United Kingdom* EctHR 8691/79 (2 August 1984); *Leander v Sweden* EctHR 9248/81 (26 March 1987); *Amann v Switzerland* EctHR 27798/95 (16 February 2000); *Rotaru v Romania* EctHR 28341/95 (2 May 2000); *Lambert v France* EctHR 46043/14 (25 June 2015 rectified).
[118] *Klass*' case supra note 114 para 57.

This was also confirmed by the court in *Weber and Savaria v Germany*, where the court reiterated that notification of surveillance measures is 'inextricably linked to the effectiveness of remedies before the courts' and therefore also 'to the existence of effective safeguards against the abuse of monitoring powers' having regard to the fact that there would be 'little scope for recourse to the courts' by the individual concerned unless they are informed of the measures taken without their knowledge and therefore able to challenge the legality of the surveillance measures retrospectively.[119] The court further reiterated its position on the question of subsequent notification of surveillance measures:

> 'However, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not "necessary in a democratic society", as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. Indeed, such notification might reveal the working methods and fields of operation of the Intelligence Service (see *Klass and Others*, cited above, § 58, and, mutatis mutandis, *Leander*, cited above, § 66). As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned (see, mutatis mutandis, Leander, cited above, § 66, and *Klass and Others*, cited above, § 58).'[120]

On the issue of blanket secrecy on notification to the suspect/target of an interception raised in the public interest litigation in the *amaBhungane* case,[121] the High Court of South Africa agreed with the need for 'post surveillance notification as is the case in other democratic societies.'[122] The Court stated:

> 'Plainly, the illustration of the right to notice in other jurisdictions demonstrates that world opinion has embraced this right as a facet of a democratic social order, subject to safeguards against undoing the very objectives of legitimate surveillance. *What is there to the SA condition that would justify a rejection of a post interception notice, subject to judge the judge authorising delays for good cause shown? None have been shown.* Indeed, the two examples, one of clear abuse and the other of unexplained spying alluded to, point in the other direction. The resistance has been directed at circumstances which would justify a ban on notification; an absolutist stance.'[123]

---

[119] *Weber*'s case supra note 115 para 135.
[120] Supra note 115 para 135.
[121] *amaBhungane* case supra note 23 para 51.
[122] Supra note 23 para 51.
[123] Supra note 23 para 51 (emphasis added).

As such the court declared ss 16(7), 17(6), 18(3)*(a)*, 19(6), 20(6) and 22(7) of RICA as inconsistent with the Constitution and therefore invalid 'to the extent that it fails to prescribe procedure[s] for notifying the subject of the interception.'[124] In terms of the order declared by the court, the declaration of invalidity is suspended for two years, allowing the legislature time to cure the defect. By way of interim relief, the court held that ss 16(11) and 16(12) must be read to include user notification within ninety days of the surveillance operation, with exceptional orders of deferred user notification.[125]

This is the right outcome. As a starting point for the 'fundamental reorientation' in South African law, this potentially means the introduction of a new duty of general notification, such that subsequent notification to a suspect/target of an interception direction would be after the investigation or operation has been terminated, and subject to public interest exemptions in preserving the integrity of investigations, working methods and field operations by law enforcement and security and intelligence agencies.[126] In my view, this could be taken further. Instead of creating a presumption of general notification such that notification to a suspect/target of an interception direction would be after the investigation or operation has been terminated, RICA 2002 should be amended (or in new legislation) to provide for a default mandatory notification mechanism.[127] Provision for mandatory notification would allow a suspect/target of an interception direction to pursue a challenge of legality retrospectively even in circumstances where exercise of such investigative power was deemed 'reasonable and justifiable in an open and democratic society.' The brief analysis of comparative jurisprudence referred to earlier shows that such a model operates in other countries, although it is accepted that notification may be less likely where doing so may prejudice the outcome of investigations, working methods and field operations by law enforcement and security and intelligence agencies. [128] Similar to the model in the United States, notification to a suspect/target of an interception direction should be by default, within ninety days of the surveillance operation, unless law enforcement and security and intelligence agencies can show 'good cause' to withhold that information. The provision of a potential disclosure under a default mandatory notification mechanism in South African law may just 'create an additional impetus' needed

[124] Supra note 23 paras 53-54.
[125] Supra note 23 paras 53-54.
[126] Liberty op cit note 103 at 64.
[127] JUSTICE *Investigatory Powers Bill 2016: Part 8 Surveillance Oversight Briefing for House of Commons Committee Stage* (April 2016) available at https://justice.org.uk/wp-content/uploads/2016/04/JUSTICE-Briefing-IP-Bill-HC-CS-Part-8.pdf, accessed 25 March 2020 paras 63-64.
[128] Ibid.

'towards lawful decision making' by law enforcement and security and intelligence agencies exercising these investigative powers.[129]

(c) Threshold for conducting interception of communications

Following the Matthews Commission in 2008 and failure by government to implement its recommendations, the findings of the UN Human Rights Committee in 2016 on South Africa's regulation of electronic surveillance was seemingly inevitable and unsurprising. A key concern referred to the 'relatively low threshold for conducting surveillance.'[130]

Sections 16-25 of RICA 2002 sets out provisions in relation to applications for, and issuing of, directions and entry warrants. Recurrent in every investigative power in RICA 2002 is the stated formulation of 'reasonable grounds to believe'[131] as the threshold for judicial authorisation of investigative powers by law enforcement and security and intelligence agencies. Authorisation is by a designated judge, and defined in the Act to mean 'any judge of a High Court discharged from active service.' In terms of s 16(1) 'an applicant may apply to a designated judge for the issuing of an interception direction.' Interception can be authorised by a designated judge 'if there are reasonable grounds to believe'[132] inter alia that a 'serious offence has been or is being or will probably be committed'[133] or where the information sought concerns 'an actual threat'[134] to 'national security' or 'compelling economic interests of the Republic.'[135]

An application for an interception direction to a designated judge must be in writing. The requirements of the application inter alia must indicate the identity of the law enforcement official, the identity of the suspect/target of an interception, including the grounds on which the application is made, particulars of the allegation, period of the interception direction.[136] The applicant must also demonstrate 'the basis for believing that evidence relating to the ground on which the application is made will be obtained through interception.'[137] The

[129] Ibid para 64.
[130] United Nations Human Rights Committee op cit note 25 para 43.
[131] RICA 2002, ss 16(5)*(a)*, (b); 8*(b)(ii)*; 17(4); 19(4); 21(4); 22(4)*(b)*; 23(4)*(b)*; 51(7)*(b)*. See also Ugandan law in the Regulation of Interception of Communication Act 2010 which similarly requires 'reasonable grounds' threshold in section 5(1) for interception of communications.
[132] Section 16(5)*(a)*.
[133] Section 16(5)*(a)(i)*.
[134] Section 16(5)*(a)(ii)* and *(iii)*.
[135] Ibid.
[136] Section 16(2).
[137] Section 16(2)*(d)(ii)*.

applicant must also 'indicate whether other investigative procedures have been applied and failed to produce the required evidence' or 'why other investigative procedures reasonably appear to be unlikely to succeed if applied or are likely to be too dangerous to apply in order to obtain the required evidence.' [138] RICA 2002 also provides for the interception of communications in two scenarios of 'urgency'. The first scenario provides for an application to be made orally, if the applicant is 'of the opinion that it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstance' to be able to make a written application.' [139] The second scenario of urgency provides for exceptional circumstances for interception without prior authorisation from a designated judge if there are reasonable grounds to believe that a party to the communication has caused, or may cause serious bodily harm to another person[140]; threatens, or has threatened to cause serious bodily harm to another person[141]; threatens, or has threatened to take his or her own life.[142] In these scenarios of urgency, the applicant 'must as soon as practicable after the interception of communication' submit inter alia a written confirmation of request and an affidavit to the designated judge.[143]

Although RICA 2002 requires prior judicial authorisation for interception, a challenge created by the Act is that the authorisation procedure is too low, and as such does not provide for sufficient safeguards and guarantees against abuse. It has been suggested that the stated formulation of 'reasonable grounds to believe' as the threshold for judicial authorisation in RICA 2002 should be changed to a higher threshold of 'reasonable suspicion' or 'high degree of probability.'[144] Support for the higher threshold of 'reasonable suspicion' can be found in *Roman Zakharov v Russia*, a case concerning the system of secret interception of mobile telephone communications in Russia, the European Court of Human Rights referred to the 'reasonable suspicion' threshold. In view of concerns that judicial scrutiny in Russia was limited in scope 'to indicate that in their everyday practice Russian courts do not verify whether there is a reasonable suspicion against the person concerned,'[145] the European Court of Human Rights asserted that the obligations of judicial authorisation is not met on the basis of some

[138] Section 16(2)*(e)*.
[139] Section 23.
[140] Section 7(1)*(a)(i)*.
[141] Section 7(1)*(a)(ii)*.
[142] Section 7(1)*(a)(iii)*.
[143] Section 8(4).
[144] Necessary and Proportionate *International principles on the application of human rights to communications surveillance* available at *https://necessaryandproportionate.org/principles*, accessed 27 March 2020 at 8. See *amaBhungane* case applicants' heads of argument supra note 23 paras 191-221.
[145] *Roman*'s case supra note 116 para 263.

kind of involvement. The process of judicial authorisation must ensure that judges are 'sufficiently empowered' to verify the existence of reasonable suspicion against the suspect/target:[146]

> 'Turning now to the authorisation authority's scope of review, the Court reiterates that it must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular whether there are factual indications for suspecting that person of planning, committing, or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security.'[147]

The concern is that 'designated judge',[148] or 'judge of a High Court',[149] or 'a regional court magistrate', [150] or 'a magistrate' [151] under the 'reasonable grounds to believe' authorisation threshold are not expressly directed to verify the existence of a 'reasonable suspicion' against the suspect/target concerned, or to apply the 'reasonable and justifiable in an open and democratic society' test. However, while some formulations of the threshold 'are more strident than others'[152] consideration should be s 16(2)*(c)* which requires an application for an interception direction to 'contain full particulars of all the facts and circumstances.' It can be assumed that all the information provided will be interrogated by a designated judge and if satisfied on the 'reasonable grounds to believe' threshold may approve the interception direction. Perspectives on this assumption are considered below.

Arguments advanced in response to concerns of a low threshold under the stated formulation of 'reasonable grounds to believe' for conducting interception in South Africa law are said to unsubstantiated because RICA 2002 provides sufficient safeguards and guarantees against abuse. First, authorisation for interception is by a designated judge 'if there are

---

[146] See P De Hert and PC Bocos 'Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court's *Schrems* judgment' available at *https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/*, accessed 16 May 2019. See also M Rice 'Surveillance: *Zakharov v Russia* and what it means for the Investigatory Powers Bill available at *https://www.opendemocracy.net/en/zakharov-v-russia-refresher-on-how-far-europe-has-come/*, accessed 16 May 2018.

[147] *Roman*'s case supra note 116 para 260.

[148] RICA 2002, ss 1, 7(4), (5), (6); 8(4)*(b)*, (c); 8(5); 8(6); 16(1),(4), (5), (8)*(a)(iii)*, (8)*(b)(iii)*, (10), (10)(b); 16(5); 17(1), (3), (4)*(a)*, *(b)*; 19(7), (8); 20(1), (3), (4); 21(1)(a),(b);22(3), (4)(a), (b), (5)(c), 6(b); 23(3), (4)(a), (b), (7), (8)*(a)*, *(b)*, (10), (11); 24, *(a)(ii)*; 25(1), (2), (3).

[149] Ibid ss 191(1), (3)(4), (7); 48.

[150] Ibid ss 19(1), (3), (4), (7); 48.

[151] Ibid ss 19(1), 3), (4), (7); 48.

[152] *amaBhungane* case supra note 23 para 141 where the court referred to *Goodwin v United Kingdom* EctHR 17488/90 (27 March 1996) which stated the threshold for compelling disclosure by a journalist of a source: 'Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 (art. 10) of the Convention *unless it is justified by an overriding requirement in the public interest*' para 39 (emphasis added).

reasonable grounds to believe' on one of the grounds referred in s 16(5)*(a)* and 'there are reasonable grounds to believe' that the interception of particular communications on the specified ground will be obtained by means of the authorised interception direction. [153] Second, there must be reasonable grounds for believing that the evidence relating to the specified ground on which the interception direction is based will be obtained through interception.[154] Third, other investigative procedures have been applied and have failed to produce the required evidence or are unlikely to succeed or too dangerous if applied. [155] Fourth, interception directions are limited as the orders are only granted for a period of three months at a time.[156]

I am not convinced that a change in semantics of the stated threshold of 'reasonable grounds to believe' is the right approach to set adequate guarantees against abuse by law enforcement and security and intelligence agencies.[157] The state is unlikely to encounter any serious difficulty in demonstrating that the justification for interception pursues a legitimate aim, inter alia, that a 'serious offence has been or is being or will probably be committed'[158], or where the information sought concerns 'an actual threat' [159] to 'national security' or 'compelling economic interests of the Republic.'[160] This is mainly because analysis by the courts tends to focus on the legislative framework itself for the exercise of these investigatory powers rather than on a specific surveillance measure used in a particular case. [161] It is also generally accepted by the courts that investigatory powers of surveillance are necessary for specified purposes, including for the prevention and detection of 'serious offences' or in the interests of 'national security or compelling national economic interests.'[162]

If it is accepted that interception of communications is capable of being reasonable and justifiable in an open and democratic society,[163] the controversy arises in respect of risk of

[153] Section 16(5)*(b)(i)*.
[154] Section 16(2)*(d)(ii)*.
[155] Section 16(2)*(e)*.
[156] Section 16(2)*(d)*.
[157] *amaBhungane* case supra note 23 paras 128 and 141.
[158] Section 16(5)*(a)(i)*.
[159] Section 16(5)*(a)(ii)* and *(iii)*.
[160] Ibid.
[161] With reference to European human rights law, see Necessary and Proportionate *International principles on the application of human rights law to communications surveillance: Background and supporting international legal analysis* at 19 available at *https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf*, accessed 29 March 2020. This report of legal analysis recognises that the need for surveillance measures to be more specifically 'targeted' is an aspect more closely tied to the question of the proportionality of the measure itself but, in practice, is rarely examined by the court in European human rights law. There are exceptions, see *Uzunv Germany* EctHR 35623/05 (2 September 2010) and *Peck v the United Kingdom* EctHR 44647/98 (28 January 2003).
[162] See *Klass' case* supra note 114.
[163] Having regard to the factors specified in s 36 of the Constitution, see op cit note 97.

abuse and exercising these investigatory powers without lawful authority. A contrasting position to acceptable justification is offered by the United Nations Special Rapporteur on Freedom of Expression, Frank LaRue, whom expressed concerns in a report that 'vague and unspecified' notions of 'national security' in particular had been unduly used to justify interception and access to communications without adequate safeguards.[164] The Special Rapporteur concluded:

> 'The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern. The concept is broadly defined and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable grounds such as human rights defenders, journalists or activists. It also acts to warrant often unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability.'[165]

Having regard to the potential for abuse inherent in such overly broad concepts, there are recommendations in the Necessary and Proportionate principles for states to adopt a more stringent standard as to what constitutes a 'legitimate aim' in relation to surveillance powers:

> 'For this reason, the "pressing and substantial objective" test applied in Canada and the "compelling government interest" test used in the United States were also discarded as being insufficiently rigorous. Instead, the Principles reflect a higher standard imposed in Germany. In particular, the German Constitutional Court has ruled that deeply intrusive measures such as a search of a computer by law enforcement agencies cannot be justified merely by reference to some vaguely defined general interest. The German Constitutional Court held that such a measure had to be justified on the basis of evidence that there is "a concrete threat to an important legally-protected interest," such as a threat to the "life, limb or liberty of a person" or to "public goods, the endangering of which threatens the very bases or existence of the state, or the fundamental prerequisites of human existence.'[166]

Irrespective of the descriptions of justification and semantics used, whether this is stated as 'reasonable grounds to believe' or 'pressing and substantial objective' or 'compelling government interest' or 'a concrete threat to an important legally-protected interest,' the key

---

[164] United Nations Human Rights Council 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank LaRue' A/HRC/23/40 (17 April 2013) at 3 available at *https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf*, accessed 4 July 2019.
[165] Ibid at 15-16. Equally so by the Matthews Commission note 22 at 263-64:'The justification for secrecy should not rest on the concept of 'national security'. …If secrecy can be justified on these expansive and inexact grounds, then there is a great danger of excessive and spurious classification of information.'
[166] Necessary and Proportionate *International principles: Background* op cit note 161 at 19-20 (footnotes omitted).

issue is the breadth of the powers exercised by law enforcement and the security and intelligence agencies. The concern in South African law is that interception and access to communications is without sufficient safeguards against the risk of abuse of power – even if they were adequate in theory, the safeguards are simply not effective in practice.

As argued earlier, provision of a potential disclosure to the subject/target of interception under a default mandatory notification mechanism in South African law may act as a strong deterrent to prevent abuse of power needed 'towards lawful decision making' by law enforcement and security and intelligence agencies.[167] If this is so, and a 'one-threshold-fits-all' approach in RICA 2002 is regarded as satisfactory, then a key issue for consideration is whether RICA 2002 provides sufficient safeguards for interception with regard to what would be covered by legal privilege or the identification of an investigative journalist's confidential source. The contention advanced is 'that a higher threshold should be used in respect of surveilling journalists or lawyers, because the extent of the infringement to the right to privacy becomes amplified.'[168]

Both lawyers and journalists have obligations to preserve confidential communications, respectively from clients or confidential sources. Should they be especially protected in relation to ordinary subjects of the state, having regard to the effect of interception in the performance of their professional roles and the efficacy with which those professional roles can be performed?[169] These professional roles, especially considerations of journalist freedom apply to what has been called by the Strasbourg Court as 'social watchdogs', in particular, non-governmental organisations whose work is important in informing the public and exposing the truth, including potentially unlawful action by the state.[170]

It is therefore important to consider what protections are in place to manage interception of communications in relation to legal privilege and journalists' confidential sources. The issues are twofold: (a) whether RICA 2002 expressly requires the applicant of an interception direction to inform the designated judge that the subject/target of the interception direction is a journalist or lawyer; and (b) if the interception direction includes communications covered

[167] JUSTICE op cit note 127 para 64.
[168] *amaBhungane* case applicants' heads of argument supra note 23 paras 191-221.
[169] *amaBhungane* case supra note 23 para 112.
[170] See *The Queen (on Application of National Council for Civil Liberties (Liberty) v Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs* [2019] EWHC 2057 (Admin) para 293. See also *Sanoma Uitgevers BV v Netherlands* [2011] EMLR 4; *Telegraaf Media Nederland Landelijke Media BV v Netherlands* (Application No 39315/06, judgment of Third Section, 22 November 2012); and *Nagla v Latvia* (Application No 72469/10, judgment of Fourth Section, 16 July 2013)

by legal privilege or the identification of an investigative journalist's confidential source – is there sufficient protection in RICA 2002 expressly for situations where the subject/target of an interception is a lawyer or a journalist.

With regard to the first issue, s 16(2)*(c)* comes into consideration which requires an application for an interception direction to 'contain full particulars of all the facts and circumstances.' By virtue of this section, the argument of the state is that the designated judge has a discretion to take into account if the subject/target whose communication is required to be intercepted is a lawyer or a journalist, and empowers the designated judge to impose certain conditions and restrictions. However, there is no statutory obligation in RICA 2002 that requires an applicant to inform the designated judge that the subject/target of the interception is a lawyer or a journalist. Even if a liberal reading of s 16(2)*(c)* is accepted, on the second issue there are no provisions in RICA 2002 prescribing limitation procedures or conditions in the event of the subject/target of an interception being a lawyer or a journalist.[171]

There are no provisions to ensure the proper collection, storage, access to and use of intercepted communications. There are no safeguards concerning the number of persons, copies and times that intercepted communications are shared. There are no safeguards that such information must be destroyed as soon as there are no longer grounds for retention. The Act itself offers no guidance concerning the treatment and handling of intercepted communications covered by legal privilege or the identification of an investigative journalist's confidential source, or even confidential personal information of the subject/target such as medical records. This is problematic.

The assumption that all the information provided will be interrogated by designated judge, overlooks the possibility that the designated judge will be misled.[172] Reports of incidents and allegations of abusive and unlawful surveillance of campaigners, unionists, lawyers, journalists and opposing factions of ruling political party interests referred elsewhere in the thesis highlight the vulnerabilities in RICA 2002. In an incident involving journalists Stephan Hofstatter and Mzi wa Afrika, it was alleged that Crime Intelligence misled the designated judge by stating that the mobile numbers of the journalists belonged to automated teller machine bombing suspects. As a result thereof, the warrant authorised the interception of their

[171] *amaBhungane* case applicants' heads of argument supra note 23 paras 191-221.
[172] *amaBhungane* case supra note 23 para 139.

calls and text message, including metadata.[173] In a Media Policy and Democracy Project, Mare remarked on the need for a higher authorisation threshold, especially in relation to journalists and lawyers:

> 'The Crime Intelligence Division of the South African Police Service (SAPS) also took advantage of the low threshold of targeted surveillance as set out in RICA to obtain judicial approval to intercept the mobile phones of two Sunday Times journalists (Stephan Hofstätter and Mzilikazi wa Afrika) in 2010 by giving fictional names and suggesting such interception was needed to investigate a criminal syndicate. Subsequently, the Sunday Times took the case to court and two officers were charged with violations of RICA. This incident has fuelled fears that other applications to tap the communications of journalists and public figures may have been granted under false pretences. Not only journalists have been targeted for state surveillance, but trade unionists have not been spared either, with media reports indicating that state intelligence officers were spying on senior National Union of Metalworkers of South Africa13 (NUMSA) officials as well as attempting to recruit some of their members work as spies.'[174]

With specific reference to the relationship between journalist and their sources, there is general recognition of their important role and need for protection.[175] By allowing law enforcement and security and intelligence agencies to identify sources without clear safeguards would undermine these principles. A 'one-size-fits-all' approach to interception without the provision of special protections and clear safeguards for sensitive information as is the case in RICA 2002 is, it is argued, unsatisfactory and potentially unlawful. There are concerns regarding the risks of handling procedures for such intercepted information, in that it could be

---

[173] An account of this incident is reported in J Duncan 'Communications surveillance in South Africa: The case of the Sunday Time's newspaper' available at *https://www.academia.edu/9170517/Communications_surveillance_in_South_Africa_the_case_of_the_Sunday_Times_newspaper*, accessed 19 June 2019. See also J Duncan 'The bugging of South Africa' (29 July 2013) available at *http://sacsis.org.za/site/article/1739*, accessed 17 May 2016; H Swart 'Secret state: How the government spies on you' (14 October 2011) available at *http://mg.co.za/article/2011-10-14-secret-state/*, accessed 17 May 2016.

[174] Mare op cit note 77.

[175] *Nova Property Group Holdings Ltd 7 Others v Cobbett & Another* 2016 (4) SA 317 para 38: ''Access to information is crucial to accurate reporting and thus to imparting accurate information to the public. Interference with the ability to access information impedes the freedom of the press. The right to freedom of expression is not limited to the right to speak, but includes the right to receive information and ideas. Preventing the press from reporting fully and accurately, does not only violate the rights of the journalist, but it also violates the rights of all the people who rely on the media to provide them with 'information and ideas.' See also *Bossasa Operations (Pty) Ltd v Basson & Another* 2013 (2) SA 570 (GSJ) para 38: '…it is apparent that journalists, subject to certain limitations, are not expected to reveal the identity of their sources. If indeed the freedom of the press is fundamental and a sine qua non for democracy, it is essential that in carrying out this public duty for public good, the identity of sources should not be revealed, particularly when the information so revealed would not have been publicly known. The essential and critical role of the media, which is more pronounced in our nascent democracy, founded on openness, where corruption has become cancerous, needs to be fostered rather than denuded.' See also *Government of RSA v The Sunday Times* 1995 (2) BCLR 182 (T) para 188.

abused or accessed (without lawful authority). RICA 2002 is not capable of providing adequate and effective guarantees against abuse.

The court in the *amaBhungane* case described the role of investigative journalism as the 'ferreting out of fact by enquiry, largely, from whistle-blowers and others who rat on their fellows and their bosses.'[176] In the court's view, the central issue was not about compelling journalists to reveal their sources but the ability of third parties to identify 'who the rats are' through intercepting a journalist's communications. The court made reference to the harsh reality of corruption in South Africa and noted that '[i]n a country that is as wracked by corruption in both our public institutions and in our private institutions as ours is, and where the unearthing of wrongdoing is significantly the work of investigative journalists, in an otherwise, seemingly, empty field, it is hypercritical to both laud the press and ignore their special needs to be an effective prop of the democratic process.'[177]

The court was not prepared to ignore the argument that investigative journalists in South Africa have attracted the attention of 'powerful and influential' individuals 'who are capable of suborning the apparatus of the State to smell out their adversaries'[178] and that this exacerbated the potential for abuse in the current framework of RICA 2002. The court made specific reference to the incident involving journalists Stephan Hofstatter and Mzi wa Afrika referred to above. The court found a deficiency in s 16 of RICA 2002 because 'the peculiar position of journalists is not expressly catered for,' and as with the need to protect legal privilege, the risk inherent of 'spying on a journalist' would be to investigate persons with whom that journalist is in contact, which the court expressed as conduct that 'cannot be appropriate.'[179] Pending confirmation by the Constitutional Court on the declaration of unconstitutionality, in terms of interim relief the court ordered mandatory notification under statutory obligation such that if the subject/target whose communication is required to be intercepted is a lawyer or a journalist, the applicant of an interception direction must inform the designated judge.[180] The interim relief measures further expressly allow a designated judge to impose limitation or conditions as deemed necessary based on the fact that the subject/target is a lawyer or a journalist.

[176] *amaBhungane* case supra note 23 para 129.
[177] Supra note 23 para 131.
[178] Supra note 23 para 138.
[179] Supra note 23 para 136.
[180] Supra note 23 para 167.

This is an appropriate outcome. In doing so, it emphasises the need in the regulation of electronic surveillance in South African law to have regard to whether the level of protection to be applied in relation to the obtaining of information is 'higher' because of the 'particular sensitivity' of that information which identifies/confirms the source of journalistic information or is subject to legal privilege.[181] The considerations which apply to the importance of legal privilege and journalists' confidential sources in legislative amendments to RICA 2002, or in new law, must therefore require prior independent authorisation where an *order* is sought of subject/target who is a journalist or a lawyer, or where the purpose of *obtaining* material (in exceptional or compelling circumstances) is to discover a journalistic source or legally privileged information. This could be taken further by (i) mandatory reporting to an independent oversight authority; and (ii) at the stage of *selection for examination* of journalistic or legally privileged material that has already been obtained under targeted or bulk powers. Where intercepted information has been obtained pursuant to a warrant, and at the stage at which a decision is to be made as to whether to *examine* that intercepted information, there should be an additional warrant requirement for selection for examination.[182] Such a safeguard may include a consideration of rationale – where purpose of the criteria to be used for selecting such material for examination is to identify items subject to legal privilege or is journalistic material, or where the use of those criteria is likely to be revealing.[183] The decision to be taken, preferably by an independent oversight authority, should be governed by exceptional and compelling guidelines, including a consideration of whether public interest in the selection for examination outweighs the public interest in the protection of information subject to legal professional or 'source' privilege. In addition, whether there are less intrusive or any other means by which the information could reasonably be obtained and would suffice to serve the overriding public interest justifying interception and subsequent selection for examination of intercepted materials of particular sensitivity.[184] The independent body must have the power to decline a disclosure order or to make a limited or qualified order so as to protect information from being revealed or accessed, including safeguards for handling, retention, use and

[181] See See also *The Queen (on Application of National Council for Civil Liberties (Liberty)* supra note 170 paras 271-292 (legally privileged items) and paras 293-352 (the challenge in respect of confidential journalistic material).
[182] Supra note 181 para 302 (based on claimant's challenges to the United Kingdom's Investigatory Powers Act 2016).
[183] See ss 153(2), (5), (6)-(8) and s 194(2), (3), (6)-(8), Investigatory Powers Act 2016.
[184] Section 153(5) and ss 194(3), Investigatory Powers Act 2016. See also *The Queen (on Application of National Council for Civil Liberties (Liberty))* supra note 170 paras 287 and 302 (based on claimant's challenges).

destruction of material.[185] Any other alternative, in my view, would be a missed opportunity for safeguards appropriate to the use of powers of surveillance against journalists and lawyers.

(d) Lack of any adversarial processes

One of the key issues in the existing RICA 2002 model of prior judicial authorisation is the fact that applications for interception directions are inevitably made *ex parte* without notice. The provisions of ss 16(7)*(a)* applies with the necessary changes to the following investigative powers in RICA 2002: (1) application and issuing of a real-time communication-related direction in terms of ss 17(6); (2) a combined application and issuing of an interception direction, real-time communication-related direction and archive-related direction or interception direction supplemented by a real-time communication-related direction in terms of ss 18(3)*(a)*; (3) application and issuing of an archive-related direction in terms of ss 19(6); (4) amendment or extension of existing direction in terms of s 20(6); (5) application and issuing of a decryption direction in terms of ss 21(6); (6) the issuing of an entry warrant in terms of ss 22 (7). There is no adversarial process before the designated judge. Such a process appears to operate on the assumption that the designated judge is not misled and that the applicant of an interception direction will make a full disclosure on all the factors.

The nature of such applications means that the designated judge will be asked to determine the application in secrecy based on one-sided information presented by the law enforcement and the security and intelligence officials. There is no robust scrutiny mechanism to hear complaints about conduct in connection with interception of communications. As Duncan states: 'the granting of directions is an inherently one-sided process, which means that the judge has to take the information that is given to him on trust.'[186] It is only as a result of sustained pressure from civil rights campaigns and investigative journalism in South Africa that unlawful surveillance practices have been revealed.[187] It has also led to significant disclosures from law enforcement and security and intelligence agencies and to admissions of unlawfulness.[188]

The lack of any adversarial process in RICA 2002 implicates s 34 of the Constitution which provides that: '[e]veryone has the right to have any dispute that can be resolved by the

[185] Supra note 181 para 302 (based on claimant's challenges).
[186] Duncan op cit note 173 at 226.
[187] Op cit note 23, 77.
[188] Ibid. See *amaBhungane* case supra note 23 para supra note 23 paras 19-21.

application of law decided in a fair public hearing before a court or, where appropriate, another independent and impartial tribunal or forum.' A key component in the right to a fair hearing, in particular the principle of *audi alteram partem* – to hear the other side. This is premised on the rationale that a party should be given an opportunity of being heard before an order is made that might adversely affect their rights. The Constitutional Court in South Africa has been clear that principle of *audi alteram partem* is one of the main pillars of the s 34 right to a fair-hearing,[189] and has emphasised that 'even in an apparent 'open and shut' case, an affected party must be given an opportunity to meet the case advanced by an adversary.[190] The importance of the principle of *audi alteram partem*, captured by the often quoted passage in *John v Rees*, was endorsed by the Constitutional Court:

> 'As everybody who has anything to do with the law well knows, the path of the law is strewn with examples of open and shut cases which, somehow, were not; of unanswerable charges which, in the event, were completely answered; of inexplicable conduct which was fully explained; of fixed and unalterable determination that, by discussion, suffered a change.' [191]

The provision of a public advocate system in RICA 2002 has been suggested as a remedy to the unconstitutionality of s 16(7) by fulfilling the principle of *audi alteram partem* as a key pillar in the right to a fair hearing.[192] In terms of such a system 'the public advocate would be a practising legal representative and would be statutorily and ethically bound to represent and advance the interests and rights of the subject of surveillance in order to test the propositions put forward by the law enforcement agencies.'[193] The counter argument advanced by the state is that such a proposed public advocate system would cause lengthy application processes and undermine the security services capacity to act promptly in the interests of national security.[194] As such it was argued that consideration should be given to s 16(2)*(c)* which requires an application for an interception direction to 'contain full particulars of all the facts and circumstances' and 'enhanced by the duty on an applicant to behave as counsel are expected to do in *ex parte* applications and make truly full disclosure including factors adverse

[189] See *National Director of Public Prosecutions and Another v Mohamed NO and Others* 2003 (4) SA 1 (CC) at para 36.
[190] See *My Vote Counts NPC v Speaker of the National Assembly and Others* [2015] ZACC 31, majority judgment para 176.
[191] [1970] Ch 345 at 402.
[192] *amaBhungane* case applicants' heads of argument supra note 23 paras 120-122.
[193] Supra note 23 para 120.2.
[194] Supra note 23 para 120.2.

to the success of the application.'[195] The argument contends that 'at a practical level a public advocate, can do no more than a diligent judge would in any event do.'[196]

However, it is not 'apparent' that applicants for interception directions 'understand their ethical responsibilities.'[197] In practical terms, having regard to annual statistics referred below, seemingly very few applications are refused by the designated judge and a major contributing factor is undoubtedly the lack of any kind of adversarial challenge, because the interests of the subject/target as the proposed subject of surveillance are not effectively represented.[198] The numerous reports of incidents and allegations of abusive and unlawful surveillance practices by law enforcement and the security and intelligence agencies[199] reveal vulnerabilities in the regulatory framework of RICA 2002, which in the absence of an effective oversight regime can be appropriately described as 'neither transparent nor comprehensive.'[200]

The other objections of the state to a public advocate system relate to security risks such that 'it could lead to information being leaked because the circle of people with knowledge of the surveillance has been expanded.' This is an important consideration. A recognised deficiency in RICA 2002 is the lack of adequate controls on the onward sharing of such data. This problem of unrestricted data-sharing is also a key issue in RICA 2002 for its failure to prescribe adequate safeguards for access to and use of intercepted communications in terms of handling procedures. Irrespective of the mechanism adopted, whether this might involve the appointment of a special advocate or panel of judges, the absence of an effective adversarial procedure for the authorisation of interception of communications in RICA 2002 is no longer sustainable. Lawmakers must now consider the introduction of suitable internal mechanisms to enable *ex parte* applications for interception directions to be properly challenged prior to

[195] *amaBhungane* case supra note 23 para 76.
[196] Supra note 23 para 76.
[197] Supra note 23 para 76.
[198] Necessary and Proportionate *International principles* op cit note 161 at 23.
[199] Examples cited in *amaBhungane* case applicants' heads of argument supra note 23 para 204 include that the journalist, Athandiwe Saba's, phone records had been obtained in 2016 in terms of a s 205 warrant of the Criminal Procedure Act 51 of 1977, and such records may have been unlawfully provided by the SAPS and the NPA to a third party private investigator; the Mpumalanga province Premier David Mabuza announced in January 2015 that he was receiving briefings from State Security on the movements of journalists in the province, singling out Tom Nkosi, who is the founder and publisher of Mpumalanga investigative newspaper Ziwaphi, who Mr Mabuza alleged had met with Mr Mabuza's 'enemies' within the ruling party; and journalist Sipho Masondo, who was working on a series of investigations involving corruption in South Africa's water delivery projects, was informed by a source in crime intelligence that his calls were being intercepted.
[200] Attributed to Human Rights watch in submissions on oversight to D Anderson QC *A question of trust: Report of the investigatory powers review* (2015) Independent Reviewer of Terrorism Legislation available at *www.gov.uk/government/publications*, accessed on 17 May 2016 at 235.

authorisation being granted.[201] The court in the *amaBhungane* case agreed that 'measures are needed to overcome the absence of [an] adversarial process'[202] and declared s 16(7) of RICA as inconsistent with the Constitution, and as such invalid 'to the extent that it fails to adequately provide for a system with appropriate safeguards to deal with the fact that the orders in question are granted *ex parte*.'[203]

(e) Appointment of designated judges and independence

The controversial terrain with regard to designated judges is twofold: (i) empowering provisions for the appointment of a designated judge; and (ii) independence safeguards for the designated judge. 'Designated judge' in terms of s 1 of RICA 2002 'means any judge of a High Court discharged from active service under s 3(2) of the Judges' Remuneration and Conditions of Employment Act, 2001 (Act 47 of 2001), or any retired judge, who is designated by the Minister to perform the functions of a designated judge for purposes of this Act.' There is further provision in s 1 for 'Minister' which 'means the Cabinet member responsible for the administration of justice, except in Chapter 6 where it means the Cabinet member responsible for intelligence services.' The referred 'Minister' for the purposes of this discussion is the Minister of Justice and Correctional Services.

In arguments before the Constitutional Court in the *amaBhungane* case on 25 February 2020, the issue of the empowering provision in the appointment of the designated judge was first raised by Justice Chris Jafta, who asked Steven Budlender SC, counsel for amaBhungane and applicant Sole, whether there was any section in RICA 2002 empowering the Minister to appoint the designated judge.[204] Counsel responded that the power of appointment was granted by implication in the definition of 'designated judge' in s 1 as one who is 'designated by the

[201] See *amaBhungane* case supra note 23 para 80 where the court suggested that an alternative to a public advocate might be a panel of designated judges: '[t]hat might overcome the risk of tunnel vision and ensure a diversity of perspectives in the evaluative process. If three judges, say, were appointed and two had to approve an authorization, might that not be a better solution to balancing security of the information with the need to intensively interrogate the application?'
[202] *amaBhungane* case supra note 23 para 81.
[203] Supra note 23 para 82. The declaration of invalidity is suspended for two years, allowing the legislature time to cure the defect.
[204] See 'Top court questions surveillance laws' (February 2020) available at *https://mg.co.za/article/2020-02-28-top-court-questions-surveillance-laws/*, accessed 29 March 2020 and 'Power of minister to appoint Rica judge in spotlight at ConCourt' (February 2020) available at *https://www.timeslive.co.za/news/south-africa/2020-02-25-power-of-minister-to-appoint-rica-judge-in-spotlight-at-concourt/*, accessed 29 March 2020. See also J Duncan 'The loophole in South Africa's state spying laws' (March 2020) available at *https://www.dailymaverick.co.za/article/2020-03-09-the-loophole-in-south-africas-state-spying-laws/amp/?__twitter_impression=true*, accessed 31 March 2020.

Minister to perform the functions of a designated judge for purposes of this Act.' It is reported that Chief Justice Mogoeng retorted 'no, you can't exercise a power from a definition.' Counsel for the state conceded on the 'apparently unanswerable question' that there was no such empowering provision in RICA 2002. In response to a question from the Chief Justice on what should happen to the surveillance regime if the court found there was no power in RICA 2002 for the Minister to appoint the judge, counsel for the state responded: '[t]his means the court will have to craft a just and equitable order that will address the lacuna.'[205] This places the state contentions on the legality of RICA 2002 and its safeguards, which largely rests on authorisation by a designated judge in a difficult position.

On the issue of institutional safeguards for the designated judge, it was argued that RICA 2002 failed to secure the independence of the designated judge because the designated judge is appointed at the instance of a member of the executive, the Minister.[206] It was so contended that 'permitting a member of the executive to select one judge without any other process in place for such a sensitive constitutional function undermines the public confidence in the designated judge's independence and accordingly the constitutional requirement of independence.'[207] It was argued by the applicants that the role of the Minister of Justice, at his discretion alone, in selecting a judge to perform 'such an inherently contentious function' which is carried out in secrecy was 'to be an anathema to the independence of the designated judge:'[208] As a remedy to insufficient protection for the designated judge's independence, it was proposed that the designated judge must be selected following a proper public interview process before the Judicial Services Commission.[209] The other argument raised related to designated judge's term: '[t]here is no term specified under RICA for the designated judge. A term of one year has emerged as a matter of practice … the short duration and renewability of the designated judge's term has the potential to undermine the independence of the designated judge.'[210] It was argued on behalf of the applicants that '[s]ecurity of tenure requires protection against termination of employment or suspension at the discretion and behest of the

[205] Ibid.
[206] *amaBhungane* case applicants' heads of argument supra note 23 paras 134 and 144.
[207] Supra note 23 para 144.
[208] *amaBhungane* case supra note 23 para 62.
[209] *amaBhungane* case applicants' heads of argument supra note 23 para 144.
[210] Supra note 23 para 134. At para 141, remarks by the court in *Helen Suzman Foundation v President, RSA: in re Glenister v President, RSA* 2014(4) BCLR 841 (WCC) at para 68 were cited in support: [R]enewability of the term at the behest of the Minister is intrinsically inimical to independence. It is clear from the CC's judgments in Glenister 2 and JASA that it is renewability as such, rather than the insufficiency of conditions or constraints imposed on renewability, which jeopardises independence. Renewability thus has no valid place in the scheme of a unit that is constitutionally required to be adequately independent.'

Executive.'[211] Further, '[t]he secrecy of the process is aberrant to the usual judicial role and thus a greater need…exists to bolster the perceived and actual independence of the incumbent. The present system…fails dismally.'[212] In support of the importance of security of a designated judge's tenure, reference was made to Constitutional Court judgments, as explained by Moseneke DCJ and Cameron J:[213]

> 'While it is not to be assumed, and we do not assume, that powers under the SAPS Act will be abused, at the very least the lack of specially entrenched employment security is not calculated to instil confidence in the members of the DPCI that they can carry out their investigations vigorously and fearlessly. *In our view, adequate independence requires special measures entrenching their employment security to enable them to carry out their duties vigorously*.' [214]

Guidance on appointment of designated judges can be gleaned from the Investigatory Powers Act 2016[215] in the United Kingdom which offers an appropriate alternative remedy. Approval of interception warrants is by a group of Judicial Commissioners,[216] whom are appointed by the Prime Minister but only in consultation with, and by agreement with the Lord Chancellor, including the Lord Chief Justice of England and Wales, Scotland and Northern Ireland.[217] This is intended to provide a degree of judicial independence by ensuring that appointments by the Prime Minister cannot be regarded as 'tame' nor appointment of a 'former judge in return for patronage.'[218] Judicial independence is also in part secured by security of their tenure. Judicial Commissioners are appointed for a renewable fixed terms of three years. [219] Other than instances where a Judicial Commissioner is bankrupt, has a disqualification order from being a director or is convicted and receives a sentence of imprisonment (whether suspended or not), a Judicial Commissioner may not be removed from office before the end of the term of appointment, unless a resolution approving the removal has been passed by each House of Parliament.[220] The security of their tenure means that Judicial Commissioners cannot be removed from office if their decisions are contrary to the expectations of the state.

---

[211] *amaBhungane* case applicants' heads of argument supra note 23 para 139-141.
[212] *amaBhungane* case supra note 23 para 62.
[213] Supra note 23 para 62.
[214] *Glenister v President of the Republic of South Africa and Others* 2011 (3) SA 347 (CC) (referred to as 'Glenister II') para 222 (emphasis added). See also *Helen Suzman Foundation* case supra note 210 para 32
[215] Hereafter 'IPA 2016'.
[216] Section 23-25.
[217] Section 227-240.
[218] Gillespie op cit note 8 at 341.
[219] Section 228(2).
[220] Section 228(4) and (5).

I am not convinced that the question of the designated judge's independence as contemplated in RICA 2002, arguably 'compromised by the selection process and *de facto* unlimited duration of appointment'[221] is a failure in law. Chief Justice Mogoeng warned against impliedly maligning the integrity of judges, responding that once a judge was appointed, he or she was independent and, even after they retired, still received a salary pegged to the salary of active judges: '[y]ou've got to have something concrete to begin to question the independence of the judges. Just to say 'Okay, it's the minister who appointed her, [so] she must be, or she is potentially, the minister's lackey', I think it's a bit dangerous.'[222] Any suggestion of judicial impropriety 'serving in any capacity at the pleasure of the Minister'[223] as claimed by the applicants is therefore without substance and short-sighted. Perhaps the issue arising from the appointment process is more historical and institutional rather than being a questionable issue of the designated judge's independence.[224] As the High Court in the matter observed '[t]he present appointment process of the designated judge is plainly on the wrong side of history.'[225] The High Court ordered that subject to confirmation by the Constitutional Court, the Minister of Justice would continue to appoint the designated judge, but only on nomination from the Chief Justice and for a non-renewable term of two years. The Constitutional Court reserved judgment.

IV THE FUTURE OF INTERCEPTION OF COMMUNICATIONS IN SOUTH AFRICA

(a) '*...central to all of it, is interception*'[226]

Concerns of the 'broad intelligence mandate' in South Africa was highlighted by the Matthews Commission that '[a]n overly broad definition of security and overly broad intelligence mandate can lead the intelligence agency to focus in an inappropriate manner on lawful

[221] *amaBhungane* case supra note 23 para 61.
[222] 'Top court questions surveillance laws' (February 2020) op cit note 204.
[223] Supra note 23 para 64.
[224] Budlender responded that he was not questioning the integrity of any individual judge, and his argument was an institutional one. He referred to earlier judgments of the Constitutional Court and argued there would be a 'reasonable perception that a judge hand-picked by the executive for a renewable term is not going to be seen as independent.' As reported in 'Top court questions surveillance laws' (February 2020) op cit note 204.
[225] *amaBhungane* case supra note 23 para 64. At para 68, the court remarked impudently 'it must be an embarrassment to the Minister of Justice to have to select and appoint the designated judge in terms of the present provisions of RICA.'
[226] Attributed to a former intelligence operative in an article by H Swart 'You always feel like somebody's watching you? They probably are' *Daily Maverick* (June 2016) available at *https://www.dailymaverick.co.za/article/2016-06-03-you-always-feel-like-somebodys-watching-you-they-probably-are./*, accessed 16 September 2017.

political and social activities.'[227] Notwithstanding the dramatic events that led to the Matthews Commission, including the Commission's significant findings of apparent 'unlawful and unconstitutional'[228] surveillance practices by law enforcement and security and intelligence agencies, reports of such unlawful activities continued to emerge in post-democratic South Africa. In 2016, the state was asked to respond to the United Nations Human Rights Committee on its regulation of electronic surveillance, specifically on the following: '[i]nterception of communications outside the RICA regime would be unlawful, but, according to information before us, surveillance is being carried out outside the RICA regime. The Ministerial Review Commission on Intelligence, known as 'Matthews Commission' found that the National Communications Centre (NCC) carries out unlawful surveillance.'[229] The state responded as follows: '[t]he Report was never officially adopted. The Report was finalised in 2008. However, even if the NCC was used for illegitimate interceptions, it was used in limited circumstances only and not officially sanctioned. …[A]dequate measures were implemented to curb any further abuses.'[230] The state's response is unconvincing, albeit conceding to the 'illegitimate' conduct of the NCC in its operational activities. Concessions that it only happened in 'limited circumstances' and was 'not officially sanctioned' is hardly justification for such conduct and ignores the doctrine of legality.[231] Contrary to the written submissions by the state, the conduct of the NCC acting without lawful authority or judicial supervision continued and without adequate measures capable of preventing abuse of power.

Despite these concerning issues raised, including those by the Matthews Commission in 2008, and by numerous other entities in between, a decade later the Supreme Court of Appeal in *Zuma v Democratic Alliance and Others*[232] noted with 'unsettling' concern 'that different law enforcement agencies of government appear to be spying upon each other.'[233] The court, in particular, was concerned about the authenticity and legality of the recorded conversations,

[227] The Matthews Commission op cit note 22 at 73.
[228] Ibid at 180.
[229] South Africa's written responses to the UN Human Rights Committee following South Africa's review ref 50/2016 (10 March 2016) para 26.3 available at *https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/ZAF/INT_CCPR_AIS_ZAF_23518_E.pdf*, accessed 2 April 2020.
[230] Ibid para 26.3.
[231] The rule that the principle of legality functions as a restriction on the exercise of public power in South Africa's new constitutional order may be traced back to the Constitutional Court's judgment in *Fedsure Life Insurance v Greater Johannesburg Transitional Metropolitan Council* 1999 (1) SA 374 (CC). At para 58, the Court stated that the doctrine of legality is 'central to the conception of our constitutional order that the legislature and executive in every sphere are constrained by the principle that they may exercise no power and perform no function beyond that conferred upon them by law.' See also *Pharmaceutical Manufacturers'* case op cit note 48.
[232] 2018 (1) SA 200 (SCA).
[233] See references earlier, including op cit note 77.

which was considered vital in the decision by the then acting National Director of Public Prosecutions to discontinue the prosecution of former President, Mr J Zuma on serious criminal charges. The court held that the authenticity and legality of the recorded conversations 'ought' to have received 'greater consideration' particularly as judicial authorisation for the recordings in terms of RICA 2002 requirements was not made available despite its 'very specific requirements' intended to ensure that no infringement of rights took place other than in the manner provided for by law.[234]

Justice Yvonne Mokgoro is the designated judge appointed to adjudicate warrants in terms of RICA 2002 on which she is required to publish annual reports. The reports are presented to the parliamentary Joint Standing Committee on Intelligence,[235] comprising of members of the six largest political parties in South Africa. The contents of the reports by the designated judge are considered by the JSCI and dealt with mostly in a classified manner. Publication of these reports by the JSCI are intermittent, with the most recent publicly available report covering the period 2014/2015. In the report, Justice Mokgoro highlighted the following, acknowledged concerns of unfettered discretion and abuse of powers by law enforcement and security and intelligence agencies that do not appear speculative or 'in limited circumstances':

> 'There is a continued general public perception that some law enforcement and other institutions and/or officers use these intrusive interception methods to advance their own interests with no regard to the rights and values the RICA aims to protect in the context of the Constitution. The media, in particular the social networks, are inundated with reports, allegations and comments of manipulation and abuse of the interception system by officials and even individuals, ranging from–
>
> - obtaining of information in less than 36 hours, without the Designated Judge's knowledge;
> - acquisition of cell phone billing and ownership records through crime intelligence, without the Judge's knowledge or approval, in order to expedite the investigation; obtaining text messages and cell phone billing records needed for personal reasons, through a contact at crime intelligence and/or the service providers;
> - the popularity of interception method which is preferred over conventional methods of investigation;

[234] Supra note 232 para 63.
[235] Hereafter 'JSCI'. It is one of only two bodies that oversee the intelligence services in South Africa. The other is the Inspector-General of Intelligence, which reports to the JSCI.

- the apparent lack of trust of the Designated Judge with regard to information gathered through crime intelligence;
- failure of applicants to provide fact-based justification for an application to the Judge;
- applicant's need to comprehend that suspicion of crime without any factual basis is not sufficient for application for interception;
- the tendency for vagueness of basis for an application, the cut and paste approach to an affidavit and the tendency to regard the authorisation for interception as a given and therefore the taking and
- wide allegations of bribery of contacts at banks and telecommunications service providers etc.'[236]

The report also provided statistical information of applications for directions,[237] revealing significant increases in applications inter alia from the Crime Intelligence Division[238] and the State Security Agency:[239]

Agency	**2013/2014**	**2014/2015**
State Security Agency	231	348
Applications declined	5	10
Crime Intelligence Division	219	386
Applications declined	0	0

Reasons for the increase in application numbers are unknown. The state has argued that we should not worry about the interception of communications because interception directions are rare. In a request for written responses from the state, the UN Human Rights Committee specifically referred to the following: '[a]ccording to the written replies, interception of communications occurs "in exceptional cases". However, according to the Annual Report of the Joint Standing Committee on Intelligence, of the 387 directions sought under RICA, only

[236] *Annual report on the interception of private communications* 15 October 2015 available at *http://pmg-assets.s3-website-eu-west-1.amazonaws.com/intelligence.pdf*, accessed 22 June 2019. See also P Du Toit 'A judge's report shows SA's police, spies are requesting more wiretapping' (20 December 2012) available at *https://www.huffingtonpost.co.uk/2016/12/20/parliament-isnt-happy-sas-police-spies-are-requesting-more-wi_a_21631740/?_7trCw* accessed 22 June 2019; J Duncan 'New year's resolution for 2017: Stop unaccountable state spying' (8 January 2017) available at *https://www.dailymaverick. co.za/article/2017-01-08-new-years-resolution-for-2017-stop-unaccountable-state-spying/*, accessed 22 June 2019; J Duncan 'Op-Ed: What Ramaphosa needs to do to fix state spying, Part One: Rica and lawful interception' (19 February 2018) available at *https://www.dail maverick.co.za /article/2018-02-19-op-ed-what-ramaphosa-needs-to-do-to-fix-state-spying-part-one-rica-and-lawful-interception/*, accessed 22 June 2019; and J Duncan 'Government's thinking on surveillance law is regressive' (5 June 2019) available at *https://mg.co.za/article/2019 -06-05-governments-thinking-on-surveillance-law-is-regressive*, accessed 22 June 2019.
[237] Annual report on the interception of private communications' op cit note 236 at 48-52.
[238] Hereafter 'CID'.
[239] Hereafter 'SSA'.

5 were refused. If that is the case, can one still say that interception occurs only in exceptional cases?'[240] The state responded: '[t]aking into account that the total population of South Africa is in the region of 50 Million persons, it is submitted that the amount of interceptions which take place is relatively insignificant. Since only an "applicant" (which is a senior officer at the law enforcement agency), can approach the judge for a direction, various applications [are] already refused at Departmental level. Only applications which [have] real merit are sent through to the office of the designated judge.'[241]

The state's response is yet again unsatisfactory. Whilst 387 directions may not seem as a significant number to the state – if only 5 interception directions were refused by a designated judge out of 387 directions sought, this raises key questions about the robustness and effectiveness of the procedural safeguards in RICA 2002. A one hundred per cent success for the CID and an almost one hundred per cent success for the SSA appear to reveal a 'long-standing tendency' for the designated judge to refuse 'only a fraction' of applications.[242] For majority of the applications, it does not appear that any were disputed by the designated judge.

The one-sidedness and bias towards the applicants is therefore almost inevitable, as RICA ensures that the application process is not adversarial.' [243] The ripple effect is exacerbated by issues relating to blanket prohibition on user notification and lack of oversight mechanisms in RICA 2002. The success rate of application numbers is a disturbing trend, and the concluding remarks of Justice Mokgoro is compelling that we should not be 'blinded' to concerns of abuse and arbitrary interference with our rights.[244] Justice Mokgoro goes further to question the purported success of interception as an investigative method in the prevention and detection of criminal activity as one that 'is not easily discernible' and 'highly subjective.'[245]

Another key concern relates to the unregulated use of international mobile subscriber identity catchers, known 'IMSI catchers' or 'grabbers'. Justice Mokgoro's report omits any mention of IMSI catchers and is limited to conventional interception. IMSI catchers are mobile

[240] South Africa's written responses to the UN Human Rights Committee op cit note 229 at para 26.5.
[241] Ibid para 26.5. See chapter three below at 118-124, where the provisions of s 205 of the Criminal Procedure Act 51 of 1977 are considered as a parallel process for law enforcement and security and intelligence agencies that provides different sets of rules for essentially the same measures, which in practise is less strictly regulated under different standards of conduct and authorisation. The contrast in the numbers between s 205 subpoenas (estimated between twenty-five to fifty thousand annually) and RICA 2002 directions (a few hundred annually) for obtaining electronic information is remarkable.
[242] Duncan 'New year's resolution for 2017: Stop unaccountable state spying' op cit note 236.
[243] Ibid.
[244] *Annual report on the interception of private communications* op cit note 236 at 52.
[245] Ibid at 52.

interception devices that make it possible for law enforcement and security and intelligence agencies to intercept communications without having to involve third party telecommunication service providers.[246] The use of ISMI catchers is intrusive and invasive technology that can be used to indiscriminately monitor communications in real-time, without user knowledge, by tracking and locating mobiles phones that are switched on in a particular area. With varying capabilities a basic model is limited to detecting the location of a device, but more sophisticated catchers can monitor internet communications and messenger services of a single device, or intercept communications of multiple devices, simultaneously, and store them.[247]

The use of these types of invasive technology devices is not regulated by RICA 2002, and there is no corresponding evidence to support the contention that law enforcement and security and intelligence agencies apply for the issue of directions before its use.[248] In response to whether the necessary RICA 2002 processes are followed for the use of ISMI catchers, a former crime intelligence official is reported to have stated: 'No! No. That stuff is all illegal … All of it! Where are you going to find a judge who you can convince to quickly approve the thing for you on a 12-hour basis, in a place like Newcastle or Estcourt?'[249] In 2015, concerns about the use of such technology was raised by the Parliament Joint Standing Committee on Intelligence which expressed its intentions to 'revisit RICA with a view of whether any changes would be required to strengthen the Act in the likely event that the Judge is not sufficiently empowered to deal with matters such as grabbers.' [250] To date there has been no such meaningful amendments to RICA 2002. The concerns are exacerbated in that the technical capabilities of law enforcement and security and intelligence agencies to conduct surveillance are 'unknown' and the state 'refuses to respond to requests of more information under the policy that they cannot "disclose" operational details and capabilities.'[251]

---

[246] Hosein and Palow op cit note 84 at 1086; See also J Duncan, 'Spies are all set to grab your metadata' (11 September 2015) available at *https://mg.co.za/article/2015-09-10-spies-are-all-set-to-grab-your-metadata*, accessed 30 June 2019.

[247] For an account of the use of ISMI catchers see H Swart 'How cops and crooks can "grab" your cellphone – and you' (November 2015) available at *https:// mg.co.za/article/2015-11-29-how-cops-and-crooks-can-grab-your-cellphone-and-you*, accessed February 2019.

[248] Privacy International, Right2Know, and the Association for Progressive Communications 'Submission in advance of the consideration of the periodic report of South Africa, Human Rights Committee, 116th Session, 7-31 March 2016' (March 2016) available at *https://www.apc.org/en/pubs/submission-advance-consideration-periodic-report-s*, accessed 02 July 2019.

[249] Swart 'op cit note 247. Swart's reference to Newcastle and Estcourt are notably small rural towns in South Africa's Kwazulu-Natal province.

[250] Ibid at 3-4, referring to Parliament's Joint Standing Committee on Intelligence November 2015 available at *http://www.parliament.gov.za/live/content.php?Item_ID=8495*.

[251] Ibid 3, referring to response from spokesperson for the State Security Agency in Swart op cit note 247.

In a another recorded and controversial incident, a telecommunication signal jamming device was used in Parliament unlawfully.[252] On 12 February 2012, then President of South Africa, Jacob Zuma, was scheduled to deliver the annual State of Nation Address at a joint session of Parliament. As soon as the sitting began, the SSA, without seeking permission from Parliament, used a telecommunication signal jamming device that disrupted telecommunication signals inside the Chamber, depriving members of the Parliament and journalists from using their mobile phones to inform the public about the State of Nation Address. In a case brought by Primedia Broadcasting, an independent South African media company, and a number of local and international non-governmental organisations, the court found that the state's use of a telecommunication signal jamming device to temporarily disrupt communications during the session without the permission of Parliament was unlawful.

The legal challenge by the amaBhungane Centre for Investigative Journalism to the constitutionality of RICA 2002 is a remarkable development in South African law. The outcome thereof even more so, as certain provisions of RICA 2002 have been declared inconsistent with the Constitution, and accordingly invalid.[253] The question of whether the South African courts or the legislature are the more appropriate forums to address the use of these investigative powers by law enforcement and the security and intelligence agencies, is debatable.[254] Indeed, the respondents in the matter, including inter alia the Minister of Justice and Correctional Services, Minister of State Security and Minister of Communications argued that the challenges to RICA 2002 as raised by the applicants were 'premature' and stated that 'the state is at work adapting RICA [2002]' and 'should be left to get on with the task.[255] In rejecting the argument, the respondents were found wanting in demonstrating progress: 'it must be asked what is the State actually doing?'[256] Irrespective of arguments of prematurity, the court referred to Constitutional Court precedent stating 'that there can be no merit in delaying a challenge to the inconsistency of a statute with constitutional norms on the ground that a repair job on the statute is work-in-progress.'[257] Moreover, as observed by the court that 'given the spirited resistance to almost every contention advanced by the applicant in criticising RICA [2002], there can be no expectation that the reforming legislation, which we are told is being

[252] *Primedia Broadcasting v Speaker* (784/2015) [2016] ZASCA 142 (29 September 2016).
[253] *amaBhungane* case supra note 23.
[254] Hosein and Palow op cit note 84 at 1089.
[255] *amaBhungane* case supra note 23 para 7.
[256] Supra note 23 paras 8-9.
[257] Supra note 23 paras 11-12, with reference to *Mazibuko v Sisulu* 2013 (6) SA 249 (CC) para 70.

contemplated at this time, is in the least benign towards the criticisms advanced and solutions offered to address the criticisms.'[258]

The court noted the 'several examples of abuse' some undisputed, to which 'no rebuttal or explanation or effort to justify the interception' which only 'became public knowledge fortuitously.'[259] The court recognised that the risk of abuse and exercise of investigatory powers without lawful authority was 'not academic in South Africa'[260] Among them, the court noted that it was 'common cause that at least one applicant [of an interception direction] lied blatantly to a designated judge to obtained an interception order in respect of the journalists Hofstatter and Wa Afrika, claiming falsely that their details were that of criminals. The designated judge, doubtless in good faith, was taken in by the lies and authorised a surveillance for a corrupt purpose.'[261]

This reflects a fundamental imbalance in South African law. For many years the lack of effective oversight regimes and clear statutory authority for these investigative powers shielded law enforcement and security and intelligence agencies from oversight and public scrutiny. At a general level, concerns with the legislative framework of RICA 2002 are far from new. However, they have taken on a renewed intensity following the *amaBhungane* case. What is clear is that the outcome of this public interest litigation will now force parliament to address the constitutionality of RICA 2002, and the 'concrete question' of how the use of emerging surveillance technologies as an intelligence gathering and investigative capability should be regulated in South African law with sufficient safeguards against risk of abuse.[262] Greater transparency is needed by law enforcement and security and intelligence agencies exercising these investigative powers. In the preceding analysis it has become clear that some of these investigative powers do not have a clear and explicit basis in legislation. They include inter alia bulk interception, foreign signal surveillance, IMSI catchers and signal jamming devices. It is therefore important that broad powers such as bulk interception must be set out in legislation after full and proper public consultation and debate. In order to ensure accountability for surveillance, an independent oversight authority should be required to notify the subject/target of interception surveillance after an investigation or operation has terminated, unless there is an objectively justifiable reason for maintaining secrecy. There must also be the

[258] Supra note 23 para 12.
[259] Supra note 23 paras 19 and 21.
[260] Supra note 23 para 43.
[261] Supra note 23 para 20.
[262] Hosein and Palow op cit note 84 at 1089.

introduction of suitable internal mechanisms to enable *ex parte* applications for interception directions to be properly challenged prior to authorisation being granted.

I believe that a comprehensive review of all the investigative powers in RICA 2002 is necessary to ensure that the powers are used to its greatest potential with minimal interference with individual rights. The safeguards contained within the new law must be capable of preventing abuse of power.

V CONCLUSION

As the year 2020 information age continues to rapidly evolve with a modern fast-paced environment of technological advancements dominated by connectivity, data and devices, the stakes are extremely high. Leaning on policy remarks by the then newly elected South African President The Honourable Cyril Ramaphosa and his 'new deal' for South Africa[263] – in the context of interception of communications 'the essence of a new deal'[264] is between the South African government and its citizens: '[a] clear and transparent new legal framework and a more coherent, visible and effective oversight regime should be the basis for a public discussion about the appropriate and constrained power the…state should have to intrude into the lives of its citizens.'[265]

The second deal would be the relationship between government and third party telecommunication service providers[266] and the legal responsibilities on the latter in terms of RICA 2002. This relationship, including obligations of third party telecommunication service providers and the impact on individual right to privacy are key considerations in chapter three to follow.

[263] 'Ramaphosa proposes a new deal for South Africa' (November 2017) available at *https://www.fin24.com/economy/ramaphosa-proposes-a-new-deal-for-south-africa-20171113*, accessed 25 February 2019 and 'Ramaphosa: My new deal for SA – and 10-point action plan for jobs, growth, transformation' (November 2017) available at *https://www.biznews.com/thought-leaders/2017/11/14/ramaphosa-new-deal-for-sa/*, accessed 25 February 2019.
[264] RUSI op cit note 35 at 103.
[265] Ibid.
[266] Ibid.

CHAPTER THREE

INVESTIGATORY POWERS IN RELATION TO COMMUNICATIONS DATA: OBTAINING EVIDENCE FROM THIRD PARTY TELECOMMUNICATION SERVICE PROVIDERS

I INTRODUCTION

Perhaps the most controversial investigatory power in recent times relates to communications data. It is an issue that poses challenges for the law. There are two worrying trends in South African law. First, legislation in the form of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 Of 2002[1] has not kept pace with a modern fast-paced environment of technological advancements, particularly in relation to communications data. At the time of RICA 2002 coming into law, traditional investigative powers on surveillance of communications were established within a traditional technological environment;[2] when communications data was regarded to be less intrusive than the content of a communication. This reflected a period when 'the plain-old-telephone system' was predominantly in use and communications data was simply information about the person calling or the person called, and the duration.[3] Accordingly, one level of privacy protection was assigned to communications data, and another was applied for lawful access to the content communications.[4] The differing authorisation procedures in RICA 2002 similarly reflect a legal construct that distinguishes between what kinds of information implicate greater (content) or lesser (communications data) privacy interests. This distinction is based on the fact that because the content of the communication cannot be accessed it is, therefore, not as intrusive.

Second, the policy language developed in RICA 2002 sustained through technology-neutral terminology now gives law enforcement and security and intelligence agencies in 2020, access to highly sensitive information under the lesser privacy protections envisaged for communications data almost two decades ago.[5] The challenge for the law is aptly reflected by the United Nations Special Rapporteur on Freedom of Expression, Frank LaRue, in concerns expressed in a report:

---

[1] Hereafter 'RICA 2002'.
[2] I Hosein and A Pascual 'Understanding traffic data and deconstructing technology-neutral regulations (2002) at 1 available at *http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=55CB1A20C3B31F1687 2328C4273 EED 75?doi=10.1.1.475.5291&rep=rep1&type=pdf*, accessed 12 March 2020.
[3] Ibid.
[4] Ibid.
[5] Ibid 7-8.

> '[L]egislation has not kept pace with the changes in technology. …legal standards are either non-existent or inadequate to deal with the modern communications surveillance environments. As a result, States are increasingly seeking to justify the use of new technologies within the ambits of old legal frameworks, without recognizing that the expanded capabilities they now possess go far beyond what such frameworks envisaged. … this means that vague and broadly conceived legal provisions are being involved to legitimize and sanction the use of seriously invasive techniques.'[6]

Ever since electronic surveillance has become mainstream as an investigative power, it has been touted as 'simply using the by-product of communication devices as evidence to identify and tackle crime' with 'repeated assurance' of the fact that because content is not accessed, access to communications data is therefore 'somehow' not intrusive.[7] The counter argument, however, is that such a position in the information age is 'disingenuous'.[8] A modern fast-paced environment of technological advancements now means that monitoring communications data over a period of time could reveal sensitive content and detailed understanding of a person's life.[9]

What does this mean for our privacy interests in 2020, when telecommunication service providers are legally required to retain our communications data, and for its acquisition by law enforcement and security and intelligence agencies now performing expanded and highly intrusive capabilities under investigative powers in RICA 2002 which was established with traditional technological environments in mind? Part II begins with an analysis of the obligations of telecommunication service providers in RICA 2002 with regard to mandatory data retention. This is followed by an examination of the investigatory powers of law enforcement and security and intelligence agencies to acquire communications data. The key issues identified relate to the process of authorising the acquisition of communications data, procedures in RICA 2002 for storing, accessing, examining, using and destroying the communications data. Completing the analysis is a consideration of s 205 of the Criminal Procedure Act 25 of 1977 as a parallel process for law enforcement and security and

[6] United Nations Human Rights Council 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank LaRue' A/HRC/23/40 (17 April 2013) at 13 available at *https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf*, accessed 4 July 2019.
[7] AA Gillespie *Cybercrime: Key Issues and Debates* (2019) at 339. See also AA Gillespie 'Regulation of Internet surveillance' (2009) *European Human Rights LR* 552.
[8] Ibid.
[9] Ibid.

intelligence agencies to obtain communications data from third party telecommunication service providers. Part III concludes the chapter.

II COMMUNICATIONS DATA AND THE REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT 70 OF 2002

Any discussion on electronic surveillance often invokes Bentham's panopticon[10] and the metaphor of Big Brother from George Orwell's famous novel *Nineteen Eighty-Four* (1949) about a state that uses a bureaucratic apparatus, the 'Thought Police' and the figure of 'Big Brother' on an ever-present telescreen to intervene in the smallest details of its citizens daily lives.[11] The word 'surveillance' is etymologically associated with the French word 'surveiller' which translates simply as 'to watch over'. Both in ordinary language and within academic debate, the practice of 'watching over' has become synonymous with monitoring activities.[12] Leading the discourse of 'Orwellian' concerns and fears of 'Big Brother tactics'[13] Rule explains:

> 'Why do we find the world of *1984* so harrowing? Certainly one reason is its vision of life totally robbed of personal privacy, but there is more to it than that. For the ugliest and most frightening thing about that world was its vision of the total control of men's lives by a monolithic, authoritarian state. Indeed, the destruction of privacy was a means to this end, a tool for enforcing instant obedience to the dictates of the authorities.'[14]

---

[10] T McMullan 'What does the panopticon mean in the age of digital surveillance?' (2015) available at *https://www.guardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham*, accessed 26 October 2016, sets out the basic idea of philosopher, Jeremy Bentham's panopticon as: 'there is a central tower surrounded by cells. In the central tower is a watchman. In the tower are prisoners – or workers, or children, depending on the use of the building. The tower shines bright light so that the watchman is able to see everyone in the cells. The people in the cells, however, aren't able to see the watchman, and therefore have to assume that they are always under observation.'

[11] See P Bernal 'Data gathering, surveillance and human rights: recasting the debate' (2016) 1.2 *Journal of Cyber Policy* 243 and D Lyon 'Bentham's panopticon: from moral architecture to electronic surveillance' (1991) 98.3 *Queen's Quarterly* 596.

[12] A Albrechtslund 'Online social networking as participatory surveillance' (2008) available at *http://firstmonday.org/article/view/2142/1949*, accessed 26 October 2016.

[13] A Albrechtslund 'Surveillance and ethics in film: *Rear window* and *the conversation*' (2008) *Albany Journal of Criminal Justice and Popular Culture* available at *http://www.albany.edu/scj/jcjpc/vol15is2/Albrechtslund.pdf*, accessed 26 October 2016. See also D Lyon *The Electronic Eye: The Rise of Surveillance Society* (1994) at 57-80 for a chapter discussing Big Brother and the Panopticon as a metaphor in the context of computer surveillance.

[14] JB Rule *Private Lives and Public Surveillance* (1973) 16. See also NM Richards 'The Dangers of Surveillance'(2013) 26 *Harvard LR* 1934 and B Keenan 'Contingency and Surveillance: Framing the Risk of Taking Risks' (2014) 2.2 *Birbeck LR* 293.

Beyond Bentham's panopticon and Orwell's *Nineteen Eighty-Four*, what happens in the world of electronic surveillance where 'in the panopticon the occupants are constantly aware of the threat of being watched…but state surveillance on the internet is invisible; there is no looming tower, no dead-eye lens staring at you every time you enter a URL.'[15] The analogy is that because we have knowledge that our communications data is being retained, then we will use our devices appropriately because we will never know when our data will be accessed by law enforcement and security and intelligence agencies.[16] The relative intangibility of electronic surveillance (as opposed to CCTV, which offers a more physical sense of exposure in the tower by watchmen or thought police) is such that neither Bentham nor Orwell could have imagined the extent to which our communications data is 'watched over' and *retained* by third party telecommunication service providers, including for the *acquisition* of such data by law enforcement and security and intelligence agencies.[17] Retention and acquisition of communications data therefore has far-reaching implications for electronic surveillance activities for individual rights.[18] Solove explains the challenges:

> 'Surveillance is a sweeping form of investigatory power. It extends beyond a search, for it records behaviour, social interaction, and everything that a person says and does. Rather than targeting specific information, surveillance can ensnare a significant amount of data beyond any originally sought. If watched long enough a person might be caught in some form of illegal or immoral activity. … Moreover, unlike a typical search, which is often performed in a short once-and-done fashion, electronic surveillance "continues around-the-clock for days or months". … Part of the harm is simply not being watched, but in the lack of control that people have over the watchers. Surveillance creates the need to worry about the judgment of the watchers. Will our email be misunderstood? Will our confidential information be misunderstood? What will be done with the information gleaned from surveillance?'[19]

Bernal observes that the main difference between Bentham's panopticon (retention, and never knowing when we are watched) and electronic surveillance (acquisition) is that the latter has been designed in legislative frameworks for certain specified purposes, whereas retention of communications data by third party telecommunication service providers is performed for

[15] Ibid.
[16] Gillespie op cit note 7 at 339.
[17] Rule op cit note 14.
[18] D Trottier and D Lyon 'Key Features of Social Media Surveillance' in C Fuchs, K Boersma, A Albrechtslund and M Sandoval (eds) *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (2012) 89-105.
[19] DL Solove 'Digital Dossiers and the Dissipation of Fourth Amendment Privacy (2002) 75 *Southern California LR* 1083 at 1092.

everyone.[20] What this means in reality is that 'whilst the *retention* of [communications] data does not require anyone to be suspected of a criminal offence' it will be seen from the legislative framework of RICA 2002 that 'the *acquisition* of data can only be for specified purposes',[21] including for the prevention and detection of 'serious offences' or in the interests of 'national security or compelling national economic interests' if the 'reasonable grounds to believe' threshold has been met.[22] RICA 2002 also sets out a core provision in relation to mandatory retention of communications data by telecommunication service providers.[23]

(a) Retaining communications data

Communications data has always been likened to the 'who', 'when' and 'where' of a communication, but not the content of what was said or written.[24] RICA 2002 refers to communications data as 'communication-related information. It does not provide such a simple definition, although its likeness to the 'who', 'when' and 'where' of a communication can be gleaned from the definition adopted. For the purposes of retention this is defined as 'any information relating to an indirect communication which is available in the records of a telecommunication service provider, and includes *switching, dialling or signalling information* that identifies *the origin, destination, termination, duration, and equipment* used' and the location of the user within the telecommunication system.'[25] The definition of communications data is broad, and appears to exclude content of a communication which is defined in RICA 2002 as 'when used with respect to any communication, includes any information concerning the substance, purport or meaning of that communication.[26] RICA 2002 further delineates its

[20] Bernal op cit note 11 at 250 and Gillespie op cit note 7 at 339.
[21] Gillespie op cit note 7 at 339-40 (emphasis in original).
[22] Section 17 and 19. See also *Nampak (Pty) Ltd v Vodacom (Pty) Ltd and Others* 2019 (1) SA 257 (GJ) para 2 for a 'novel' application in which third parties can gain access to information held by telecommunication service providers to enable it to identify wrongdoers so as to take appropriate legal action against the perpetrators. In this instance, Nampak sought information from the relevant telecommunication service providers to be able to identify wrongdoers who robbed Nampak's premises, in advance of any litigation having been instituted. The order, unopposed by the telecommunication service provider, was circumscribed by the court in terms of content of the information to be accessed, duration and destruction of the information provided, including a bar on user notification for three months.
[23] Section 30.
[24] Home Office *Acquisition and disclosure of communications data – Code of Practice* (TSO 2007) available at *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf*, accessed 4 July 2019.
[25] Section 1 (emphasis added). 'Indirect communication' is defined to mean 'the transfer of information, including a message or any part of a message, whether- (a) in the form of- (i) speech, music or other sounds; data; (ii) text; (iii) visual images, whether animated or not; (iv) signals; or (v) radio frequency spectrum; or (b) in any other form or in any combination of forms, that is transmitted in whole or in part by means of a postal service or a telecommunication system.'
[26] Section 1.

provisions on communications data between *real-time* (immediately available up to 90 days after transmission) communication-related information and *archived* (stored after the 90 day transmission period) communication-related information, and its authorisation and warrantry process is referred to as a 'direction'.[27]

Section 30(1)*(b)* requires that 'notwithstanding any other law' a telecommunication service provider '*must* store' communications data. This is the core provision in RICA 2002 in relation to mandatory retention of communications data by telecommunication service providers. Section 30 also grants the Minister of Communications the power to issue a 'retention directive' in respect of that telecommunication service provider determining the '*type* of communication-related information which must be stored' and the '*period* for which such information must be stored' which period may 'not be less *than three years and not more than five years* from the date of the transmission of the indirect communication to which that communication-related information relates.'[28]

The issuing of a retention directive by the Minister is not linked to any specified purpose, such as for the prevention and detection of 'serious offences' or in the interests of 'national security or compelling national economic interests.' Further, the decision to issue a retention directive is not required to be approved by a judicial authority. There is no requirement to prove that such measure is necessary and proportionate. RICA 2002 effectively allows the state to require telecommunication service providers to perform untargeted and indiscriminate mandatory retention of communications data. Concerns about untargeted and indiscriminate mandatory retention of communications data raises questions about the 'increasing reliance' on third party telecommunication service providers 'to retain data "just in case" it is needed for government purposes'[29] to be able to 'preserve evidence of historic

[27] Section 1. For example, a direction issued under s 17(3) or s 18(3) means that a telecommunication service provider is directed to provide real-time communication-related information in respect of a customer, on an ongoing basis, as it becomes available.
[28] Section 30(2)*(a)(iii)* (emphasis added).
[29] Human Rights Council 'The right to privacy in the digital age' A/HRC/27/37 (30 June 2014) at 6-7 available at *http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf*, accessed 04 January 2016 at 9. D McKinley 'New terrains of privacy in South Africa' December 2016 at 16 available at *https://www.mediaa nddemocracy.com/uploads/1/6/5/7/16577624/r2kmpdp_new_ terrains_ of_ privacy_in_south__africa_masterset_small.pdf*, accessed February 2019. See also A Mare & J Duncan 'An analysis of the communications surveillance legislative framework in South Africa' (November 2015) at 20 available at *https://www.mediaandd emocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf*, accessed February 2019: 'RICA does not specify what kind of 'capability' is required, this facilitates unknown and unregulated equipment to be built into networks/systems, leaving users completely in the dark and compromising the integrity of the entire system. …this introduces vulnerabilities into the network…there is no information in the public domain about how these security holes haves been abused or what, if anything, has been or is being done about it.'

criminality.'[30] The bulk of communications data retained by telecommunication service providers will therefore be irrelevant to any investigation or operation.[31] Section 30(1)*(a)* requires that a telecommunication service provider '*must* provide a telecommunication service which has the capability to be intercepted.' Beyond this obligation, RICA 2002 does not specify the type of 'capability' or what is allowed by telecommunication service providers nor any protections against abuse or arbitrary interference such as safeguards relating to retention, disclosure and destruction of retained data. This means that retention of communications data by third party telecommunication service providers is performed for everyone[32] for a period between three and five years and does not require anyone to be suspected of a criminal offence or for the data to be retained for any specified purpose.

As referred earlier in chapters 1-2, the Constitution Republic of South Africa Act 108 of 1996 confers upon everyone the right to privacy, including the right not to have their person or home searched, their property searched, their possessions seized, or the privacy of their communications infringed.[33] The section itself places no limits on the right. This does not mean, however, that the right to privacy is protected against the general limitation clause contemplated in s 36 of the Constitution. Nor does the Constitution accord hierarchical precedence to any particular right entrenched in the Bill of Rights over other rights referred to therein.[34] In determining the constitutionality of alleged violations of rights, a two-stage approach is applied by the courts underpinned by a limitations justification.[35]

In terms of the Constitution the right to privacy may be limited provided the limitation is justified.[36] That s 30 of RICA 2002 infringes on the right to privacy is not disputed by the

[30] D Anderson QC *A question of trust: Report of the investigatory powers review* (2015) Independent Reviewer of Terrorism Legislation available at *www.gov.uk/government/publications*, accessed on 17 May 2016.
[31] G Hosein and CW Palow 'Modern safeguards for modern surveillance: An analysis of innovations in communications surveillance techniques' (2013) 74.6 *Ohio State LJ* 1071 at 1092.
[32] Bernal op cit note 11 at 250 and Gillespie op cit note 7 at 339.
[33] Hereafter 'the Constitution'. Other constitutional rights implicated by RICA 2002 provisions on untargeted and indiscriminate mandatory retention of communications data include the right of access to courts (s 34); the right to freedom of expression and the media (s 16); and the right of legal privilege protected by sections 34 and 35 of the Constitution. However, paramount to concerns about the constitutionality of RICA 2002 in general relate to the right to privacy, and hence dealt with in more detail. The other constitutional rights are analysed to the extent that the discussion focuses on other particular challenges with RICA 2002 provisions, such as legal privilege.
[34] *Johncom Media Investments Limited v M and Others* 2009 (4) SA 7 (CC) para 19.
[35] See *Coetzee v Government of the Republic of South Africa* 1995 (4) SA 631 (CC) para 9. See also *Moise v Greater Germiston Transitional Local Council: Minister of Justice and Constitutional Development Intervening (Women's Legal Centre as Amicus Curiae)* 2001 (4) SA 491 (CC) para 7; *S v Williams and Others* 1995 (3) SA 632 (CC) para 54.
[36] See earlier chapter one at and 19-25 and chapter two at 66-68.

state, which relies on the justificatory argument that it 'is a less invasive form of surveillance.'[37] The legal construct of communications data distinguished between what kinds of information implicate greater (content) or lesser (communications data) privacy interests. Based on the distinction between content and envelope information, it was originally envisioned and reasoned that the content of communications was deserving of stronger safeguards than communications data:

> '[E]very communications network features two types of information: the contents of the communications, and the addressing and routing information that the networks use to deliver the contents of communications. The former is "content information" and the latter is 'envelope information'. The essential distinction between content and envelope information remains constant across different technologies, from postal to e-mail. … The envelope information is the information derived from the outside of the envelope, including mailing and return address, the stamp and postmark, and the size and weight of the envelope when sealed.'[38]

However, while the above distinction works well in relation to the physical aspects of a postal letter, the effects thereof cannot be said to remain 'constant across different technologies, from postal to e-mail.'[39] In 2020, the value and sensitivity of communications have dramatically increased, such that the envelope information can be regarded as intrusive as the content of a communication.[40] A modern fast-paced environment of technological advancements not only means instantaneous communications, it has also made available volumes of transactional information about our privates lives.[41] For example, while the numbers dialled from a private telephone will reveal nothing of the contents of the

---

[37] *amaBhungane Centre for Investigative Journalism NPC and SP Sole v Minister of Justice and Correctional Services and Others* Case No: 25978/2017 (16 September 2019), subject to confirmation by the Constitutional Court. See applicants' heads of argument paras 45-51 available at *https://amabhungane.org/wp-content/uploads /2019/06/ 190212_amaB-heads-of-argument.pdf*, accessed 24 March 2020.

[38] OS Kerr 'Internet surveillance law after the USA Patriot Act: The Big Brother that isn't' (2003) 97 *Northwestern University LR* 607 at 611-16.

[39] Ibid.

[40] Applying the distinction between content and envelope information to an Internet Protocol address and to a Uniform Resource Locator, which is used to specify addresses on the World Wide Web, is another example demonstrating that the distinction is not always clear and certain. The non-content part of an Internet communication, referred to as a 'header', and every communication sent across the Internet includes both the originating and destination IP address. A list of IP addresses can reveal a wealth of information about our Internet activities: 'That A has telephoned B on a particular date from a particular location is actually quite intrusive … If a [member of parliament] logged on to a site selling Viagra, that tells you quite a lot. If a 16-year-old girl goes on to a website about abortion that tells you an awful lot about her too. I don't think there's a black-and-white distinction between communications data and content.' Attributed to the former Information Commissioner Richard Thomas quoted in Liberty *Liberty's response to the Home Office consultation: "Protecting the public in a changing communications environment"* at 19 available at *https://www.libertyhum anrights.org.uk/site / default/files/liberty-s-communications-data-consultation-response.pdf*, accessed 4 July 2019.

[41] See MW Clark 'Cell phones as tracking devices' (2007) 41 *Valparaiso University LR* 1414.

conversations, the list of numbers cannot be said to be without content, and could easily reveal the identities of persons and places called which, if collated, could reveal sensitive details of a person's life.[42] A lengthy telephone call may well suggest that 'two people on opposite ends of the line knew each other or at least had something substantial to discuss.'[43] In other situations, it may reveal activity in relation to a suspect/target of an investigation or operation that informs law enforcement and security and intelligence agencies of the location of the suspect/target, the time and duration of, including whom s/he spoke to.[44] For journalists with confidential sources, disclosure of their mobile phone contacts as communications data is just as revealing.

In terms of opportunities for law enforcement and security and intelligence agencies, this means the ability to access the 'what' of communications held by telecommunication service providers, that is, information about our locations, online activities and related information about e-mails and messages we send or receive – all of which under RICA 2002 is deemed to be less invasive and therefore worthy of lesser privacy protections.[45] This was confirmed by the state as recently as 2016 in which it reiterated its position: 'the interception of direct and indirect communications are regarded as extremely intrusive and a higher level of judicial authorisation is required before law enforcement is entitled to this information. Call related information is regarded as less intrusive and a lower standard of judicial authorisation is necessary before it can be made available.'[46]

I am of the view the 'envelope is the content'[47] and so it is argued that the distinction between the content of communications and its communications data in a year 2020 information age is no longer sustainable. The type of communication-related information which telecommunication service providers must retain 'include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called

[42] DJ Solove 'Reconstructing electronic surveillance law' (2004) 72 *The George Washington LR* 1701 at 1726.
[43] Kerr op cit note 38 at 643.
[44] Ibid.
[45] United Nations Human Rights Council 'Report of the Special Rapporteur' at 5 op cit note 6.
[46] South Africa's written responses to the UN Human Rights Committee following South Africa's review ref 50/2016 (10 March 2016) at 2 available at *https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/ZAF/INT_CCPR_AIS_ZAF_23518_E.pdf*, accessed 2 April 2020.
[47] Solove op cit note 42at 1727.

and an IP address for Internet services.'[48] In doing so, it makes it possible to identify the person(s) with whom a user has communicated, including by what means, the time, the place and the frequency of communications during a given period.[49] This type of information 'taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.'[50]

RICA clearly infringes the constitutional right to privacy which brings us to the second leg of the enquiry, namely, whether the limitation on the right to privacy in RICA 2002 is reasonable and justifiable as envisaged in s 36 of the Constitution. The process of determining whether a limitation of the right to privacy is reasonable and justifiable within s 36 involves the balancing of competing interests. It entails taking account of the considerations enumerated in s 36. This process has been described by the court as a proportionality analysis.[51] In *National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others*, the limitation exercise was defined in these terms:

> 'The balancing of different interests must still take place. On the one hand there is the right infringed; its nature; its importance in an open and democratic society based on human dignity, equality and freedom; and the nature and extent of the limitation. On the other hand there is the importance of the purpose of the limitation. In the balancing process and in the evaluation of proportionality one is enjoined to consider the relation between the limitation and its purpose as well as the existence of less restrictive means to achieve this purpose.'[52]

In *Johncom Media Investments Limited v M and Others*, the Constitutional Court provided further guidance on the proportionality analysis: '[t]o effect a proper balance, the right infringed must be identified, and its nature as well as its importance in a particular context must be considered. The purpose of the limitation must be pin-pointed, together with its extent, so as to determine the relation between the limitation and the purpose it is designed to achieve. We must also consider whether the purpose could be achieved by less restrictive means.'[53] In other words, for a limitation to be permissible, it is not enough that it serves one of the

[48] *Digital Rights Ireland Ltd (C-293/12) and Kärntner Landesregierung and Others* (C-594/12) CJEU (08 April 2014) para 26.
[49] Supra note 48 paras 26-27.
[50] Supra note 48 para 27.
[51] *Phillips and Another v Director of Public Prosecutions and Others* 2003 (3) SA 345 (CC) para 22.
[52] 1999 (1) SA 6 (CC) para 35 (footnote omitted).
[53] *Johncom's* case supra note 34 para 24.

enumerated legitimate aims, it must be necessary for reaching the legitimate aim.[54] Similarly, interpretation of the International Covenant on Civil and Political Rights clearly indicates that it is not sufficient that the restrictions serve the permissible purposes, it requires restrictive measures to conform to the principle of proportionality: the measure must be appropriate to achieve its protective function, the measure must be the least intrusive instrument amongst those which might achieve the desired result, and the measure must be proportionate to the interest to be protected.[55]

The key issue in this regard is the balance between the right of privacy and the right of the state to infringe on those privacy rights in the furtherance of its goals, notably the need to investigate and combat crime. In South Africa's written responses to the United Nations Human Rights Committee following South Africa's Review, the state explained that RICA 2002 is 'a response to crimes committed through modern communication devices.'[56] The 'legitimate purpose' of RICA was explained by the state as follows:

> 'The sole reason why the RICA was put on the Statute Book is to provide for a mechanism to investigate and combat serious crimes which are planned, facilitated or executed through the use of electronic communications. Most constitutional democracies followed this route in order to investigate crime.'[57]

While it is accepted that RICA 2002 is necessary for reaching a legitimate aim, that is, to 'investigate and combat serious crimes'[58] in the circumstances it is argued that the limitation on the right to privacy cannot be justified. In the analysis of factors (d) and (e) of s 36 of the Constitution, respectively, the relation between the limitation and its purpose and less

---

[54] South Africa's written responses to the UN Human Rights Committee op cit note 46 at 1-2.
[55] Human Rights Committee General Comment No. 27 (1999) CCPR/C/21/Rev.1/Add.9, reproduced in Human Rights Instruments (2008) *Compilation of general comments and general recommendations adopted by Human Rights Treaty Bodies* HRI/GEN/1/Rev.9 (Vol. I) paras. 11-16. Although explained on Article 12 (freedom of movement), the same principles apply to the interpretation of Article 17.
[56] South Africa's written responses to the UN Human Rights Committee op cit note 46.
[57] Ibid at 6. The long title of RICA 2002 further conveys the intended purpose of the legislation, inter alia: 'To regulate the interception of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information; to regulate the making of applications for, and the issuing of, directions authorising the interception of communications and the provision of communication- related information under certain circumstances; to regulate the execution of directions and entry warrants by law enforcement officers and the assistance to be given by postal service providers, telecommunication service providers and decryption key holders in the execution of such directions and entry warrants.'
[58] Ibid at 6. The South African state further responded on legitimacy: [t]hese laws act as a shield and sword against the protection of human rights and specify how the State must exercise its powers in the investigation of criminal offences facilitated through the use of communication technologies. That is precisely what RICA aims to do. From a Constitutional perspective the interception of communications can be justified in terms of the limitation clause to our constitution (section 36).'

restrictive means to achieve the purpose, the state falls short in its adamant position on mandatory data retention. The RICA 2002 provisions that require telecommunication service providers to perform untargeted and indiscriminate mandatory retention of communications data cannot be justified.

The state was specifically asked to respond to the following by the United Nations Human Rights Committee: 'Article 30(1)(b) of RICA requires retention of communications data. Could you explain how the mandatory retention of communications data is justified under Article 17 of the Covenant?'[59] Article 17 of the International Covenant on Civil and Political Rights reads: '1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.'[60] The totality of the state's unsatisfactory response was recorded as follows: '[t]he information which is being stored is typically call related information. In the past it has solved various serious criminal cases in the Republic. The UK, Australia, New Zealand and certain countries in Europe also keep this information for the purposes of criminal investigations. Information must be stored for a 5 year period.'[61] The state's response misses the key point, specifically concerns about the regulation of mandatory retention of communications data and infringements of rights, not the value of communications data as the state referred to in response. The state was unable to demonstrate, effectively, how the RICA 2002 provisions on untargeted and indiscriminate mandatory retention of communications data as a restrictive measure on the right to privacy conforms to the principle of proportionality, how the measure is appropriate to achieve its protective function, how the measure is the least intrusive instrument amongst those which might achieve the desired result, and how the measure is proportionate to the interest to be protected.[62] As an umbrella response to justify all its electronic surveillance provisions in RICA 2002 as proportional, the state reverted as follows: [i]n terms of the RICA an interception can only be authorised if 'other investigative procedures have been applied and have failed to produce the required evidence or reasonably appear to be unlikely to succeed if applied or are likely to be too dangerous to apply in order to obtain the required evidence and that the offence therefore cannot adequately be investigated, or the information therefore cannot adequately be obtained, in another appropriate manner (s

[59] South Africa's written responses to the UN Human Rights Committee op cit note 46 at 10.
[60] Available at *http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx*, accessed 02 March 2018
[61] South Africa's written responses to the UN Human Rights Committee op cit note 46 at 11.
[62] Ibid at 1-2.

16(5)*(c)*).'[63] However, does such provision apply to mandatory retention of communications data by telecommunication service providers? No, it does not. The issuing of a retention directive by the Minister to telecommunication service providers is not linked to any specified purpose, such as the prevention and detection of 'serious offences' or in the interests of 'national security or compelling national economic interests.' Further, the decision to issue a retention directive is not required to be approved by a judicial authority.

In applying s 36(1)(*d*) of the Constitution, which requires consideration of the relation between the limitation and its purpose, it is clear that the provisions to perform untargeted and indiscriminate mandatory retention of communications data is not rationally linked to the legitimate purposes the state seeks to achieve. In terms of Constitutional Court guidance, this analysis evaluates the logical relationship between the purpose sought to be achieved by the provision and the means used.[64] The aim of the evaluation is not to determine whether some measure will achieve the purpose better, only whether the selected measures could rationally achieve the same end.[65]

Section 36(1)*(e)* asks whether there is a less restrictive means to achieve the purpose. The Constitutional Court has been very clear that where a right is being limited, if there are less-restrictive means available by which the same end could be achieved, these less-restrictive means must be used.[66] If the provisions of legislation are 'overbroad in its reach' the extent of the infringement on rights is considered 'substantially disproportionate to its public purpose.'[67] In *S v Manamela and Another (Director-General of Justice Intervening)*, the Constitutional Court has stated that s 36 limitations analysis 'however, does not permit a sledgehammer to be

[63] Ibid at 1-2.
[64] *Minister of Safety and Security v South African Hunters and Game Conservation Association* 2018 (2) SACR 164 (CC) para 14. See also *amaBhungane* case applicants' heads of argument supra note 37 paras 67-68.
[65] Ibid.
[66] See *amaBhungane* case applicants' heads of argument supra note 37 paras 67-68.
[67] *Mistry v Interim National Medical and Dental Council of South Africa and Others* 1998 (4) SA 1127 (CC) para 30: 'To sum up: irrespective of legitimate expectations of privacy which may be intruded upon in the process, and without any predetermined safeguards to minimise the extent of such intrusions where the nature of the investigations makes some invasion of privacy necessary, section 28(1) gives the inspectors carte blanche to enter any place, including private dwellings, where they reasonably suspect medicines to be, and then to inspect documents which may be of the most intimate kind. The extent of the invasion of the important right to personal privacy authorised by section 28(1) is substantially disproportionate to its public purpose; the section is clearly overbroad in its reach and accordingly fails to pass the proportionality test laid down in *S v Makwanyane and Another*' (footnote omitted).

used to crack a nut.'[68] The enactment of a provision which infringes on constitutional rights must be 'appropriately tailored and more narrowly focussed.'[69]

Although the s 30(1)*(b)* provision in RICA 2002 will likely be deemed legitimate in its aim of investigating and combatting serious crime, it does not pass the proportionality test that the Constitutional Court applies to evaluate the appropriateness of the measure undertaken to achieve its legitimate aim. It can be rightly regarded as 'overbroad in its reach' and 'substantially disproportionate to its public purpose.' To a great extent, the provision in RICA 2002 interferes with the right to privacy for an unspecified length of time, falling between three and five years. There are also no safeguards and protections to be followed for storing, accessing, examining, using and destroying the communications data.

European human rights jurisprudence often cite the joined cases of *Digital Rights Ireland Ltd* (C-293/12) and *Kärntner Landesregierung and Others* (C-594/12). [70] The European Court of Justice found that a Council of the European Union adopted Directive 2006/24/EC, which regulated Internet Service Providers' storage of telecommunications data that could be used to fight serious crime in the European Union, to be invalid to the extent that such directive 'entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the European Union, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.'[71] The Court of Justice of the European Union found that the data retention directive was problematic in that:

> 'it did not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.'[72]

---

[68] 2000 (3) SA 1 (CC) para 34.
[69] See *Islamic Unity Convention v Independent Broadcasting Authority and Others* 2002 (4) SA 294 (CC) para 49 and *South African National Defence Union v Minister of Defence and Another* 1999 (4) SA 469 (CC) para 18: 'At the second stage of the constitutional enquiry, the relevant questions are what is the purpose of the impugned provision, what is its effect on constitutional rights and is the provision well-tailored to that purpose.'
[70] *Digital Rights Ireland* case supra note 48.
[71] Supra note 48 para 65.
[72] Supra note 48 para 59. See Privacy International *Submission to the joint committee on the draft Investigatory Powers Bill* (21 December 2015) available at *https://privacyinternational.org/sites/default/files/2017-12/Submission_IPB_Joint_Committee.pdf*, accessed 2 July 2019 para 225: 'Even before the CJEU issued its judgment in Digital Rights Ireland, the constitutional or administrative courts of Bulgaria, Cyprus, the Czech

The retention of communications data is untargeted and indiscriminate in South African law, and without any protection against arbitrary interference. Unlimited in scale, and a generous duration period for retention, the majority of information retained by telecommunication service providers for an unspecified length of time, falling between three and five years in terms of RICA 2002, will be irrelevant to any criminal or national security investigation. The untargeted and indiscriminate mandatory retention of communications data, without suspicion, unjustifiably violates the right to privacy. In *S and Marper v United Kingdom*, a case concerned the 'blanket and indiscriminate' retention of DNA samples from persons arrested but not charged or convicted, the Grand Chamber of the European Court of Human Rights held that 'the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data.'[73] In comparison with the features of the European Union adopted Directive 2006/24/EC on data retention, the RICA 2002 provisions require telecommunication service providers to perform untargeted and indiscriminate mandatory retention of communications, and similarly does not:

> 'provide for sufficient safeguards to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data.
>
> …
>
> lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required…, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality.
>
> …
>
> does not ensure the irreversible destruction of the data at the end of the data retention period.'[74]

Republic, Germany and Romania declared part or all of the relevant national legislation implementing the Data Retention Directive to be unlawful. Following the Digital Rights Ireland judgment, the courts of Austria, Slovenia, Belgium, Bulgaria, the Netherlands, Poland, Romania, and Slovakia have struck down national laws that had implemented or replicated the Data Retention Directive (or, in the case of Romania and Bulgaria, subsequent amendments to the original implementing laws).'

[73] EctHR 30562/04 and 30566/04 (4 December 2008) para 121.

[74] Supra note 73 para 121. See also *Scarlet Extended SA v SABAM* (CC-70/10) CJEU (24 November 2011), the CJEU similarly held that a filtering system proposed by rights-holders in order to combat copyright infringement was unlawful on the basis that it would require internet service providers to engage in real-time 'preventative monitoring' of customers' communications. The court held that such a measure would be incompatible with European Union Directives, namely with Article 15(1) of Directive 2000/31, which prohibits imposition of an obligation on an Internet service provider to carry out general monitoring of the information that it transmits on its network, and would be against the fundamental rights of Internet users to the protection of

Notably, in European human rights jurisprudence there is recognition of a margin of appreciation that states' enjoy for the way in which a measure is designed to achieve its stated aim in light of present day threats of serious criminal activity. In *Centrum för Rättvisa v Sweden*,[75] for instance, the case concerned a complaint brought by a public interest law firm alleging that domestic legislation permitting the bulk interception of electronic signals in Sweden for foreign intelligence purposes breached its Article 8 privacy rights. Although the Court found some shortcomings in the Swedish legislation, in particular its intelligence sharing regime and the lack of public reasons for decisions reached by one of its oversight bodies, it held that the Swedish system of bulk interception provided adequate and sufficient safeguards against arbitrariness and the risk of abuse. In doing so, the Court gave a wide margin of appreciation to states to adopt bulk interception regimes in light of 'the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the internet, and the unpredictability of the routes via which electronic communications are transmitted.'[76]

In its analysis, the European Court of Human Rights has considered the Convention compatibility of regimes which expressly permit the bulk interception of communications on two occasions: first in *Weber and Saravia v Germany*[77] and then also in *Liberty and Others v The United Kingdom*:[78]

---

their personal data and freedom of expression guaranteed under the European Union Charter of Fundamental Rights.

[75] EctHR 35252/08 (19 June 2018).

[76] Supra para 112.

[77] EctHR 54934/00 (29 June 2006). At para 109: 'In *Weber and Saravia* the applicants complained about the process of strategic monitoring under the amended G10 Act, which authorised the monitoring of international wireless telecommunications. Signals emitted from foreign countries were monitored by interception sites situated on German soil with the aid of certain catchwords which were listed in the monitoring order. Only communications containing these catchwords were recorded and used. Having particular regard to the six "minimum safeguards" the Court considered that there existed adequate and effective guarantees against abuses of the State's strategic monitoring powers. It therefore declared the applicants' Article 8 complaints to be manifestly ill-founded.'

[78] EctHR 58243/00 (1 July 2008). At para 109: 'In *Liberty and Others* the Court was considering the regime under the Interception of Communications Act 1985 which allowed the executive to intercept communications passing between the United Kingdom and an external receiver. … The Court held that the domestic law at the relevant time did not indicate with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material.'

'*The Court has expressly recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security.* … the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation. Nevertheless, it is evident from the Court's case-law over several decades that all interception regimes (both bulk and targeted) have the potential to be abused, especially where the true breadth of the authorities' discretion to intercept cannot be discerned from the relevant legislation …*Therefore, while States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary to protect national security, the discretion afforded to them in operating an interception regime must necessarily be narrower.*'[79]

In this regard, the Court applied the identified six minimum safeguards on electronic surveillance that contracting states must incorporate in order to be sufficiently foreseeable to minimise the risk of abuses of power. Following a careful assessment of the minimum safeguards developed by the Grand Chamber in its 2015 judgment in *Roman Zakharov v Russia*,[80] the court found that the Swedish system of signals intelligence provided adequate and sufficient guarantees against arbitrariness and the risk of abuse. The court noted that the regulatory framework had been reviewed several times with a view to notably enhancing protections of privacy, and had in effect developed in such a way that it minimised the risk of interference with privacy and compensated for the lack of openness of the system. Specifically the court found that the scope of the electronic surveillance powers and its treatment of data clearly defined in law; the scope and duration of signals intelligence were clearly regulated, the authorisation of the measures was detailed and entrusted to a judicial body and there were several independent bodies; the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data were clearly defined, as well as the arrangements for supervising the implementation of the measures, and also considered any notification mechanisms and the remedies provided for by national law.[81]

A key lesson for South African law is that 'discretion afforded' to the state in operating an electronic surveillance regime 'must necessarily be narrower.' There can no longer be untargeted and indiscriminate mandatory retention of communications data applicable to everyone without the requirement of a suspicion that a crime has been committed. Specifically

[79] *Centrum för Rättvisa* supra note 75 paras 112-113 (emphasis added).
[80] EctHR 47143/06 (4 December 2015).
[81] *Centrum för Rättvisa* supra note 75 paras 115-178.

on retention of communications data, there should be the introduction of targeted retention orders instead. I believe that the Investigatory Powers Act 2016[82] adopted in the United Kingdom offers a remedy for lawmakers in South African to consider. Powers to require retention of certain data is exercised by the Secretary of State, for specified purposes including inter alia in the interests of national security or public safety or the economic well-being of the United Kingdom.[83] The decision to give the notice to require a telecommunications operator to retain relevant communications data must have been approved by a Judicial Commissioner.[84]A retention notice must not require any communications data to be retained for more than twelve months.[85] Before giving a retention notice, the Secretary of State must, inter alia, take into account: (a) the likely benefits of the notice; (b) the appropriateness of limiting the data to be retained; (c) the likely number of users (if known) of any telecommunications service to which the notice relates; and (d) the technical feasibility of complying with the notice.[86] Before giving such a retention notice, the Secretary of State must take reasonable steps to consult any operator to whom it relates.[87] In terms of procedures to be followed for storing, accessing, examining, using and destroying the communications data, a telecommunications operator who retains relevant communications data must: '(a) secure that the data is of the same integrity, and subject to at least the same security and protection, as the data on any system from which it is derived, (b) secure, by appropriate technical and organisational measures, that the data can be accessed only by specially authorised personnel, and (c) protect, by appropriate technical and organisational measures, the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure.'[88] A telecommunications operator who retains relevant communications data must destroy the data if the retention of the data ceases to be authorised and is not otherwise authorised by law.[89] The destruction of the data may take place at such monthly or shorter intervals as appear to the operator to be practicable.[90]

[82] Hereafter 'IPA 2016'.
[83] Section 87(1)*(a)*.
[84] Section 87(1)*(b)*. In terms of approval of retention notices by Judicial Commissioners, s 89 provides that in deciding whether to approve a decision to give a retention notice, a Judicial Commissioner must review the Secretary of State's conclusions as to whether the requirement to be imposed by the notice to retain relevant communications data is necessary and proportionate for one or more of the stated specific purposes.
[85] Section 87(3).
[86] Section 88(1).
[87] Section 88(2).
[88] Section 92(1).
[89] Section 92(2).
[90] Section 92(3).

(b) Acquiring communications data

As has been rightly pointed out, communications data 'is ultimately retained so that it can be later acquired'[91] by law enforcement and security and intelligence agencies. To acquire access to communications data, law enforcement and security and intelligence agencies must apply for a 'direction' to a judicial officer. RICA 2002 distinguishes between two kinds of communications data: *real-time* (immediately available up to 90 days after transmission) and *archived* (stored after the 90 day transmission period) with differing authorisation procedures for access. For law enforcement and security and intelligence agencies to gain access to real-time communications data, as with interception directions, there must be an application to a designated judge for the issuing of a real-time communication-related information direction.[92] There are different judicial officers for applications, almost a separate process, to access archived communications data. 'If only' access to archived communications data 'is required', there must be an application to a 'judge of a High Court'[93], or 'a regional court magistrate'[94], or 'a magistrate'.[95] It is not clear why different judicial officers are required for applications apply for real-time and archived communications data in RICA 2002. The position of the state, after all, is to regard access to *all* communications data as less intrusive than accessing the content of a communication.[96] The threshold for the referred judicial officers to issue a real-time and archived communications data direction is 'reasonable grounds to believe.'[97] The stated specified purposes for access to real-time and archived communications data is the same, namely, inter alia, that a 'serious offence has been or is being or will probably be committed,'[98] or where communication-related information sought by law enforcement and security and intelligence agencies concerns 'an actual threat'[99] to 'national security' or 'compelling economic interests of the Republic'.[100] There are no specified procedures to be followed for storing, accessing, examining, using and destroying the communications data, whether real-

[91] Gillespie op cit note 7 at 343.
[92] Sections 1, 7(4), (5), (6); 8(4)*(b)*, *(c)*; 8(5); 8(6); 16(1),(4), (5), (8)*(a)(iii)*, (8)*(b)(iii)*, (10), (10)*(b)*; 16(5); 17(1), (3), (4)*(a)*, *(b)*; 19(7), (8); 20(1), (3), (4); 21(1)*(a)*,*(b)*;22(3), (4)*(a)*, *(b)*, (5)*(c)*, 6*(b)*; 23(3), (4)*(a)*, (b), (7), (8)*(a)*, *(b)*, (10), (11); 24, *(a)(ii)*; 25(1), (2), (3).
[93] Sections 19(1), (3)(4), (7); 48.
[94] Sections 19(1), (3), (4), (7); 48.
[95] Sections 19(1), (3), (4), (7); 48.
[96] South Africa's written responses to the UN Human Rights Committee op cit note 46 at 2: '[communications data] is regarded as less intrusive and a lower standard of judicial authorisation is necessary before it can be made available.'
[97] Sections 17(4) and 19(4).
[98] Sections 17(4)*(a)* and 19(4)*(a)*.
[99] Sections 17(4)*(b)* and 19(4)*(b)*.
[100] Sections 17(4)*(b)* and 19(4)*(b)*.

time or archived. In respect of both types of communications data, it is stated that the direction issued 'may specify conditions or restrictions relating to the provision' of real-time or archived communications data. [101]

A direction for real-time communications data 'may be issued for a period not exceeding three months at a time, and the period for which it has been issued must be specified therein.'[102] As regards a direction for archived communications data it 'must state the period within which the archived communication-related information must be routed or provided.'[103] In terms of s 19(7) '[i]f a judge of a High Court, regional court magistrate or magistrate issues an archived communication-related direction, he or she must, as soon as practicable thereafter, submit a copy of the application and communication-related direction to a designated judge.' However, there is no indication of a requirement that the designated judge must review the conclusions or information on which approval of an archived communication-related direction is based or whether it is necessary and proportionate for one or more of the stated purposes in s 19(4). Further applications for access to real-time or archived communications data do not require law enforcement and security and intelligence agencies to indicate whether 'other investigative procedures have been applied and have failed to produce the required evidence or reasonably appear to be unlikely to succeed if applied or are likely to be too dangerous to apply in order to obtain the required evidence and that the offence therefore cannot adequately be investigated, or the information therefore cannot adequately be obtained, in another appropriate manner.'[104] In other words, there is no proportionality analysis for real-time or archived communications data directions.

To fully understand the challenges with this split regime for real-time or archived communications data directions in RICA 2002, it becomes important to consider the provisions of s 205 of the Criminal Procedure Act 51 of 1977. The implications thereof and obligations on third party telecommunications service providers are now considered.

[101] Sections 17(5)*(c)* and 19(5)*(d)*.
[102] Section 17(5)*(d)*.
[103] Section 19(5)*(c)*.
[104] As applicable to interception directions in terms of s 16(5)*(c)*.

(c) The provisions of s 205 of the Criminal Procedure Act 51 of 1977

Section 205 of the Criminal Procedure Act 51 of 1977[105] further provides another evidence gathering mechanism in relation to powers of law enforcement and security and intelligence agencies to access information related to communications, such as cellular phone records, including itemised billing, identification of the subscriber to a specified cellular number, and where the cellular handset was geographically located during a call.[106] Similar to applications for archived communications data in RICA 2002, s 205 provides that an application must be made to a 'judge of a High Court, a regional court magistrate or a magistrate.'

Originally, s 205 did not have anything to do with communications data or with the obligation of telecommunication service providers to provide information to the state. The main purpose of s 205 is regulation of how a witness is called to provide evidence in court. Where an alleged offence has taken place, s 205 allows a 'judge of a High Court, a regional court magistrate or a magistrate' upon the request of a Director of Public Prosecutions or a duly authorised public prosecutor, to summons 'any person who is likely to give material or relevant information as to any alleged offence, whether or not it is known by whom the offence was committed.'[107] A person 'who refuses or fails to give the information' contemplated above 'shall not be sentenced to imprisonment' unless 'the judge, regional court magistrate or magistrate concerned … is also of the opinion that the furnishing of such information is necessary for the administration of justice or the maintenance of law and order.'[108] Section 205 is now 'subject to the provisions' of s 15 of RICA 2002.[109] In other words, s 15 of RICA 2002 allows law enforcement and security and intelligence agencies to use s 205 to obtain communications data from telecommunication service providers. Where a complainant has opened criminal charges, upon the request of a Director of Public Prosecutions or a duly authorised public prosecutor, information relevant to the alleged offence, regardless of its severity, can be obtained from a telecommunication service provider by using s 205. In the same way, communications data is viewed as evidence, and the telecommunication service

[105] Hereafter 'CPA 51 of 1977'.
[106] See *S v Phillip Miller and 8 Others* 2016 (1) SACR 251 (WCC) (2 September 2015), *Haysom v Additional Magistrate, Cape Town and Another* 1979(3) SA 155 (C), *S v Matisonn* 1981(3) SA 302 (A), *Nel v Le Roux NO and Others* 1996(3) SA 562 (CC), *S v de Vries and Others* 2009(1) SACR 613 (C).
[107] Section 205(1).
[108] Section 205(4).
[109] Section 205(1). Section 15 of RICA 2002 reads as follows: '(1) Subject to subsection (2), the availability of the procedures in respect of the provision of real-time or archived communication-related information provided for in section 17 and 19 does not preclude obtaining such information in respect of any person in accordance with a procedure prescribed in any other Act; (2) Any real-time or archived communication-related information which is obtained in terms of such other Act may not be obtained on an ongoing basis.'

providers is ordered to provide those records, and to testify about those records in court if necessary. The witness in this instance is an employee representative of the telecommunication service provider. The telecommunication service provider's representative must appear at court on the date specified in the s 205 subpoena or provide the information 'prior to the date on which he or she is required to appear before a judge, regional court magistrate or magistrate' in which case the representative will be excused from appearing in court.[110] Law enforcement and security and intelligence agencies do not have power to intercept real-time communications data in terms s 205. Further communications data may not be obtained from a telecommunication service provider in terms of s 205 on the basis that an offence is likely to be committed in future. In both these instances, the provisions of RICA 2002 must be used to obtain the relevant communications data.

There are concerns that s 205 has created a parallel process for law enforcement and security and intelligence agencies to obtain communications data from third party telecommunication service providers, with less oversight and protections than RICA 2002.[111] These concerns do not appear unfounded. A comparison of statistics between s 205 applications and RICA 2002 applications for communications data indicate that s 205 applications are used more by law enforcement and security and intelligence agencies than RICA 2002 directions. As observed by Duncan:

> 'In essence, the largest part of communications surveillance in South Africa is legislated by the Criminal Procedures Act via the ordinary courts, despite all the special provisions introduced by Rica. For an indication of the relatively small portion of interception-related court orders that are actually issued by the Rica judge, it's useful to look at the statistics from the country's largest service provider, Vodacom. For the 2016/2017 financial year, the company was served with 1,075 interception directions (court orders) issued in terms of Rica by the Rica judge. For the same period, they received 19,850 Section 205 court orders from ordinary magistrates and judges. So, the Rica judge oversaw only 5.4% of all interception cases related to Vodacom customers.'[112]

In statistics obtained by a privacy advocacy group, the Right2Know Campaign, information from South Africa's leading telecommunication service providers reveal that they

---

[110] Section 205(4).
[111] Right2Know 'SPOOKED: Surveillance of journalists in SA' (June 2018) at 4 ,36 available at *https://www.sanef.org.za/wp -content/uploads/2018/07/R2K-Surveillance-of-Journalists-Report-2018-web.pdf.*, accessed 17 June 2019.
[112] J Duncan 'The loophole in South Africa's state spying laws' (March 2020) available at *https://www.dailymaverick.co.za/article/2020-03-09-the-loophole-in-south-africas-state-spying-laws/amp/?__twitter_impression=true*, accessed 31 March 2020.

received 'twenty-five to fifty thousand s 205 warrants' from law enforcement and security and intelligence agencies, in contrast to 'five or six hundred RICA warrants.'[113] Spokesperson for the Right2Know Campaign, Murray Hunter explains that situation is problematic for several reasons and that s 205 is 'essentially a loophole' that allows law enforcement and security and intelligence agencies to bypass the privacy protections in RICA 2002:[114]

> 'these numbers are "shocking", and says the fault lies in poor legislation. "These policies have let government spying go out of control. We never thought we'd find out that this loophole was being used to the tune of 70,000 or more phone numbers a year. It's a rate of surveillance that's easily 50 times what we've previously seen reported through RICA statistics. All this is further proof that the people of South Africa need to take back control of their privacy."'[115]

The contrast in the numbers between s 205 subpoenas and RICA 2002 directions for access to communications data retained by telecommunication service providers is attributed to the less stringent provisions in s 205 that allows law enforcement and security and intelligence agencies to avoid the designated RICA judge and make applications before a 'judge of a High Court, a regional court magistrate or a magistrate.'[116] This likely reflects the position of the state that communications data retained by telecommunication service providers is considered to be less intrusive, and therefore should be more easily accessible by law enforcement and security and intelligence agencies.[117] Further, while RICA 2002 stipulates that communications data, real-time or archived, may only be obtained for purposes inter alia that a 'serious offence has been or is being or will probably be committed'[118] or where the information sought concerns 'an actual threat'[119] to 'national security' or 'compelling economic interests of the Republic';[120] s 205 is far more wide-ranging in scope and may be

---

[113] Right2Know 'SPOOKED' op cit note 111 at 4.
[114] Duncan op cit note 112.
[115] Spokesperson for privacy advocacy group Right2Know (R2K), Murray Hunter quoted in H Swart 'Cell phone privacy: Law enforcement pulls 70,000 subscribers' call records each year – and that's a minimum estimate' (23 August 2017) available at *https://www.dailymaverick.co.za/article/2017-08-23-cell-phone-privacy-law-enforce ment-pulls-70000-subscribers-call-records-each-year-and-thats-a-minimum-estimate/*, accessed 5 July 2019. See also H Swart 'Your cellphone records and the law: The legal loophole that lets state spying run rampant' 20 May 2018 available at *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 5 July 2019.
[116] Section 205(1).
[117] As spokesperson for privacy advocacy group Right2Know (R2K), Murray Hunter stated: 'When lawmakers passed Rica, they assumed that the information about your communication was less sensitive than the contents of the communication. That assumption is out-of-date and just wrong, and has put whistle-blowers, journalists and others at risk, and left all of us vulnerable to spying' as quoted in H Swart 'Your cellphone records and the law: The legal loophole that lets state spying run rampant' op cit note 115.
[118] Sections 17(4)*(a)* and 19(4)*(a)*.
[119] Sections 17(4)*(b)* and 19(4)*(b)*.
[120] Ibid.

invoked where a person is able 'to give material or relevant information as to any alleged offence.'[121] Therefore, access to retained communications data in s 205(1) is not limited to the purpose of combatting 'serious' crimes, and is wide-ranging and includes 'any alleged offence.' Further, access to communications data under s 205 and RICA 2002 is not subject to review by any independent administrative body. Rightly so, it is argued:

> '[T]he law needs to set to a new, universal standard … The Section 205 procedure needs to be thrown into the bin. Any interception of communications has to go through a specially appointed judge, who is expertly attuned to issues of privacy and digital rights, who is transparent and publicly accountable. No more back doors, no more loopholes.'[122]

It must be acknowledged that the acquisition of communications data by law enforcement and security and intelligence agencies in 2020 cannot continue on the state's insistence that we apply traditional investigatory powers to new technological infrastructures. The acquisition of communications data today is far from tradition we knew two decades ago with the 'plain-old-telephone system.'[123] It must be recognised communications data as highly sensitive and deserving of strong privacy protections in law. As referred earlier on retaining communications data, I believe that the Investigatory Powers Act 2016[124] adopted in the United Kingdom offers a standard to consider as a starting point for reform in South African law. In terms of the 2016 Act there are three steps in authorising the acquisition of communications data. Firstly, in terms of s 61(1)*(a)* it must be for a specified purpose when read with s 61(7). In terms of stated purposes, inter alia, it is necessary to obtain the data for the purpose of

[121] In 1996, the Constitutional Court in *Nel v Le Roux N O & Others* 1996 (3) SA 562 (CC) rules that s 205 did not infringe a number of fundamental constitutional rights, including equality, privacy, freedom of speech and expression, an accused's right to be presumed innocent and to remain silent, and an accused's right against self-incrimination. The Constitutional Court held that s 205 was 'narrowly tailored as possible to meet the legitimate state interest of investigating and prosecuting crime' without infringing the constitutional rights of the examinee (para 20). See also *Panday v Minister of Police and Others* (12044/10) [2012] ZAKZDHC 20; 2012 (2) SACR 421 (KZD) (18 April 2012) para 7 in reference to *Nel's* case, Murugasen J observed: '[d]espite a scrutiny of Section 205, when the Constitutional Court held that the provisions thereof were not unconstitutional, the Court did not find it necessary to interfere with the procedure envisaged by the section as being inconsistent with the Constitution or potentially unconstitutional, or prescribe any procedural formality to preserve the constitutionality, although it is apparent that applications in terms of Section 205 although demanding 'the exercise of invasive and compulsive powers' are subject only to the exercise of judicial discretion by the presiding officers after due consideration of the facts disclosed in the application.' Thus, Murugasen J was satisfied that such scrutiny was adequate prevent abuse and arbitrary interference with individual rights. See also *R v Parker* 1966 (2) SA 56 (RA); *Bernstein and Others v Bester NO and Others* (1996 (2) SA 751 (27 March 1996).

[122] Spokesperson for privacy advocacy group Right2Know (R2K), Murray Hunter quoted in H Swart 'Your cellphone records and the law: The legal loophole that lets state spying run rampant' op cit note 115.

[123] Hosein and A Pascual op cit note 2 at 8.

[124] Hereafter 'IPA 2016'.

preventing or detecting serious crime,[125] in the interests of national security[126] and in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security.[127] Secondly, it is necessary to obtain the data: (i) for the purposes of a specific investigation or a specific operation, or (ii) for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data.[128] Thirdly, authorisation for access to communications data must be proportionate to what is sought to be achieved.[129] There are additional restrictions in relation to internet connection records,[130] and many other restrictions which ensure there is independent oversight on the need for such investigatory powers.[131] The use of emergency powers for acquiring communications data is for situations where there is 'an imminent threat to life or another emergency'[132] or an opportunity to obtain information in circumstances where the opportunity is rare, the time to act is short, and the need to obtain the information is significant and in the interests of national security.[133] An authorisation for the acquisition of communications data will be for a period of one month.[134] Authorisations can be renewed[135] and should be cancelled where it is no longer necessary.[136] Duties of telecommunication service providers are clearly stated, specifically they are under a statutory duty to comply with an authorised request.[137] In relation to the obtaining of communications data for the purpose of identifying or confirming a source of journalistic information, the authorisation does not take effect until such time as it is approved by a Judicial Commissioner.[138] The applicant of an authorisation order for acquisition of communications data 'must consult a person who is acting as a single point of contact.'[139] As an expert, the single point of contact is 'specially trained in communications-data handling and will build up a rapport with the various communication providers to ensure that information can flow

[125] Section 61(7A).
[126] Section 61(7)(*a*).
[127] Section 61(7)(*c*).
[128] Section 61(1)(*b*).
[129] Section 61(1)(*c*).
[130] Section 62.
[131] Section 63.
[132] Section 63(3)*(a)*.
[133] Section 63(3)*(c)*.
[134] Section 65(1).
[135] Section 65(2).
[136] Section 65(4).
[137] Section 66(1).
[138] Section 77.
[139] Section 76.

securely and appropriately' and 'not least because they may be aware of a less-intrusive way of getting the information.'[140]

Duties in connection with the operation of filtering arrangements for the communications data falls on the Secretary of State whom must secure the data such that: '(a) only the Secretary of State and designated individuals are permitted to read, obtain or otherwise process data for the purposes of support, maintenance, oversight, operation or administration of the filtering arrangements, and (b) no other persons are permitted to access or use the filtering arrangements except in pursuance of an authorisation or for the purpose mentioned in section 67(1)(a).'[141] The Secretary of State must further: '(a) put in place and maintain an adequate security system to govern access to, and use of, the filtering arrangements and to protect against any abuse of the power of access, an (b) impose measures to protect against unauthorised or unlawful data retention, processing, access or disclosure.'[142] The provisions of the Act in this regard continue. The Secretary of State must: '(a) put in place and maintain procedures (including the regular testing of relevant software and hardware) to ensure that the filtering arrangements are functioning properly, and (b) report, as soon as possible after the end of each calendar year, to the Investigatory Powers Commissioner about the functioning of the filtering arrangements during that year.'[143]

My proposals for change in the concluding chapter of the thesis, in part, are done in the context of acquisition and retention of communications data, inter alia, with a focus on the overall importance of clear and accessible laws that avoids different sets of rules in different legislation covering essentially the same investigative activities. While the degree of intrusion into privacy rights is not affected by whether it involves the conduct of law enforcement or the intelligence agencies – whether one or the other, maximum oversight and transparency is just as necessary.[144] They key issue is oversight and its effect on the electronic surveillance culture of the state: to subject law enforcement or the intelligence agencies to different sets of rules for essentially the same investigative activities could give rise to a 'dilution in the regulatory' frameworks.[145] As has happened in South Africa where different sets of rules, in different laws, have resulted in different standards of oversight and different standards of conduct in the exercise of intrusive powers. This has happened in the preferred use of s 205 of the CPA 51 of

[140] Gillespie op cit note 7 at 345.
[141] Section 69(3).
[142] Section 69(5).
[143] Section 69(6).
[144] Anderson op cit note 30 at 255.
[145] Ibid.

1977 to obtain communications data from third party telecommunication service providers – the exercise of such powers prompted the tendency to follow whichever rule 'was perceived to be less strictly regulated.'[146] None of this should apply in a proposed new legal framework for South African law.

(d) Procedures in RICA 2002 for storing, accessing, examining, using and destroying the communications data

A key concern linked to the issue of the state requiring telecommunication service providers to perform untargeted and indiscriminate mandatory retention of communications data is the lack of specified procedures in RICA 2002 to be followed for storing, accessing, examining, using and destroying the communications data. 'At the very least' RICA 2002 'should specify the minimum technical requirements for securing retained data, and describe how any breaches will be addressed and revealed to oversight bodies and the public.'[147] It does not do so, and in the manner of its operation at an 'unacceptable level of risk'[148] can be approximated to being a 'honeypot for casual hackers, blackmailers, criminals large and small.'[149] The lack of specified procedures in this regard attracts the risk that that the information 'may be hacked into or may fall accidentally into the wrong hands, and that, if this were to happen, potentially damaging inferences about people's interests or activities could be drawn.'[150]

In a reported incident of abuse within telecommunication service providers, an employee at a telecommunication service provider was allegedly paid ZAR3,750 by a private investigator for the phone records of a South African journalist. The journalist had become aware of this after being informed by the telecommunication service provider that an employee had illegally accessed his account.[151] The illegally obtained information of the journalist

[146] Ibid.
[147] Privacy International op cit note 72 para 188.
[148] Ibid at 47.
[149] Attributed to a Liberal Democrat peer, Lord Strasburger in A Travis 'MPs call communications data bill "honeypot for hackers and criminals"' 31 October 2012 *The Guardian* available at *https://www.theguardian.com/technology/2012/oct/31/communications-data-bill-honeypot-hackers-criminals*, accessed 4 July 2019.
[150] Liberty 'Liberty's briefing on the Investigatory Powers Bill for report stage in the House of Commons June 2016' at 47 available at *https://www.libertyhumanrights.org.uk /sites/ default/files/campaigns/resources/Liberty%27s%20Briefing%20on%20the%20Investigatory%20Powers%20Bill%20for%20Report%20Stage%20in%20the%20House%20of%20Commons.pdf*, accessed 22 May 2019 quoting Joint Committee on the Draft Communications Bill: Report 11 December 2012 at 28-29.
[151] Right2Know 'SPOOKED: Surveillance of journalists in SA' op cit note 111 at 17-19.

subsequently found its way into the public domain.[152] There are likely many more unreported incidents of abuse where telecommunication service providers are not as forthcoming.

Comparative European human rights jurisprudence is clear that minimum safeguards that should be set out in law as 'effective guarantees against abuse'[153] including specifically for the protection of sensitive information, such as 'legal' or 'source' privilege. The European Court of Human Rights in *S and Marper v United Kingdom*[154] emphasised the importance of 'minimum safeguards':

> '[The Court] reiterates that it is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.'[155]

In the *amaBhungan*e case,[156] the applicant submitted that RICA 2002 was deficient in how it governed where and how intercepted data was stored, who had access to that data and how that was regulated, whether copies of the data could be made, whether copies had to be recorded, whether access could be shared within the intelligence or security communities, whether the data had to be destroyed and how irrelevant material would be separated and destroyed from the relevant material. [157] The court agreed and s 35 (powers, functions and duties of [Interception Centre] Director) and s 37 (keeping records by heads of interception centres and submission reports to Director) of RICA 2002 were declared inconsistent with the Constitution and accordingly invalid insofar as it failed to 'prescribe proper procedures to be followed when state officials are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from interceptions.'[158]

In respect of both types of communications data, RICA 2002 provides that the direction issued 'may specify conditions or restrictions relating to the provision' of real-time or archived

---

[152] Ibid. See also P Bruce 'The price of writing about the Guptas' 29 June 2017 available at *https://www.businesslive. co.za/bd/opinion/columnists/2017-06-29-peter-bruce--the-price-of-writing-about-the-guptas/*, accessed 5 July 2019.
[153] *Weber's* case supra note 77 para 95, 106.
[154] EctHR 30562/04 and 30566/04 (4 December 2008).
[155] Supra note 154 para 99.
[156] *amaBhungane* case supra note 37 paras 98-108.
[157] Supra note 37 para 98.
[158] Supra note 37 para 108.

communications data.[159] The reference to 'may' is hardly pre-emptive in terms of any legal obligations on the state for the protection of communications data. There must be safeguards in legislation on storing, accessing, examining, using and destroying communications data, such that it provides adequate safeguards against abuse of treatment of personal data and thus serve to protect individuals' personal integrity.[160] These safeguards would equally apply to intercepted data, targeted and in bulk. Warrants should not be lawfully granted unless proper handling arrangements are in place.[161] An independent judicial authority must have the power to refuse an application for a warrant to intercept or obtain communications data in the absence of proper mechanisms for retention and destruction of retained data. Therefore in the process of authorisation, an independent judicial authority must be satisfied that the warranted data, once obtained, will be appropriately safeguarded. Handling arrangements safeguarding the retention of warranted data may include the following to ensure that (i) the number of persons involved, extent of any disclosure, including the extent of any copying and number of copies made are kept to the minimum necessary; (ii) the retained data must be stored in a secure manner; and (iii) each copy made of any material or data must be destroyed as soon as its retention is no longer necessary or lawfully authorised.[162]

III CONCLUSION

However the state chooses to respond to the above concerns, one thing is certain: the investigative powers of law enforcement and security and intelligence agencies to conduct electronic surveillance activities will not be a simple matter of adapting the 'square pegs' of traditional investigative powers to fit into the 'round holes' of the information age and a modern fast-paced environment of technological advancements. Communications data now being collected is different from that collected in the past and can no longer be simply regarded as less intrusive and subject to a lower standard of judicial authorisation. There must there be sufficient safeguards in place against the risk of abuse of discretionary powers in the retention and acquiring of communications data. This includes ensuring that warranted data once obtained must be on the basis of arrangements for retention safeguards in related provisions. If

[159] Section 17(5)*(c)* and 19(5)*(d)*.
[160] *Centrum för Rättvisa* supra note 75 para 147.
[161] For example, see handling arrangements in provisions of the IPA 2016 referred earlier.
[162] See *The Queen (on Application of National Council for Civil Liberties (Liberty) v Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs* [2019] EWHC 2057 (Admin) paras 353-392 (the challenge in respect of MI5's handling arrangements and provision of the IPA 2016.).

not, an application for a warrant should not be granted. Another key area identified as requiring reform relates to addressing concerns that s 205 of the CPA 51 of 1977 has created a parallel process for the state to obtain communications data from third party telecommunication service providers, with less oversight and protections than RICA 2002.

Another investigatory power identified in the thesis as requiring essential reform in South African law, relates to access to data protected by encryption from a suspect/target of an investigation. This is the subject of chapter four to follow.

CHAPTER FOUR

OBTAINING EVIDENCE FROM A SUSPECT/TARGET OF AN INVESTIGATION: COMPELLED DECRYPTION AND THE CONSTITUTIONAL RIGHT AGAINST SELF-INCRIMINATION

I INTRODUCTION

The ability and use of encryption to conceal information is not new: '[i]n 1807, during the treason trial of Aaron Burr, the prosecution attempted to decipher Burr's encrypted messages by forcing his private secretary to testify about their plaintext meaning. Even further back, in 1587, Mary Queen of Scots was convicted of treason and then beheaded when her role in an assassination plot against Queen Elizabeth was revealed by the decryption of private letters among the conspirators.'[1] Encryption 'is a technological implementation of cryptography: information is converted to an unintelligible form – encoded – such that it can only be translated into an understandable form – decoded – with a key.'[2] There are different types of encryption. Encryption by a passcode, pattern or password is the modern-day and information era method of protecting electronic information, especially on most smartphone mobile devices. Doing so unlocks the device and decrypts its contents.[3] Essentially, a passcode, pattern or password is 'a unique combination of characters that acts as a key' that must be typed into the device to unlock the encrypted device.[4] Biometic features such facial recognition or fingerprint-based encryption technology are also common measures. More sophisticated applications such as cryptography involve the process of scrambling stored or transmitted information such that it is unintelligible without the correct key.

Companies such as Apple and Samsung, including other social media and messenger communication platforms such as WhatsApp and Facebook, as a matter of course have made *end-to-end encryption* standard in its services. In this type of encryption, only the sender and recipient hold the keys to encrypt and decrypt messages, and the service provider has no way of accessing the actual content of the communications.[5] Similarly, *encryption in*

[1] OS Kerr & B Schneider 'Encryption workarounds' (2018) 106 *Georgetown LR* 989 at 991 referring to D Kahn *The Codebreakers: The story of secret writing* (1996) 119-124.
[2] See 'What is encryption' in *Google transparency report* available at *https://support.google.com/transparency report/answer/7381231*, accessed 13 April 2020.
[3] OS Kerr 'Compelled decryption and the privilege against self-incrimination' (2019) 97 *Texas LR* 767.
[4] Ibid 768.
[5] See 'What are some types of encryption' in *Google transparency report* available at *https://support.google. com/transparencyreport/answer/7381231*, accessed 13 April 2020.

transit protects the flow of information from the end user to a third-party's server. For example, in online financial transactions, when on a shopping site and credit card credentials are entered, a secure connection protects our information from interception by a third party while in transit only the user and the server they connect to can decrypt the information.[6] According to recent report, as at 29 March 2020, Google has achieved ninety-five percent encryption across its products and services by default.[7] *Encryption at rest* protects information when it is not in transit.[8] For example, the hard disk in a computer may use encryption at rest to ensure the files are protected from unauthorised access.

While encryption is a powerful tool for safeguarding sensitive information, especially in response to increased levels of privacy awareness, data breaches and identity theft, the proliferation of robust digital encryption technologies have also presented opportunities for criminals to encrypt data in order to conceal their criminal activities and so evade detection and prosecution. For example, in 2016 the FBI sought to access the encrypted phone of one of the accused's' of the December 2015 San Bernardino shooting, who was killed during the attack. In order to access the contents of the phone, the FBI wanted Apple to create or to enable installation of bespoke software to circumvent the security protections built into all of its iPhones.[9] Apple argued it was a demand too sweeping to be compatible with responsible security practices and individual privacy rights.[10]

The focus of this chapter is on another legally and very different situation, the end-point user who is compelled to either enter or provide a passcode or decrypt the data contained in a device pursuant to legitimate legal process set out in law, as opposed to compelled assistance on the part of the device and software manufacturer. With modern-day types of encryption being frequently used, this means that law enforcement and security and intelligence agencies cannot easily have access to such electronic information, real-time or archived, from third party

---

[6] Ibid.
[7] See 'Encryption traffic across Google' in *Google transparency report* available at *https://transparencyreport.google.com/https/overview?hl=en*, accessed 13 April 2020.
[8] See 'What are some types of encryption' op cit note 5.
[9] See A Selyukh 'A year after San Bernardino and Apple-FBI, where are we on encryption?' (Dec 2016) available at *https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-*encryption, accessed 8 April 2020 and by the same author 'Apple vs. The FBI: The unanswered questions and unsettled issues' available at *https://www.knkx.org/post/apple-vs-fbi-unanswered-questions-and-unsettled-issues*, accessed 8 April 2020. See also 'Apple v. FBI concerning an order requiring Apple to create custom software to assist the FBI in hacking a seized iPhone' available at *https://epic.org/amicus/crypto/apple/*, accessed 8 April 2020.
[10] The Oscar Pistorius trial provides a South African example. See 'How police accessed Pistorius's iPhone (March 2014) available at *https://wwwtechcentral.co.za/how-police-accessed-pistoriuss-iphone-47127/*, accessed 8 April 2020.

telecommunication service providers as they perhaps once could be able to do so. They must seize encrypted devices, which of course can be validly obtained. However, once they have the seized encrypted device, the challenge is that they will be unable to decrypt and access the device and its contents without a password or passcode.

A recourse for law enforcement and security and intelligence agencies in South African law is to 'compel the key'. Part II is an overview of the powers of law enforcement and security and intelligence agencies to compel decryption. The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002[11] provides a legal framework for compelled decryption from the suspect/target of an investigation. RICA 2002 compels (a) disclosure of the decryption key; or (b) provision of decryption assistance[12] to obtain access to the encrypted information or to put that encrypted information in an intelligible form.[13] The provision also enables law enforcement and state and security officials to serve a direction requiring disclosure of an encryption key to enable such encrypted data to be made intelligible. Part III considers certain legal issues that may arise in relation to compelled decryption. Compelled decryption directions inevitably engage the constitutional right against self-incrimination.[14] These powers anticipate, at the very least, that the potential disclosure of information may incriminate the suspect/target to whom a compelled decryption order is directed. This chapter examines the constitutional protections against self-incrimination, as it applies to decryption orders by a designated judge directing a suspect/target of an investigation to provide assistance in the decryption of specific encrypted data or devices. Applying the constitutional law framework on the right against self-incrimination, two distinct issues arise with regard to compelled disclosure and modern technology: (a) compelled disclosure of a user's passcode (reveal/enter the passcode); and (b) compelled entry of a biometric based information (by placing a finger on a device or by facial recognition).

[11] Hereafter 'RICA 2002'.
[12] Section 29(1)*(a)* and *(b)*.
[13] Section 29(2).
[14] See Kerr op cit note 3 at 768 for recent cases and differing outcomes in the United States of America: *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011 (Doe II)* 670 F.3d 1335, 1349 (11th Cir 2012) (declaring that the government could not compel decryption); *United States v Apple MacPro Computer* 851 F.3d 238, 248 & n.7 (3d Cir 2017) (allowing compelled decryption), cert. denied, 138 S Ct 1988 (2018); *United States v Spencer* No. 17-cr-00259-CRB-1, 2018 WL 1964588 (ND Cal Apr 26, 2018) (same); *United States v Fricosu* 841 F. Supp. 2d 1232, 1237 (D Colo 2012) (allowing compelled decryption); *United States v Mitchell II* 76 M.J. 413, 424–25 & n.5 (CAAF 2017) (Ryan, J dissenting) (allowing compelled decryption, in dissenting opinion); *State v Stahl* 206 So. 3d 124, 136–37 (Fla Dist Ct App 2016) (same); *Seo v State* 109 N.E.3d 418, 425–31 (Ind Ct App. 2018) (compelled decryption not allowed), *transfer granted, opinion vacated*, 2018 WL 6565988 (Ind Dec 6 2018); and *Commonwealth v Gelfgatt* 11 N.E.3d 605, 614–15 (Mass 2014) (allowing compelled decryption).

The South African courts have yet to address these issues. The realities of a fast-paced environment of modern technology may well require such rethinking of doctrines to adequately safeguard constitutional rights into the future. In the analysis, a nuanced understanding of the interaction between modern technology and legal doctrine will therefore be integral in the development of doctrinal principles that involve 'reveal-the-passcode', 'use-a-fingerprint-or-facial-recognition', 'enter-the-passcode' or 'produce-the-decrypted-data' scenarios. Part IV considers the development of a doctrinal approach in South African law. A conclusion is drawn in Part V.

II REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT 70 OF 2002 AND ACCESS TO DATA PROTECTED BY ENCRYPTION

One of the most controversial provisions of RICA 2002 allows law enforcement and state and security officials to require a subject/target to disclose the key, or decrypt encrypted data. The preamble to RICA 2002 states: 'to regulate the execution of directions and entry warrants by law enforcement officers and the assistance to be given by … decryption key holders in the execution of such directions and entry warrants.' The relevant provision of RICA 2002 gives to law enforcement and state and security officials the power to require a person to put encrypted electronic information into intelligible form - that is, to provide access to it, decrypt it or decode it. The purpose of compelled decryption is that law enforcement and security and intelligence agencies encounter encrypted data more frequently and that this trend will continue as encryption becomes more pervasive, posing challenges to, among others, criminal investigators seeking to put encrypted information into intelligible form. A compelled decryption direction[15] is often a useful default, and can be used in a wide range of cases, and sophisticated technical resources are not required.[16] It does raise, however, certain practical and legal issues.

As regards applications and issuing of a decryption direction, in terms of s 21 of RICA 2002, an applicant of a decryption direction must specify, if known: (i) the decryption key which must be disclosed, or (ii) decryption assistance which must be provided, and the form

[15] '"Decryption direction" means a direction issued under section 21(3) in terms of which a decryption key holder is directed to-(a) disclose a decryption key; or (b) provide decryption assistance in respect of encrypted information, and includes an oral decryption issued under section 23(7).'

[16] The subject/target of a decryption direction may of course refuse to hand over the key, or use it to decrypt a device or information. See Kerr and Schneider op cit note 1 at 1004.

and manner in which it must be provided.[17] The application for a decryption direction is made to a designated judge and may 'only be issued' if 'there are reasonable grounds to believe' that: (i) the communication contains encrypted information; (ii) the decryption key holder specified in the application is in possession of the encrypted information and the decryption key; (iii) the purpose for which the interception direction was issued would be defeated if the decryption direction was not issued; and (iv) it is not reasonably practicable for the applicant to obtain possession of the encrypted information without the issuing of a decryption direction.[18] The designated judge must also give consideration to the following: (i) the extent and nature of the encrypted information; and (ii) any adverse effect that the issuing of a decryption direction may have on the business of the decryption holder.[19] In terms of s 21(5)*(d)*, a decryption direction may 'specify conditions or restrictions relating to decryption authorised.' In addition, a decryption direction 'may be issued for a period not exceeding three months at a time.'[20] Section 16(7) which provides for blanket prohibition on notification to the subject/target of the application, also applies in respect of the issuing of a decryption direction.[21]

The empowering provision of compelled decryption is s 29. The decryption key holder must (a) disclose the decryption key; or (b) provide decryption assistance.[22] In complying with a decryption direction, a decryption key holder (a) *must* only disclose the decryption key or provide decryption assistance *which is necessary* to obtain access to the encrypted information or to put that encrypted information in an intelligible form; (b) *may* only disclosure the decryption key or provide decryption assistance to the authorised person; and (c) *may* not disclose any other information which is not specified in the interception direction.[23] Provision is also made for a decryption key holder who is in possession of both the encrypted information and the decryption key who (a) may use the decryption key in his possession to provide decryption assistance; and (b) must make a disclosure of the encrypted information in an

[17] Section 21(2)*(c)*.
[18] Section 21(4)*(a)*. Section 1 sets out the following definitions and interpretation of relevant key terms: '"decryption assistance" means to-(a) allow access, to the extent possible, to encrypted information; or (b) facilitate the putting of encrypted information into an intelligible form'; '"decryption key" means a key, mathematical formula, code, password, algorithm or any other data which is used to-(a) allow access to encrypted information; or (b) facilitate the putting of encrypted information into an intelligible form'; '"decryption key holder" means any person who is in possession of a decryption key for purposes of subsequent decryption of encrypted information related to indirect communications; "intelligible form" means the form in which electronic data was before an encryption or similar process was applied to it.'
[19] Section 21(4)*(b)*.
[20] Section 21(5)*(e)*.
[21] Section 21(6).
[22] Section 29(1).
[23] Section 29(2) (emphasis added).

intelligible form.[24] A decryption key holder required to provide decryption assistance in respect of encrypted information will be regarded as having complied with a decryption direction, if (a) the decryption key to the encrypted information is by disclosure of the key (instead of providing decryption assistance); and (b) makes such disclosure of the decryption key to the authorised person in accordance with the decryption direction and within the time period specified by which decryption assistance was to be provided.[25] If a decryption key holder is (a) not in possession of the encrypted information, or (b) incapable of complying with the decryption direction, without the use of a decryption key that is not in their possession, 'must endeavour to comply, to the best of his or her ability, with that decryption direction.'[26] An authorised person to whom the decryption key is disclosed: (a) may only use the decryption key for the encrypted information specified in the decryption direction; and (b) must, on or before expiry of the period of the decryption direction, destroy all records of the disclosed decryption key, if in the opinion of the applicant (i) there will be no criminal or civil proceedings; or (ii) such records will not be required in criminal or civil proceedings as evidence or for the purposes of an order of court.[27] A decryption holder, or employee of a decryption holder who fails to comply with a decryption direction is guilty of an offence and subject to penalties, including fines and/or imprisonment.[28]

III COMPELLED DECRYPTION: LEGAL ISSUES

In keeping with the analytical layout of this thesis, which follows the temporal development of an investigation, this section of the chapter focuses on a type of investigative power requiring a subject/target to disclose the key to a device, or decrypt encrypted data in terms of RICA 2002. There are many aspects to the encryption debate, in particular, levels of concern amongst law enforcement and intelligence agencies by the increased trend towards user-controlled encryption. Recent privacy-enhancing changes introduced by companies such as Google, Apple, WhatsApp, include encryption by default on its devices and operating systems, and effectively mean that the encryption of devices and the information contained therein are now user-controlled. I therefore also examine below the other necessary accompanying aspect of the encryption debate insofar as it relates to user rights.

[24] Section 29(3).
[25] Section 29(4).
[26] Section 29(5).
[27] Section 29(8).
[28] Section 51(4).

(a) The right against self- incrimination

The courts in South Africa have yet to address compelled disclosure of a user's passcode (reveal/enter the passcode) and compelled entry of a biometric based information (by placing a finger on a device or by facial recognition), but has provided some insight in dicta on how it might rule on this issue. The right against self-incrimination has been recognised, and is deeply rooted in common law,[29] and also in certain statutory provisions.[30] In terms of constitutional protections, the Constitution of the Republic of South Africa Act 108 of 1996[31] places the right against self-incrimination,[32] as with the right to remain silent, in s 35 which provides for the 'rights of arrested, accused and detained persons' in relation to a fair trial 'not to be compelled to give self-incriminating evidence.'[33]

The jurisprudence of the South African courts has been rather rudimentary on the distinction between self-incriminating testimonial communications and incriminating non-testimonial real evidence[34] in relation to evidence 'emanating from the accused'[35] by some degree of compulsion.[36] Thus, a suspect/target may be compelled to provide physical evidence that may be incriminating such as a blood sample[37], to provide a palm print[38], or finger prints[39],

[29] *Blunt v Park Lane Hotel* [1942] 2 KB 53 257, Goddard LJ stated: 'no one is bound to answer any question if the answer thereto would, in the opinion of the judge, have a tendency to expose [him] to any criminal charge, penalty or forfeiture which the judge regards as reasonably likely to be preferred.'
[30] For example, s 14 of the Civil Proceedings Evidence Act 25 of 1965 and s 203, 217 and 219A of the Criminal Procedure Act 51 of 1977.
[31] Hereafter 'the Constitution'.
[32] *S v Gqoza* (1) 1994 1 BCLR 1 (Ck); 1994 2 SACR 228 (Ck); *S v Maseko* 1996 9 BCLR 1137 (W); *Wehmeyer v Lane* 1994 2 BCLR (C); 1994 4 SA 441 (C).
[33] Section 35(1) and s 35(3)(j).
[34] Email communication Professor PJ Schwikkard, 16 July 2019.
[35] PJ Schwikkard & SE van der Merwe *Principles of Evidence* 4ed (2015) at 253: 'Ever since the decision in *Ex Parte Minister of Justice: In Re Rex v Matemba*, and even after constitutionalization, our courts have – in line with the majority decision in *Schmerber v California* and the common-law rule as formulated by Wigmore – consistently held that the privilege against self-incrimination is confined to testimonial utterances or communications (statements and pointings out) and does not extend to real evidence emanating from an accused, such as hair samples, blood samples, fingerprints, voice, handwriting, and even a bullet lodged in the body of a suspect.' (footnotes omitted).
[36] Ibid at 145-149 and 253-256. See also DT Zeffertt & DT Paizes *The South African Law of Evidence* 2ed (2003) at 607-613.
[37] *S v Binta* 1993 (2) SACR 553 (C); *S v Orrie and Another* 2004 1 SACR 162 (C). See also *Schmerber v California* 384 US 75 (1966) at 763-64: 'it is clear that the protection of the privilege reaches an accused's communications, whatever form they might take.'
[38] *Ex parte Minister of Justice: In re R v Matemba* 1941 AD 75; *R v Camane* 1925 AD 570.
[39] *S v Huma and Another (2)* 1995 (2) SACR 411 (W); *S v Maphumulo* 1996 (2) SACR 84 (N); *Msomi v Attorney-General of Natal* 1996 (8) BCLR 1109 (W).

or a voice exemplar[40], submit to an operation[41], provide a handwriting sample[42], to stand in a line-up[43], and to wear a particular set of clothing.[44] Real evidence 'emanating from an accused' may well be incriminatory against the accused. The question that arises is whether such acts of compulsion conflict with s 35(1)*(c)* of the Constitution, which provides for the right 'not to be compelled to give self-incriminating evidence.' This brought to the fore judicial debate as to whether the right against self-incrimination applied to real evidence, and if so, should the evidence be excluded.[45]

In *R v Camane and Others*,[46] Innes CJ analysed the same some sixteen years before *Matemba's* case, and in referring to autoptic evidence held that 'a man may be compelled, when in Court, to do what he would rather not. His features may be of importance, and he may be made to show them; his complexion, his stature, mutilations, or marks on his body, may be relevant points, and he may be compelled to show them to the Court.'[47] Despite the clarity of Innes CJ's judgment, competing approaches as to whether such evidence derived from an accused's physique violates the right against self-incrimination continued to endure in South Africa law. Sixteen years later, Watermeyer JA in *Ex Parte Minister of Justice: In Re Rex v Matemba*[48] confirmed the approach taken in *Camane*. The accused was charged with a house-breaking and before trial a print of the palm of one of the accused's hands was 'compulsorily taken' by a police officer without his consent. At trial the print taken from the accused's palm was tendered as evidence for the purpose of making a comparison with the

[40] *R v Gericke* 1941 CPD 211; *Levack v Regional Magistrate, Wynberg and Another* 2003 (1) SACR 187 (SCA). See also *United States v. Dionisio* 410 U.S. 1, 6 (1973) where the Court held: '[t]he voice recordings were to be used solely to measure the physical properties of the witnesses' voices, not for the testimonial or communicative content of what was to be said.'
[41] *Minister of Safety and Security v Gaqa* 2002 (1) SACR 654 (C) and *Minister of Safety and Security v Xaba* 2004 (1) SACR 149 (D).
[42] *S v Duna and Others* 1984 (2) SA 591 (CkS). See also *Gilbert v California* 388 U.S. 263, 265 (1967) stating: '[a] mere handwriting exemplar…is an identifying physical characteristic.'
[43] See *United States v Wade* 388 U.S. 218 (1967) that 'privilege prohibits compulsion to disclose any knowledge he might have or to speak his guilt.'
[44] In *Holt v United States* 218 U.S. 245, 251 (1910) the Court stated: '[b]ut the prohibition…is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence.'
[45] For case law on the common law right against self-incrimination, see *Goorpurshad v R* 1914 35 NLR 87 and *R v Maleke* 1925 TPD 491. In the latter case, the court refused to admit evidence of a footprint obtained by compelled force. At 534, it was held: '[I]t compels an accused person to convict himself out of his own mouth; that it might open the door to oppression and persecution of the worst kind; that it is a negation of the liberty of the subject and offends against our sense of natural justice and fair play ....'
[46] Supra note 38.
[47] Supra note 46 at 575. Cited with approval in *Levack's* case supra note 40 para 17; *S v Zuma and Others* 1995 (2) SA 642 (CC) para 31, and in *Ferreira v Levin NO and Others; Vryenhoek and Others v Powell NO and Others* 1996 (1) SA 984 (CC) paras 23, 96.
[48] Supra note 38.

print found on the window sill, and thus to identify the accused as the person who had broken into the premises.[49]

The adoption of the principle of constitutional supremacy and a Bill of Rights in the 1990's gave rise to renewed debate. The task of explaining 'that "autoptic evidence" – evidence derived from the accused's own bodily features – does not infringe the right to silence nor the right not to be compelled to give evidence has continued to fall upon' the courts.[50]

In *S v Huma and Another (2)*,[51] in a matter dealing with the taking of fingerprints the accused claimed the protections of the constitutional right against self-incrimination. Claassen J found the 'objection' to be 'entirely without substance' as the privilege against self-incrimination did not apply to procedures relating to the ascertainment of bodily features such as identification parades, the taking of finger- and footprints, blood samples and the showing of bodily scars.[52] These procedures, he held, relate to what has been termed 'real' evidence, as opposed to oral or testimonial evidence by the accused.[53] In support thereof, Claassen J found the 'logic and reasoning of Brennan J compelling'[54] in *Schmerber v California*[55] where the court held that the right against self-incrimination 'protects an accused only from being compelled to testify against himself or otherwise provide the State with evidence of a testimonial or communicative nature, and that the withdrawal of blood and use of the analysis in question in this case did not involve compulsion to these ends.'[56] In doing so, the court referred to '[t]he distinction which has emerged' in that the right against self-incrimination protects 'against compelling "communications" or "testimony"' but does not violate the constitutional right against self-incrimination where 'that compulsion which makes a suspect or accused the source of "real or physical evidence".'[57]

This approach was adopted by the Supreme Court of Appeal in *Levack v Regional Magistrate, Wynberg and Another* a case in which Cameron JA concluded that '[t]he

[49] Supra note 38 at 77, 82-83. Cf *S v Sheehama* 1991 (2) SA 860 (A).
[50] *Levack's* case supra note 40 para 19 with reference to *Nkosi v Barlow NO en Andere* 1984 (3) SA 148 (T) at 151-152; *Binta's* case supra note 37 at 562d-e; *Huma's* case supra note 39 at 237-240; and *Maphumulo's* case supra note 39 at 87-90.
[51] 1995 (2) SACR 411 (W).
[52] Supra note 51 at 417.
[53] Supra note 51 at 417.
[54] Supra note 51 at 419.
[55] *Schmerber's* case supra note 37.
[56] Supra note 55 at 761 (footnotes omitted).
[57] Supra note 55 at 764.

explanations given in these cases apply in all details to the human voice.[58] It falls within the same category as complexion, stature, mutilations, marks and prints.'[59] An order was granted that the accused in the presence of their legal representatives give the state voice samples as specified by a named 'voice expert' and the purpose was to compare the samples with tape recordings of telephone conversations in the state's possession, for possible later use during the trial. The grounds of review relied on by the appellants included inter alia that 'an order that voice samples be provided under compulsion would effectively breach the appellants' constitutionally protected privilege against self-incrimination and result in an unfair trial.'[60] Applying the distinction made in case law, Cameron J held that 'there is no difference in principle between the visibly discernible physical traits and features of an accused and those that under law can be extracted from him through syringe and vial or through the compelled provision of a voice sample. In neither case is the accused required to provide evidence of a testimonial or communicative nature, and in neither case is any constitutional right violated.'[61] Put differently, it would be wrong to suppose that requiring appellants to submit voice samples infringed their right to remain silent or not to give self-incriminating evidence.[62]

The other approach of the appellant's argument that a compelled order violates the appellants' fair trial rights was also rejected by Cameron J.[63] The alternate view is to apply a generous interpretation to the content of the privilege against self-incrimination and recognise that the ascertainment of bodily feature may infringe the privilege, but that it is a justified limitation of the right not to self-incriminate in terms of s 36 of the Constitution having regard to the factors specified.[64]

In *S v Orrie and Another*,[65] the High Court found that 'there can be little doubt' that the involuntary taking of a blood sample for the purposes of DNA profiling is both an

---

[58] This is also the position in the United States of America. See *Wade's* case supra note 43; *Gilbert's* case supra note 42; and *Dionisio's* case supra note 40.
[59] Supra note 40 paras 17, 19.
[60] Supra note 40 para 7.
[61] Supra note 40 paras 20-21 (footnotes omitted).
[62] Supra note 40 paras 15-23.
[63] Supra note 40 paras 22-23 (footnotes omitted). Cameron JA: 'At present the only question before us is whether an order requiring an accused to supply in the presence of defence lawyers voice samples indicated by a State-designated 'expert' is competent. Those samples have not yet been procured. The 'expert's' report has not yet been prepared. Its value and the weight that should properly be accorded it have not arisen for determination.'
[64] Including '(a) the nature of the right; (b) the importance of the purpose of the limitation; (c) the nature and extent of the limitation; (d) the relation between the limitation and its purpose; and (e) less restrictive means to achieve the purpose.' See earlier chapter 2 at 66-70 and chapter 3 at 104-111.
[65] 2004 1 SACR 162 (C). See also *Ferreira's* case supra note 47, which dealt with s 417(2)(b) of the Companies Act 68 of 1973 that compelled a person summoned to an enquiry to testify and produce documents, even though the evidence may be incriminating. At para 259 Sachs J observed that 'the more that self-incrimination takes the

infringement of the right to privacy and an infringement of the right to bodily security and integrity.[66] Bozalek J held that the infringement was justifiable: 'to the extent, however, that the involuntary taking of a blood sample from an accused for the purposes of compiling a DNA profile for use in criminal proceedings infringes his or her right to privacy, dignity and bodily integrity, I am of the view that the limitation clause in the Constitution (s 36 of Act 108 of 1996) permits the limitation of these rights, through the medium of s 37 of the Criminal Procedure Act.'[67] As also held by the Privy Council in *Brown v Stott*,[68] the right against self-incrimination is not absolute and incursions may be justified where the demand for incriminating information pursues a legitimate aim (e.g. a response to a social problem of dangerous driving) and the incursion is no greater than necessary.

An interesting question arises: in following the rudimentary treatment in legal precedent, is the distinction between self-incriminating testimonial communications and incriminating non-testimonial real evidence 'emanating from the accused' as clear-cut and precise? Notably, four dissenting Justices in *Schmerber*, in equally compelling dissenting opinions, thought not.[69] Black J, with whom Douglas J joined in dissent, argued that the

---

form of oral communication, the more compelling will the protection be; the more objective or real the existence of the incriminating material, on the other hand, the more attenuated. …pre-trial procedures of a non-communicative or non-testimonial kind, such as compulsory fingerprinting, blood tests, blood-alcohol tests, attendance at identity parades, DNA and other tests of an objective nature, or, in company fraud matters, hand-writing tests, all of which would seem to fall directly under the concept of freedom and personal security, have become well-established processes regarded in many parts of the world as being consistent with the values of an open and democratic society based on freedom and equality, and in suitably controlled conditions, would have far less difficulty in passing section 33 scrutiny in terms of our Constitution.'

[66] Supra note 65 at 168.

[67] Supra note 65 at 169. See also *Gaqa's* case supra note 41 at 658; which involved an application to surgically remove a bullet from the accused's body contrary to the accused's express wishes, Desai J held that the relevant provisions of the Criminal Procedure Act 51 of 1977 'permit the violence necessary to remove the bullet' and that although the 'proposed surgical intervention to remove the bullet would undoubtedly be a serious affront to the respondent's human dignity and an act of State-sanctioned violence against his bodily and perhaps also psychological integrity' the infringement of rights was justifiable. Cf *Xaba's* case supra note 41.

[68] [2001] 2 WLR 817. At 836: 'The jurisprudence of the European Court very clearly establishes that while the overall fairness of a criminal trial cannot be compromised, the constituent rights comprised, whether expressly or implicitly, within article 6 are not themselves absolute. Limited qualification of these rights is acceptable if reasonably directed by national authorities towards a clear and proper public objective and if representing no greater qualification than the situation calls for … The Court has also recognised the need for a fair balance between the general interest of the community and the personal rights of the individual, the search for which balance has been described as inherent in the whole of the Convention.'

[69] Chief Justice Warren at 773 found it 'sufficient' to reiterate his dissenting opinion in *Breithaupt v Abram* 352 U. S. 432, 352 U. S. 440, as the basis on which to reverse this conviction. Justice Black found that the officers violated Schmerber's right against self-incrimination. At 778, he wrote, '[b]elieving with the Framers that these constitutional safeguards broadly construed by independent tribunals of justice provide our best hope for keeping our people free from governmental oppression, I deeply regret the Court's holding.' Justice Douglas (at 778-79) also reiterated his dissent in *Breithaupt v Abram* supra, as the basis on which to reverse this conviction, and also referred to 'a zone of privacy enumerated in *Griswold v Connecticut,* 381 U. S. 479 that '[n]o clearer invasion of this right of privacy can be imagined than forcible bloodletting of the kind involved here.' Finally, Justice Fortas held that the right against self-incrimination applies, and at 779 stated 'the State has no right to

'compulsory extraction of petitioner's blood for analysis so that the person who analyzed it could give evidence to convict him had both a "testimonial" and a "communicative nature".'[70] The report of the blood test was 'testimonial' or 'communicative' because the test was performed in order to obtain the testimony of others, communicating to the jury facts about the petitioner's condition: '[t]he sole purpose of this project, which proved to be successful, was to obtain "testimony" from some person to prove that petitioner had alcohol in his blood at the time he was arrested. And the purpose of the project was certainly "communicative" in that the analysis of the blood was to supply information to enable a witness to communicate to the court and jury that petitioner was more or less drunk.'[71] Black J found it 'unfortunate' that the majority relied 'so heavily for its very restrictive reading of the Fifth Amendment's privilege against self-incrimination on the words "testimonial" and "communicative".'[72] The use of these particular words he argued 'are not models of clarity and precision.'[73] Brennan J considered the same and noted that 'all evidence received in court is "testimonial" or "communicative" … [b]ut the Fifth Amendment relates only to acts on the part of the person to whom the privilege applies, and we use these words subject to the same limitations. A nod or headshake is as much a "testimonial" or "communicative" act in this sense as are spoken words. But the terms as we use them do not apply to evidence of acts noncommunicative in nature as to the person asserting the privilege, even though, as here, such acts are compelled to obtain the testimony of others.'[74]

At present it appears to be an open question in South African law. In my view, even if in future cases, the South African courts take the approach of the dissenting opinions in *Schmerber*, particularly that of Justice Black, acts of compulsion in terms of certain statutory provisions may well survive a constitutional challenge.[75] Although the court may find that the compelled act infringes the right against self-incrimination, the limitations clause in this regard will certainly be in the reckoning, such that an infringement can be justified in terms of s 36 of the Constitution, if it is reasonable and justifiable in an open and democratic society, having regard to the factors specified in s 36.[76] While this makes good sense, a notably different

commit any kind of violence upon the person, or to utilize the results of such a tort, and the extraction of blood, over protest, is an act of violence.'

[70] Supra note 40 at 774.

[71] Supra note 40 at 774.

[72] Supra note 40 at 774.

[73] Supra note 40 at 774.

[74] Supra note 40 at footnote 5.

[75] See Schwikkard and Van der Merwe op cit note 35 at 149.

[76] See *Orrie's* case supra note 37. See also *S v R and Others* 2000 (1) SACR 33 (W) in which Willis J found that although 'an involuntary blood test unquestionably constituted an invasion of privacy' (at 39) and a person's

approach was taken by the Supreme Court of Canada in *R v Stillman*,[77] where the majority held that for the purposes of s 24(2) of the Charter that 'the compelled use of the body or the compelled provision of bodily substances in breach of a Charter right for purposes of self-incrimination will generally result in an unfair trial just as surely as the compelled or conscripted self-incriminating statement.'[78] In doing so, the majority favoured the dissenting reasons of Black J and Douglas J, and 'were of the view that taking the blood constituted a breach of the right against self-incrimination.'[79] The issue was whether evidence relating to the analysis of hair samples and teeth impressions forcibly taken rendered the trial unfair. In the classification of evidence, the court drew a distinction between 'conscriptive' and 'non-conscriptive' evidence.[80] Cory J said the following:

> 'If the accused was not compelled to participate in the creation or discovery of the evidence (i.e., the evidence existed independently of the Charter breach in a form useable by the state), the evidence will be classified as non-conscriptive. The admission of evidence which falls into this category will, as stated in *Collins*, supra, rarely operate to render the trial unfair. If the evidence has been classified as non-conscriptive the court should move on to consider the second and third of the Collins factors, namely, the seriousness of the Charter violation and the effect of exclusion on the repute of the administration of justice.'[81]

In doing so, Cory J went further to include in the category of conscriptive evidence, 'real' evidence as 'referring to anything which is tangible and exists….quite independently of a Charter breach' which he noted as 'key to their classification that they do not necessarily exist in a useable form.'[82] In an example he said: 'in the absence of a valid statutory authority or the accused's consent to take bodily samples, the independent existence of the bodily

---

right to bodily integrity, there would also be times when fairness would require that evidence, albeit obtained unconstitutionally, nevertheless to be admitted (at 40). Having regard to the cumulative weight of various factors, including the consent given by the accused, the evidence sought to be adduced by the State was admitted in the interests of a fair trial (at 42-43).

[77] (1997) 113 CCC (3d) 321 (SCC) ((1997) 144 DLR (4th) 193 (SCC), overruled in 2009 by *R v Grant* [2009] 2 SCR 353. Therefore, reliance on this judgment in the interpretation of the fair trial requirement in s 35(5) is according to Schwikkard and Van der Merwe op cit note 35 at 255 'unnecessary' and 'artificial.'

[78] Supra op cit note 77 para 223 (DLR).

[79] Supra op cit note 77 paras 84-86 (DLR). At para 86: 'It has, for a great many years, been considered unfair and indeed unjust to seek to convict on the basis of a compelled statement or confession. If it was obtained as a result of a breach of the Charter its admission would generally tend to render the trial unfair. Similarly, to compel an accused to use his body or to provide bodily substances in order to incriminate himself would generally render the trial unfair. This is so because the compelled production of bodily parts or substances is just as great an invasion of the essence of the person as is a compelled conscripted statement. The unauthorized use of a person's body or bodily substances is just as much compelled "testimony" that could render the trial unfair as is a compelled statement.'

[80] Supra op cit note 77 paras 75-83 (DLR).

[81] Supra op cit note 77 paras 75-83 (DLR).

[82] Supra op cit note 77 paras 76 (DLR).

evidence is of no use to the prosecution since there is no lawful means of obtaining it.'[83] Therefore, depending on the circumstances, the admission of real evidence, may well have a detrimental effect on the administration of justice.

Another interesting issue that arises in the consistently held distinction by our courts between self-incriminating testimonial communications and incriminating non-testimonial real evidence emanating from the accused, is the interpretation of the fair trial requirement in s 35(5) of the Constitution in relation to real evidence which has been discovered as a result of self-incriminating testimonial communications unconstitutionally obtained from the accused. Is it the case that the real evidence discovered should be treated as self-incriminating derivative evidence which, if admitted would violate the right against self-incrimination and therefore render the trial unfair? Put differently, should real evidence be excluded because it was unconstitutionally obtained, and admitting it would render the trial unfair or was otherwise be detrimental to the administration of justice.[84] Or is it the case that focusing the enquiry on the classification of the evidence, which distinguishes between the nature of the evidence – testimonial or real, is misleading, since the question should be whether the accused was compelled to provide the evidence?[85]

---

[83] Supra op cit note 77 paras 76 (DLR).

[84] See *R v Collins* (1987) 33 CCC (3d) 1 (SCC) ((1987) 38 DLR (4th) 508 (SCC), a Canadian decision, in which it was held that such evidence 'will rarely operate unfairly for the reason alone' that it was obtained in a manner that violated the Canadian Charter of Rights and Freedoms (hereafter 'the Canadian Charter) (at 526 DLR). The court drew a distinction between real and testimonial evidence, and expressed doubt that real evidence, discovered derivatively as a result of unconstitutional conscription, could render a trial unfair: '[t]he real evidence existed irrespective of the violation of the Charter and its use does not render the trial unfair' (at 526 DLR). This doctrine was invoked by the trial court in the South African case, *S v Tandwa and Others* 2008 (1) SACR 613 (SCA). The trial judge admitted the real evidence (the money from a bank robbery and an AK 47 rifle). At 646: 'The evidence is real evidence which existed independently from the pointing out made by accused no, 8 it was common cause that the accused was in possession of the money and he provided an exculpatory explanation for his possession thereof. The inclusion of such evidence would not render the trial unfair within the meaning thereof and on any of the aspects as contained in section 35(3) which aspects are not intended to be exhaustive. On the contrary, and especially in the light of the accused being in a position of providing an exculpatory explanation for his possession thereof it would in my view be detrimental to the administration of justice to exclude such evidence.' See also *S v Mkhize* 1999 (2) SACR 632 (W) (a pistol) and *S v R* (blood samples) supra note 76, that the admissibility of unconstitutionally obtained evidence did not render the trial unfair.

[85] As noted by the Supreme Court of Canada in *R v Stillman* supra op cit note 77 para 76 (DLR): 'What has come to be referred to as 'real' evidence will not necessarily fall into the 'non-conscriptive' category. There is on occasion a misconception that 'real' evidence, referring to anything which is tangible and exists as an independent entity, is always admissible.' At para 78: [t]he concept of 'real' evidence without any further description is misleading. It will be seen that, in certain circumstances, evidence such as the gun in *R v Burlingham*, [1995] 2 SCR 206, 97 CCC (3d) 385, 124 DLR (4th) 7, may come into the state's possession as a result of the accused's compelled participation or 'conscription' against himself. Thus, while the evidence is 'real' it is nevertheless conscriptive evidence.' This approach, observed Schwikkard and Van der Merwe op cit note 35 at 258, is an 'extreme example of the "fruits of the poisonous tree" doctrine.'

In South African law once it is established that evidence was obtained as a result of a breach of a constitutional right the evidence may be excluded in terms of s 35(5) of the Constitution, which provides as follows: 'Evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice.'[86] The central principle embodied in s 35(5) is the 'exclusion of unconstitutionally obtained evidence despite its relevance and regardless of the fact that it would otherwise have been admissible.'[87] Ultimately, 'the law must strive to reconcile two highly important interests' as noted by Lord Cooper in *Lawrie v Muir*: '(a) the interest of the citizen to be protected from illegal or irregular invasions of his liberties by the authorities, and (b) the interest of the State to secure that evidence bearing upon the commission of crime and necessary to enable justice to be done shall not be withheld from Courts of law on a merely formal or technical ground. Neither of these objects can be insisted upon to the uttermost.'[88] As noted by the court in *S v Tandwa and Others*,[89] a 'notable feature' of s 35(5) is that it does not provide for automatic exclusion of unconstitutionally obtained evidence – evidence must be excluded only if it (a) renders the trial unfair; or (b) is otherwise detrimental to the administration of justice.

Admitting evidence that renders the trial unfair will always be detrimental to the administration of justice,[90] however, there may be cases when the trial will not be rendered unfair, but admitting the impugned evidence will nevertheless be detrimental to

---

[86] The section is, in some respects, very similar to s 24(2) of the Canadian Charter, the relevant parts of which read: 'Where … a court concludes that evidence was obtained in a manner that infringed or denied any rights guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.' In *S v Naidoo and Another* 1998 (1) SACR 479 (N) at 502, McCall J held: 'Having regard to the similarity between s 35(5) of the new Constitution and s 24(2) of the Canadian Charter (but bearing in mind the differences between the two enactments), and also the provision in s 39(1)(c) that when interpreting the Bill of Rights, a court may consider foreign law, I am of the view that it is more helpful to interpret the provisions of s 35(5) with reference to the Canadian decisions than to those South African cases dealing with a more general discretion based on the decision in *People v O'Brien*.'

[87] Schwikkard and Van der Merwe op cit note 35 at 199. The right against compelled and non-compelled self-incrimination, trial fairness and a court's discretion have been considered in a number of cases. See *S v Lottering* 1999 12 BCLR 1478 (N) where the court was prepared to exercise discretion in a 'value judgment' (para 1483B) linked to 'notions of basic fairness and justice' and held that warnings intended to protect the right against self-incrimination did not automatically demand the exclusion of evidence (in this instance non-compelled self-incrimination testimonial communication made by the accused). See also *S v Nombewu* 1996 (2) SACR 396 (E); *S v Nell* 2009 (2) SACR 37 (C); *S v Seseane* 2000 (2) SACR 225 (O); *S v Soci* 1998 (2) SACR 275 (E).

[88] 1950 SC (J) 19 at 26-7, as quoted by Schwikkard and Van der Merwe op cit note 35 at 202.

[89] Supra note 84.

[90] In *Naidoo's* case supra note 86 at 527, McCall J noted that the words 'or otherwise' in s 35(5) meant that an unfair trial is always detrimental to the administration of justice.

the administration of justice on the basis of considerations of broad public policy.[91] In determining whether the trial is rendered unfair, in a broader enquiry, courts must take into account competing social interests.[92] In *Key v Attorney-General, Cape Provincial Division and Another*,[93] Kriegler J described the fair trial inquiry as follows:

> 'What the Constitution demands is that the accused be given a fair trial. Ultimately ..., fairness is an issue which has to be decided upon the facts of each case, and the trial Judge is the person best placed to take that decision. At times fairness might require that evidence unconstitutionally obtained be excluded. But there will also be times when fairness will require that evidence, albeit obtained unconstitutionally, nevertheless be admitted.'[94]

The court's discretion must be exercised 'by weighing the competing concerns of society on the one hand to ensure that the guilty are brought to book against the protection of entrenched human rights accorded to accused persons.'[95] In doing so, Cameron JA , Mlambo JA and Hancke AJA in *Tandwa* referred to 'relevant factors' including 'the severity of the rights violation and the degree of prejudice, weighed against the public policy interest in bringing criminals to book.'[96] In a case that involved the discovery of real evidence (money from a bank robbery and an AK 47 rifle) from the accused under duress and torture by police brutality, the learned justices emphasised the importance of excluding evidence in instances of a flagrant and deliberate violation of an accused's constitutional rights:

> 'Rights violations are severe when they stem from the deliberate conduct of the police or are flagrant in nature. There is a high degree of prejudice when there is a close causal connection between the rights violation and the subsequent self-incriminating acts of the accused. Rights violations are not severe, and the resulting trial not unfair, if the police conduct was objectively reasonable and neither deliberate nor flagrant.' [97]

---

[91] *Tandwa's* case note 84 at 648.
[92] Supra note 84 at 648. In *S v Mphala and Another* 1998 (1) SACR 654 (W) at 657, Cloete J said: 'So far as the administration of justice is concerned, there must be a balance between, on the one hand, respect (particularly by law enforcement agencies) for the Bill of Rights and, on the other, respect (particularly by the man in the street) for the judicial process. Overemphasis of the former would lead to acquittals on what would be perceived by the public as technicalities, whilst overemphasis of the latter would lead at best to a dilution of the Bill of Rights and at worst to its provisions being negated.'
[93] 1996 (2) SACR 113 (CC) at 196.
[94] Supra note 93 at 196.
[95] *Lottering's* case supra note 87 at 1483, where it was held that the accused's pointing out of evidence should be admitted even though he had not been warned of his rights: constitutional rights violations only render the trial unfair (and justify exclusion of evidence) if they are deliberate or flagrant.
[96] Supra note 84 at 648.
[97] Supra note 84 at 648. See *Seseane's* case supra note 87 where the deliberate nature of police conduct in not explaining the accused's rights, as part of an attempt to 'trap the accused, justified exclusion of the incriminating statements.

Against the background that 'central in this inquiry is the public interest'[98] and that s 35(5) 'is designed to protect individuals from police methods that offend basic principles of human rights'[99] the court found that the admission of derivative evidence blemished by police brutality was undeniably detrimental to the administration of justice and that '[a]dmitting real evidence procured by torture, assault, beatings and other forms of coercion violates the accused's fair trial right at its core, and stains the administration of justice.'[100] It is submitted that in these circumstances of 'barbarous and unacceptable conduct'[101] by the police, the facts of the case demanded the exclusion of the evidence. The 'basic principles of human rights' and notions of basic fairness and justice must be applied to the facts of a case and, by reference to the approach of our courts, this necessarily involves considerations of public interest in determining whether the trial is rendered unfair by admitting the impugned evidence.

In *S v Naidoo and Another*,[102] a case considered to be a 'bold' interpretation of s 35(5),[103] the law enforcement authority furnished false and misleading affidavits to a judge in order to obtain judge's direction, in terms of Interception and Monitoring Prohibition Act 127 of 1992 permitting law enforcement to monitor certain telephones. The two main issues before the court was (a) whether the fact that the direction was granted on the basis of false, in some respects grossly false, as noted by the court, and misleading information invalidated the direction given by the judge and thus deprived the monitoring of its legality;[104] and (b) would the admission of evidence of the contents of the conversations render the trial unfair or otherwise be detrimental to the administration of justice?[105] In respect of the first issue, the court found that the direction issued by the judge was invalid. Further, that there was a violation of the accused's right to personal privacy and, in particular, the right not to be subject to the violation of private communications.[106] On the second issue, the court held that the admission of the evidence of the two telephonic conversations, which violated the right against self-incrimination, would render the trial unfair and would be detrimental to the administration of justice, and fell to be excluded in terms of s 35(5) of the Constitution.[107] The conflicting

[98] Supra note 84 at 649.
[99] Supra note 84 at 649.
[100] Supra note 84 at 649.
[101] Supra note 84 at 649.
[102] Supra note 86.
[103] Schwikkard and Van der Merwe op cit note 35 at 199.
[104] Supra note 86 at 523.
[105] Supra note 86 at 525-31.
[106] Supra note 86 at 525.
[107] Supra note 86 at 531. See also *S v Nkabinde* 1998 (8) BCLR 996 (N) where it was held that the accused's right to privacy was violated when law enforcement authorities monitored conversations between the accused and his lawyers.

interests underlying the exclusion of relevant evidence is reflected in the following observation of the court:

> 'There may be those members of the public who will regard the exclusion of the evidence as being evidence of undue leniency towards criminals. The answer to that is that crime in this country cannot be brought under control unless we have an efficient, honest, responsible and respected police force, capable of enforcing the law. One of the mistakes which must be learnt from the past is that illegal methods of investigation are unacceptable and can only bring the administration of justice into disrepute, particularly when they impinge upon the basic human rights which the Constitution seeks to protect.'[108]

On the issue of whether the admissibility of the evidence would have rendered the trial unfair, McCall J distinguished between a confession or admission conscripted against an accused and evidence of an unlawfully monitored telephonic conversation. He found that both types of evidence 'offended the right against self-incrimination' and 'which inevitably "strikes at one of the fundamental tenets of a fair trial".'[109] He concluded that the admission of the evidence of the two telephonic conversations would render the trial unfair:

> 'To admit evidence provided by an accused person against himself without his knowledge as a result of the unlawful monitoring of his conversation with someone else would offend against the notion of basic fairness in no less a measure than the admission of evidence of a confession or admission made by an accused person without having been informed of his right to legal representation, which has been held to result in an unfair trial...'[110]

Two crucial elements of the judgment are worthy of further discussion, the second of which is considered more contentious. First, the court was clearly correct in finding the accused's right to privacy had been infringed as a result of police dishonesty in obtaining the monitoring direction and in its finding that to exclude the evidence on the basis that the admissibility of the impugned evidence would be detrimental to the administration of justice. The police conduct in providing false and misleading information in their application for the direction for the monitoring operation weighed heavily in favour of the exclusion of unconstitutionally obtained evidence.[111] It rendered the accused's trial unfair because it introduced into the process of proof against him evidence obtained by a flagrant and deliberate disregard of rules governing the investigative powers of law enforcement which seek to protect

[108] Supra note 86 at 531.
[109] Supra note 86 at 527.
[110] Supra note 86 at 527.
[111] Supra note 86 at 515.

constitutional rights. The approach of our courts to invoke with vigour the renunciation of such conduct, not merely in principle, but in police practice, is apt.[112]

Second, however, it is not clear that the court was correct in its finding that that there had been an infringement of the right against self-incrimination such that trial fairness would have been affected by the admissibility of the impugned evidence. While there was certainly bad faith and unreasonable conduct of the police, and while my position should not be construed as a sanction of police practice to ignore constitutional rights protections, this is very different from the admission of derivative evidence obtained in circumstances involving some form of compulsion as a result of torture or obtained in the absence of a constitutional rights warning or legal representation, which would be undeniably detrimental to the administration of justice. In the circumstances of the case coupled with considerations of public policy, it is submitted that it is not detrimental to the interests of justice to admit the disputed evidence. The focus of the enquiry perhaps should have been on the nature and extent of the infringement of the accused's constitutional right to privacy, and not on the participation of the accused in certain voluntary inculpatory conversations which took place without knowledge of the unlawful monitoring – potentially, the accused would have participated in the voluntary inculpatory conversations even if there had been no unlawful monitoring.[113]

This distinction between the nature of the rights infringed is important. In relation to privacy rights, invasions of privacy seldom breach the right to a fair trial but evidence obtained as a result of the breach generally falls to be excluded in terms of the second leg of s 35(5) enquiry, namely, detrimental to the administration of justice.[114] An infringement of the right to a fair trial, such as a violation of the right against self-incrimination will inevitably render a trial unfair, however the admissibility status of real evidence obtained as a consequence of conscripted evidence is less clear. As was in the case, *S v Pillay and Others*[115] that followed *Naidoo's* case, and can be considered a sequel, as other persons were later charged on the same facts that led to prosecution of the accused in *Naidoo*.[116] The police, using information improperly obtained, raided accused 10's house and found some of the robbery money concealed in the ceiling, where it had been placed by one of the alleged perpetrators of the

[112] For examples on the extent to which good faith, or the absence thereof, by law enforcement authorities can be considered in the exclusion of unconstitutionally obtained evidence, see also *S v Hena and Another* 2006 (2) SACR 33 SE; *S v Madiba* 1998 1 BCLR 38 (D) and *Mphala's* case supra note 92.
[113] Schwikkard and Van der Merwe op cit note 35 at 250-51.
[114] Email communication Professor PJ Schwikkard, 2 September 2019.
[115] 2004 (2) SACR 479 (N) (SCA).
[116] See Schwikkard and Van der Merwe op cit note 35 at 251.

robbery – this was discovered on the undertaking by the police to accused 10 that she would not be prosecuted and would be used as a State witness in the event that she gave them the information they required. Accused 10 was subsequently convicted in the court a quo as an accessory after the fact to robbery.

The real evidence admitted by the court a quo was the discovery of the money concealed in the roof. On the issue whether the admission of real (or derivative) evidence would render a trial unfair, and having considered in particular Canadian jurisprudence, Mpati DP and Motata AJA held that 'while evidence derived (real or derivative evidence) from conscriptive evidence, ie self-incriminating evidence obtained through a violation of a [constitutional] right, will be excluded on grounds of unfairness if it is found that, but for the conscriptive evidence, the derivative evidence would not have been discovered'[117] – in the present case, that information sourced from the illegal monitoring operation of accused 10's telephone line, which ultimately led to the discovery of the robbery money, was not conscriptive evidence. Scott J said:

> '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. A conversation in such circumstances may result in a form of self-incrimination, but no more so than any other conduct of an accused subsequent to the commission of the offence which may point to the latter's guilt.'[118]

On the second leg of the enquiry, that is whether the impugned evidence should be excluded on grounds that to include it will be detrimental to the administration of justice, the majority judgment in that case, per Mpati DP and Motata AJA, excluded evidence obtained as a result of an illegal monitoring operation. The majority judgment considered that although the admission of the evidence in question, obtained through an unauthorised surveillance operation, would not render the trial unfair, it should be excluded as detrimental to the administration of justice: '[t]here is no doubt that the money found in the ceiling of the house of accused 10 was found as a result of a violation, firstly, of her constitutional right to privacy (s 14 of the Constitution) in that her private communications were illegally monitored following the unlawful tapping of her telephone line, and, secondly, her right to remain silent and her right against self-incrimination (s 35 of the Constitution), in that she was induced to

[117] Supra note 115 at 432.
[118] Supra note 115 at 447.

make the statement that led to the finding of the money in the ceiling of her house.'[119] It was held that even with considerations of public interest, what happened in accused 10's house 'should not be considered in isolation, as if removed from the original violation of accused 10's right to privacy, ie the illegal monitoring of her telephone communications.'[120] The court noted that each case will depend upon its own facts, and while there may well be cases of 'serious infringement of constitutionally guaranteed rights' where the interests of the public would not be served by the exclusion of evidence obtained because of such infringement, the present case was not one of them.[121] It was held that the derivative evidence sought to be admitted should be excluded on the grounds that its inclusion will bring the administration of justice into disrepute. As the evidence of the discovery of the money was the only evidence against accused 10, its exclusion meant there was no evidence upon which she could be convicted. Her appeal accordingly succeeded and conviction and sentence was set aside.

Having regard to the issue of trial fairness and the admissibility of unconstitutionally obtained derivative evidence, it is submitted that our South African courts should not deviate from the well-settled distinction between self-incriminating testimonial communications and incriminating non-testimonial real evidence emanating from the accused. This means that in a situation where real evidence discovered is unconstitutionally obtained as a result of conscripted or self-incriminating evidence, the real evidence should not necessarily be excluded as conscriptive which, if admitted, would render the trial unfair. Scott JA in *Pillay* cautions against automatically excluding derivative real evidence: '[t]o hold that the derivative evidence, ie the discovery of the money in the roof, would render the trial unfair in such circumstances would be to extend the application of the reasoning in the *Burlingham* case simply too far.'[122] He further noted that a 'rigid application' of such an approach 'could lead to some startling results'[123] and 'if adopted as an invariable rule, would be in conflict with the

[119] Supra note 115 at 430.
[120] Supra note 115 at 432-36.
[121] Supra note 115 at 432-36.
[122] Supra note 115 at 447. See reference to *Burlingham* case supra note 85, where evidence of the discovery of the murder weapon at the bottom of a frozen river was excluded on the basis that its discovery resulted from a compelled disclosure made by the accused in circumstances involving a breach of the appellants' right to counsel in terms of the Charter. Further at 447, Scott J held: 'But save in circumstances involving some form of compulsion or, on the strength of *Burlingham's* case, when derived from an infringement giving rise to self-incriminatory evidence which would not otherwise have existed, it is difficult to see how real evidence having an independent existence can ever be said to render the trial unfair.'
[123] Supra note 115 at 446.

decisions of the Constitutional Court'[124] in cases such as *Ferreira*,[125] wherein specifically as regards derivative evidence arising from compelled self-incrimination, Ackermann J said:

> 'As far as s 25(3) is concerned, the trial Judge is obliged to ensure a "fair trial", if necessary by his or her discretion to exclude, in the appropriate case, derivative evidence. Ultimately this is a question of fairness to the accused and is an issue which has to be decided on the facts of each case. The trial Judge is the person best placed to take that decision. The development of the law of evidence in this regard is a matter for the Supreme Court. The essential content of the right is therefore not even touched.'[126]

It should not be the case that the admission of derivative real evidence will automatically rend a trial unfair.[127] Section 35(5) contains a constitutional directive in terms of which exclusion is mandatory 'if the admission of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice.'[128] If admission of the evidence would not render the trial unfair then the court must determine whether it would otherwise be detrimental to the administration of justice. Whether the admission of evidence will bring the administration of justice into disrepute requires a value judgment, which necessarily involves considerations of public interests.[129] There are certainly situations where the admissibility of unconstitutionally obtained real or derivative evidence will be a focus of the fair trial requirement enquiry in s 35(5), especially if it is 'inextricably tainted'[130] by 'torture, assault, beatings and other forms of coercion.'[131] In situations, however, where the real or derivative evidence is not tainted by police brutality or any other form of coerced conduct that procured its discovery by violating the accused's fair trial right at its core,[132] the court must exercise its discretion in terms of s 35(5) and in doing so, the 'fruits of the poisonous tree' doctrine should not be invoked to the extreme.

---

[124] Supra note 115 at 447.
[125] Supra note 47.
[126] Supra note 125 para 153, in the context of the interim Constitution.
[127] See Schwikkard and Van der Merwe op cit note 35 at 259.
[128] Ibid at 256.
[129] *Pillay's* case supra note 115 at 433.
[130] *Tandwa's* case supra note 84 at 641.
[131] Supra note 84 at 649. See also *Ferreira's* case supra note 47 para 150 in which Ackermann J observed: 'Where, for example, derivative evidence is obtained as a result of torture there might be compelling reasons of public policy for holding such evidence to be inadmissible even if it can be proved independently of the accused. Otherwise, the ends might be allowed to justify the means. The admission of evidence in such circumstances could easily bring the administration of justice into disrepute and undermine the sanctity of the constitutional right which has been trampled upon.'
[132] *Tandwa's* case supra note 84 at 649.

(b) The impact of new technologies

A central theme of the analysis presented in the thesis is the impact of modern fast-paced environment of technological advancements, and its effect on the traditional investigative powers of law enforcement and security and intelligence agencies. It is within this context that I offer a doctrinal argument for a particular application of the right against self-incrimination to compelled acts of decryption. Although I have no particular terminology coined for this doctrinal argument as it may apply in South African law, Kerr usefully refers to this as 'equilibrium-adjustment'.[133] Some courts have indicated a willingness to reconsider traditional constitutional law doctrines given the impact of new technologies.[134] In a judgment of the Supreme Court of the United States, in *Carpenter v United States*,[135] the Supreme Court indicated that changes in technology have necessitated an approach to traditional doctrinal principles, more nuanced than a 'mechanical interpretation'.[136] The Court recognised the necessary use of modern technology and its unique challenges to the law, especially in the shift in the balance between state in its use of investigative powers and its impact on individual rights: 'the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort the Framers…drafted the Fourth Amendment to prevent.'[137] The Court referred to 'seismic shifts in digital technology' that gave the state so much power that it upset traditional expectations of use of such powers, and which threatened abuses.[138] The Court further wrote: '[w]hen confronting new concerns wrought by digital technology, it becomes important 'not to uncritically extend existing precedents.'[139] Can these arguments by the Supreme Court, decided in the context of search and seizure laws in relation to electronic data,[140] apply to the right against self-incrimination and compelled disclosure cases? I think so.

---

[133] Kerr op cit note 3 at 791: 'New technologies constantly threaten the balance of power. To ensure that mechanical application of old rules does not create a dystopia in which new technologies either give the government too much powers (which could lead to abuses) or too little power (which would not protect the public), the Court often adjusts old rules to restore the prior equilibrium of government power.' See also OS Kerr 'An equilibrium-adjustment theory of the Fourth Amendment'125 (2011) *Harvard LR* 476 at 488, in which he wrote: 'The resulting judicial decisions resemble the work of drivers trying to maintain constant speed over mountainous terrain. In an effort to maintain the pre-existing equilibrium, they add extra gas when facing an uphill climb and ease of the pedal on the downslopes.'

[134] Kerr op cit note 3 at 790.

[135] 138 S Ct 2206 (2018).

[136] Supra op cit note 135.

[137] Supra op cit note 135 at 2223.

[138] Supra op cit note 135 at 2219.

[139] Supra op cit note 135 at 2222.

[140] I do not wish to belabour the point, suffice to acknowledge the different spheres of investigatory powers. Investigations in the information age now mean more overlaps between these two types of powers, and implications for state access to electronic data. The United States Supreme Court has long ago recognised in

(c) Different scenarios of compelled acts relating to encrypted devices

Applying the constitutional law framework on the right against self-incrimination, two distinct issues arise with regard to compelled disclosure and encryption that is now commonplace in modern life: (i) compelled disclosure of a user's passcode (reveal/enter the passcode); and (ii) compelled entry of a biometric based information (by placing a finger on a device or by facial recognition). A nuanced understanding of the interaction between modern technology and legal doctrine will be integral in the development of doctrinal principles that involve 'reveal-the-passcode', 'use-a-fingerprint-or-facial-recognition', enter-the-passcode' and 'produce-the-decrypted-data'.[141] Each of these actions of compelled decryption aims ultimately to allow the state to access encrypted devices, or to have such encrypted information put in an intelligible form. For example, each time a user of a smartphone device enters a password or passcode to 'unlock' a phone, in doing so, the act decrypts the contents of the smartphone, or at the very least makes them available to be decrypted.[142] Further, once the smartphone is unlocked, it also decrypts all its applications (unless individually password protected) and storage memory such that messages, documents, photos and other files and records on the device can be accessed.[143]

It is recognised that not all cases will neatly fit into these two categories of issues and other scenarios exist.[144] However, they constitute a useful starting point in South African law for a theoretical foundation for the understanding of compelled decryption, and useful for making sense of past cases and for reasoning about future cases and the laws' adaptability to future technological developments.[145] In the analysis, this chapter also highlights some challenges to applying doctrinal principles established in the traditional physical world to electronic devices and information in acts of compelled decryption.

Schmerber's case supra note 37 at 767 that: '[t]he values protected by the Fourth Amendment... substantially overlap [with] those ... [that] the Fifth Amendment helps to protect.' See D Terzian 'Forced decryption as equilibrium – Why it's constitutional and how *Riley* matters' (2014-2015) 109 *Northwestern University LR Online* 56 at 60, who argues that the right against self-incrimination should be included in the 'equilibrium adjustment'. See also Kerr op cit note 3 at 792-794 in which he considers arguments that the right against self-incrimination is 'properly sensitive to the new technological implications' in doctrinal development.

[141] See A Cohen & S Park 'Compelled decryption and the Fifth Amendment: Exploring the technical boundaries' (2018) 32.1 *Harvard Journal of Law & Technology* 170; L Sacharoff 'What am I really saying when I open my smartphone? A response to Orin S. Kerr' (2019) 97 *Texas LR* 63; J Kiok 'Missing the metaphor: Compulsory decryption and the Fifth Amendment' (2015) 24.53 *Public Interest LJ* 53. Kerr op cit note 3; Kerr and Schneider op cit note 1.

[142] See also L Sacharoff 'Unlocking the Fifth Amendment: Passwords and Encrypted Devices' (2018) 87 *Fordham LR* 203 at 221.

[143] Ibid.

[144] For example, compelling a suspect/target to hand over a document in which the password or passcode has been written down.

[145] See Cohen and Park op cit note 141 at 196.

(i) Compelled disclosure of a user's passcode (reveal/enter)

The following analysis is on the constitutional implications of compelling a suspect/target of an investigation to decrypt a digital device, for example by revealing or entering a passcode or password to unlock and have access to the contents of the device.[146] The South African courts have held that certain compelled acts, characterised as non-testimonial, though incriminating, are not within the protections of the right against self-incrimination.[147] It is in this context that the question arises whether the state can force a person to enter the password, which decrypts their phone.[148]

From a doctrinal perspective, for the right against self-incrimination to apply: the evidence sought must be (a) compelled by the state (b) it must be incriminating, and (c) it must be testimonial. Potentially, the first two requirements are easily satisfied in terms of RICA 2002 when a designate judge orders a suspect/target of an investigation to enter a passcode to decrypt a locked device that may likely contain evidence incriminating against the suspect/target., The question that remains: are passcodes 'testimonial'? Understanding the meaning of 'testimonial' is key to understanding, within this context, the right against self-incrimination. International jurisprudence, particularly from the United States of America, offers some insight on the issue, albeit one in which courts have not yet come to a consensus on whether compelled passcodes are 'testimonial'. The Fifth Amendment to the United States Constitution provides, in the relevant part, that '[n]o person … shall be compelled in any criminal case to be a witness against himself.'

In one type of scenario, law enforcement and the security and intelligence agencies may require a suspect/target of a compelled decryption direction to verbally state the password or passcode, or write it down. Arguably, these methods of compelling a password or passcode directly involve testimony 'in its purest form' and therefore should trigger direct protections of the right against self-incrimination.[149] These types of compelled verbal statements of facts will usually be considered testimonial, and it is likely that the scenario of a suspect/target being compelled to verbally state the password or passcode will be no exception.[150] The Supreme

[146] Supra note 152 para 259 at 209-10.
[147] See earlier at 133-39.
[148] See D Terzian 'The micro-hornbook on the Fifth Amendment and encryption' (2015-2016) 104 *Geo LJ Online* 168 at 170.
[149] Sacharoff op cit note 142 at 223.
[150] *Pennsylvania v Muniz* 496 U.S. 582, 589 (1990); *United States v Kirschner* 823 F. Supp. 2d 665, 669 (ED Mich 2010). See also *Doe II* supra note 14.

Court has held that in such instances 'the vast majority of verbal statements thus will be testimonial' because they likely 'convey information or assert facts.'[151]

I now consider a type of scenario central to the debate on whether the compelled act is 'testimonial': a compelled decryption direction requiring a suspect/target of an investigation to enter the password or passcode into the device to enable law enforcement and the security and intelligence agencies to access the encrypted device and its contents. In this scenario, the device itself unlocks when the password or passcode is entered, without keeping a record of it, nor is the entering of the password or passcode observed by anyone. Having regard to the provisions of RICA 2002, if a designated judge approves an application for a decryption direction for a suspect/target of an investigation to enter passcode or password to decrypt a locked mobile phone, computer or an electronic file, does such decryption direction infringe the right against self-incrimination? Put differently, is the compelled act of entering a password or passcode to a device 'testimonial' and therefore subject to protection against self-incrimination?

In the last decade, the American courts have not been able to agree on an answer offering a range of standards for how the right against self-incrimination should apply in such compelled decryption cases. According to *Doe v United States (Doe I)*[152] in order to be "testimonial" an accused's communication, or act, 'must itself, explicitly or implicitly, relate a factual assertion or disclose information.'[153]

It has also become common in the formulation of 'testimonial' in compelled decryption cases to refer to the contents of the mind, with the use of analogy and metaphor. In Justice Stevens' dissent in *Doe I*, he stated: 'A defendant can be compelled to produce material evidence that is incriminating … But can he be compelled to *use his mind* to assist the prosecution in convicting him of a crime? I think not. He may in some cases be forced to *surrender a key to a strongbox* containing incriminating documents, but I do not believe that he can be compelled to reveal the *combination to his wall safe* – by word or deed.'[154] Similarly, the Eleventh Circuit wrote: '[t]he touchstone of whether an act of production is testimonial is whether the government compels the individual to *use "the contents of his own mind"* to explicitly or implicitly communicate some statement of fact.'[155] The Supreme Court in *United*

[151] Supra note 150 at 597.
[152] 487 U.S. 201 (1988) at 210. See also *Ferreira's* case supra note 47 para 259 where it was observed that 'the more that self-incrimination takes the form of oral communication, the more compelling will the protection be.'
[153] Supra note 152 at 209-10.
[154] Supra note 152 at 219 (emphasis added).
[155] *Doe II* supra note 14 at 1345 quoting *Curcio v United States* 354 U.S. 118 (1957) at 128 (emphasis added). At 1342: 'What is at issue is whether the *act of production* may have some testimonial quality sufficient to

States v Hubbell stated: '[i]t was un- questionably necessary for respondent to make extensive *use of "the contents of his own mind"* in identifying the hundreds of documents responsive to the requests in the subpoena.'[156] In another definition of 'testimonial' offered, somewhere in-between 'disclos[ing] information' and 'us[ing] his mind to assist' used in *Doe I*, is the 'extortion of information from the accused'[157] that attempts to force him 'to disclose the contents of his own mind'[158] and that the right against self-incrimination 'protects against *any disclosures* that the witness reasonably believes could be used in a criminal prosecution or could lead to other evidence that might be so used.'[159]

This line of reasoning as to whether the evidence is 'testimonial' turns on whether the state is forcing a suspect/target in the act of compelled decryption to 'disclose the contents of his own mind.'[160] If this is applied, the extent to which a suspect/target is forced to 'use his mind' is central to determining whether an act of production of the passcode is testimonial[161] and the use of the contents of the mind of the suspect/target would be sufficient to make the act of compelled disclosure of a passcode 'testimonial.'[162] A competing interpretation is that

---

trigger Fifth Amendment protection when the production explicitly or implicitly conveys some statement of fact.' (emphasis in original).

[156] *United States v Hubbell* 530 U.S. 27 (2000) at 43 quoting *Curcio's* case supra note 155 at 128 (emphasis added).

[157] *Couch v United States* 409 U.S. 322 (1973) at 328. See also *Saunders v United Kingdom* (1997) 23 EHRR 313 where the European Court of Human Rights wrote (para 68): '[t]he right not to incriminate oneself … does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence *independent of the will* of the suspect.' In *R v S(F) and A(S)* [2009] 1 Cr App R 18 (CA Crim Div) para 19, the court acknowledged that compelled disclosure of a user's passcode is 'not susceptible of quite such rigid compartmentalisation' between 'independent of the will of the suspect' and 'coercion and compulsion.' In its analysis, the court positioned the disclosure of a user's passcode 'which provides access to protected data, like the data itself, [it] *exists separately from each defendant's will*' (paras 20-21).

[158] *Curcio's* case supra note 155 at 128.

[159] *Kastigar v United States*, 406 U.S. 441 (1972) at 445 (emphasis added).

[160] Courts considering the question have focused on whether the act revealed the contents of the mind and have often cited cases determining whether a court may compel a suspect/target to decrypt a computer to unlock it for the government. See *Doe II* supra note 14 at 1346 where it was held that compelled decryption of a computer hard drive's contents was testimonial because using a decryption password demands 'the use of the contents of the mind.' See also *Kirschner's* case supra note 150 at 668–69 held that compelling the suspect to provide passwords associated with the suspect's computer was testimonial because the act revealed the contents of the suspect's mind; *Gelfgatt's* case supra note 14 at 615–16 concluded that the act of computer decryption was testimonial because a defendant cannot be compelled to reveal the contents of his mind, but holding that the testimony was not protected because the testimony was a 'foregone conclusion'; *Securities & Exchange Comm'n v Huang* No. 15-269, 2015 WL 5611644 at 2 (E.D. Penn. Sept. 23, 2015) held that the privilege protected the production of a password because the government sought the "Defendants' personal thought processes" and intruded "into the knowledge" of the defendants.

[161] Cohen and Park op cit note 141 at 215. See also Kerr and Schneider op cit note 1 at 1002.

[162] Ibid. For case law that compelling a passcode is testimonial: *Doe II* supra note 14; *Seo's case* supra note 14; *Kirschner's* case supra note 150; *GAQL v State* 257 So.3d 1058 (Fla. Dist. Ct. App. Oct. 24, 2018); *Huang's* case supra note 160.

the use of the contents of the mind of the suspect/target is not in itself sufficient,[163] and there must be in addition an explicit or implicit communication of a statement of fact.[164]

This leads to the question of whether the state can compel a suspect/target of an investigation to disclose a password or passcode to decrypt a device, or computer or file, if such act is considered 'mentally taxing.'[165] Referring to Justice Stevens' dissent in *Doe I* on the first interpretation above, the state could not compel disclosure of a passcode because the suspect/target would be '*us[ing] his mind* to assist the prosecution in convicting him of a crime'[166] regardless of what other information is known by the state. Potentially, this means that even if the compelled act of decryption does not communicate anything testimonial, and is simply a physical act, the act itself would require the 'extensive use of the mind' of the suspect/target.[167] In *United States v Kirschner*,[168] the defendant was required 'to provide all passwords used or associated with the … computer … and any files.' [169] The court found that requiring Kirschner to provide his password would be testimonial since 'the government is not seeking documents or objects' but rather 'seeking testimony … requiring [Kirschner] to divulge through his mental processes his password – that will be used to incriminate him.'[170] The court's reasoning relied on the analogy of a password decrypting a computer to a combination unlocking a safe, citing Justice Stevens' dissent in *Doe I*, which stated that a defendant may be 'forced to surrender a key to a strongbox' but not 'to reveal the combination to his wall safe — by word or deed.'[171] Similarly, in *In re Grand Jury Subpoena to Sebastien Boucher (Boucher I)*:[172] [s]ince the government is trying to compel the production of the password itself, the foregone conclusion doctrine cannot apply. The password is not a physical thing … It is pure testimonial production rather than physical evidence having testimonial aspects.'[173]

---

[163] Cohen and Park op cit note 141 at 216.
[164] *Doe II* supra note 14 at 1345 quoting *Curcio's* case supra note 155 at 128.
[165] Cohen and Park op cit note 141 at 217. See also Kerr and Schneider op cit note 1 at 1002.
[166] Supra note 152 at 219.
[167] Cohen and Park op cit note 141 at 217.
[168] Supra note 150 .
[169] Supra note 150 at 666.
[170] Supra note 150 at 669.
[171] Supra note 168 at 669.
[172] 2007 WL 4246473 (Nov. 29, 2009).
[173] Supra note 172 at 6, reversed on other grounds by *In re Grand Jury Subpoena to Sebastien Boucher (Boucher II)* 2009 WL 424718 (D. Vt. 2009). See also *Commonwealth v Baust* 89 Va. Cir. 267, 271 (2014): [u]nlike a document or tangible thing, such as an unencrypted copy of the footage itself, if the password was a foregone conclusion, the Commonwealth would not need to compel Defendant to produce it because they would already know it.' See also *Huang's* case supra note 160 at 2: '[h]ere, the SEC seeks to compel production of the passcodes which require intrusion into the knowledge of Defendants and no one else.'

The court in *Fisher v United States*[174] created a two-part doctrinal framework as regards compelled acts: (i) the act-of-production doctrine; and (ii) the foregone conclusion doctrine. The court held that the Fifth Amendment does not afford protection to the compelled production of the *contents of papers*, and at the same time it announced an exception: depending on the circumstances of particular cases, a compelled act is testimonial when the *act of producing* the evidence implies 'tacit averments' that 'has communicative aspects.'[175] *Fischer* provides an often cited statement and example: 'The act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced. Compliance with the subpoena [for a taxpayer's financial records] tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena.'[176] In other words, the 'testimonial' act protected by the Fifth Amendment is not the content of papers, but the physical act itself of producing the evidence: '[i]n light of the records now before us, we are confident that however incriminating the contents of the accountant's workpapers might be, *the act of producing them*—the only thing which the taxpayer is compelled to do—would not itself involve testimonial self-incrimination.'[177] In doing so, the court referred to three aspects of testimonial statements implicit in the act of compelled production: (i) 'existence'; (ii) 'possession or control'; and (iii) authenticity by 'the belief that the papers are those' required by the act of compulsion.[178] A concern that arises with the court's formulation is the sheer breadth, such that potentially *every* act of compulsion will be testimonial as it will communicate statements implicit in the act concerning 'existence', 'possession or control' and authenticity.[179] Possibly with this concern in mind, the court imposed two limitations.[180] The first refers to the act of compulsion to be 'deemed to be sufficiently testimonial.' Although the court did not provide any direction as to how it would determine if a compelled act is 'sufficiently testimonial'.[181] The second limitation brings us to the other part of *Fisher's* doctrinal framework: the testimonial aspects of a compelled act should not be considered 'testimonial' when the 'existence and location' of the documents is a

[174] *Fisher v United States* 425 U.S. 391 (1976).
[175] Supra note 174 at 410.
[176] Supra note 174 at 410.
[177] Supra note 174 at 410-11.
[178] Supra note 174 at 410-11. See also Cohen and Park op cit note 141 at 181-82; Sacharoff op cit note 142 at 217 and Kerr op cit note 3 at 772-73.
[179] Sacharoff op cit note 142 at 218.
[180] Ibid.
[181] Ibid.

'foregone conclusion.'[182] This meant that because the tax authority already knew the existence and location of the documents, the taxpayers disclosure on compulsion would not implicitly relay an incriminating fact to the government:

> 'It is doubtful that implicitly admitting the existence and possession of the papers rises to the level of testimony within the protection of the Fifth Amendment. The papers belong to the accountant, were prepared by him, and are the kind usually prepared by an accountant working on the tax returns of his client. Surely the Government is in no way relying on the "truthtelling" of the taxpayer to prove the existence of or his access to the documents. Wigmore § 2264, p. 380. The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers. Under these circumstances by enforcement of the summons "no constitutional rights are touched. The question is not of testimony but of surrender." *In re Harris*, 221 U.S. 274, 279 (1911).'[183]

The exception-to-the-exception formulation as expounded in *Fisher* – the state could compel decryption if the testimonial communication is regarded as a foregone conclusion.[184] The foregone conclusion doctrine is an application of the right against self-incrimination 'by which the Government can show that no testimony is at issue.'[185] Specifically, '[w]hen the 'existence and location' of the documents under subpoena are a "foregone conclusion" and the witness "adds little or nothing to the sum total of the Government's information by conceding that he in fact has the [documents]," then no Fifth Amendment right is touched because the "question is not of testimony but of surrender".'[186] Therefore, the act of entering a password or passcode to decrypt a device may be compelled by the state if the testimonial communication implicit in the physical act of doing so is a foregone conclusion.[187]

Another often referred case in which the testimonial aspects of compelled acts of production was considered and deemed to merit Fifth Amendment protections is *United States*

---

[182] Supra note 174 at 411.
[183] Supra note 174 at 411.
[184] *Doe II* supra note 14.
[185] Supra note 14 at 1344.
[186] *In re Grand Jury Subpoena Dated Apr. 18, 2003*, 383 F.3d 905, 910 (9th Cir. 2004) quoting *Fisher's* case supra note 174.
[187] *Doe II* supra note 14 at 1344: 'If in the case at hand, for example, the Government could prove that it had knowledge of the files encrypted on Doe's hard drives, that Doe possessed the files, and that they were authentic, it could compel Doe to produce the contents of the files even though it had no independent source from which it could obtain the files.' For case law where passcode is testimonial, but the foregone conclusion applies as an exception: *Commonwealth v Jones*, 481 Mass. 540 (2019); *Spencer's* case supra note 14; *Baust's* case supra note 173; *Fricosu's* case supra note 14; *Stahl's* case supra note 14; *Apple MacPro Computer's* case supra note 14.

v Hubbell.[188] This case of various tax-related and fraud charges, including the investigation of possible violations of federal law, resulted in the compelled production of 13,120 pages of documents following a subpoena requesting eleven categories of documents. The court ruled that the act of production was testimonial because the 'breadth of the description' of the requested documents made their 'collection and production … tantamount to answering a series of interrogatories asking a witness to disclose the existence and location of particular documents fitting certain broad descriptions.'[189] On the foregone conclusion aspect of the *Fisher* test, the court held that the facts in this case 'plainly [fell] outside of' the scope of the "foregone conclusion" rationale.'[190] In *Fisher*, the government 'knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity' whereas in this case, the government failed to demonstrate any 'prior knowledge of either the existence or the whereabouts of the … documents ultimately produced by the respondent.'[191] In view of the testimonial aspects of the defendant's act of compelled production, with the very broad nature of the subpoena, specifically, that the government acknowledged that it could not satisfy the 'reasonable particularity' standard prescribed,[192] it was held that the Fifth Amendment protections applied in this case.[193]

After *Hubbell* and *Fisher*, determining whether an act of production is testimonial appears to depend largely on 'the government's knowledge regarding the documents before they are produced.'[194] The court in *Hubbell* noted that the government need not 'have actual knowledge of the existence of each and every responsive document.'[195] The majority of circuit courts have held, however, that the government must establish its knowledge of the three aspects of testimonial statements implicit in the act of compelled production, that is, (i) existence, (ii) possession, and (iii) authenticity of the requested documents with "reasonable particularity.'[196] The Ninth Circuit has noted [i]t is the government's knowledge of the

[188] Supra note 156.
[189] Supra note 156 at 41.
[190] Supra note 156 at 44.
[191] Supra note 156 at 44-45.
[192] Supra note 156 at 30.
[193] Supra note 156 at 46.
[194] *United States v Ponds* 454 F.3d 313, 320 (D.C. Cir. 2006).
[195] Supra note 156 at 44-45.
[196] *Ponds'* case supra note 194; *In re Grand Jury Subpoena* supra note 186 at 910; *In re Grand Jury Subpoena Duces Tecum* 1 F.3d 87 (2d Cir. 1993). See also In *re Grand Jury Subpoena to Sebastian Boucher* 2009 WL 424718 (D. Vt. February 19, 2009); *Spencer's* case supra note 14; *Stahl's* case supra note 14; *Gelfgatt's* case supra note 14; Doe *II* supra note 14; *Apple MacPro Computer's* case supra note 14.

existence and possession of the *actual documents*' and 'not the information contained therein, that is central to the foregone conclusion inquiry.'[197]

Aside from the question of whether the doctrine of the foregone conclusion in *Fisher* is jurisprudentially sound, is it possible for its principles to be applied consistently in compelled decryption cases? [198] Yes, potentially so. Although the foregone conclusion exception originated in the context of the compelled production of documents in response to a government subpoena, the courts have since extended its application and underlying principles to acts of compelled production of passwords to encrypted electronic devices. However, ongoing legal debate on the matter is not in agreement with the 'correct way' to interpret *Fisher* and its application to compelled decryption and as to how these cases should be decided.[199] Two alternative doctrines have been proposed by (i) Kerr, a password based rule, and (ii) Sacharoff, a content based rule. Kerr argues that 'a simple rule should apply', that is, the right against self-incrimination '*poses no barrier to compelled decryption as long as the government has independent knowledge that the suspect knows the password and the government presents the password prompt to decrypt the device to the suspect*. When a suspect is presented with a password prompt and is ordered to enter the password, *the only implied testimony is that the suspect knows the password*. That testimony will be a foregone conclusion that defeats the assertion of the privilege when the government can independently show that the person already knows the password.'[200] Sacharoff offers a counter argument: 'The rule should not be, as Kerr argues, whether the government can show the suspect knows the password to the device. *Rather, the rule should be whether the government already knows the person possesses the files on the device and can identify them with reasonable particularity*. This rule, after all, is precisely what the case law requires in an ordinary document production situation.' [201] Sacharoff 'proposes a rule of particularity: when law enforcement agents have a warrant to search a locked, encrypted device, they can compel the suspect to enter her password to decrypt only those files that agents (1) know she possess, and (2) can describe with reasonable particularity.'[202] Under this doctrine, the 'government knows the suspect possess a particular document that it can describe with reasonable particularity then the suspect's act of production

[197] *In re Grand Jury Subpoena* supra note 186 at 910.
[198] Cohen and Park op cit note 141 at 219.
[199] Cohen and Park op cit note 141 at 219. Sacharoff op cit note 142 at 207 explains this is 'is a fundamental question bedevilling courts and scholars.'
[200] Kerr op cit note 3 at 769-70 (emphasis added). At 778: [t]his standard allow the government to compel a suspect to enter a password in many cases but not all cases.'
[201] Sacharoff op cit note 141 at 63-64 (emphasis added).
[202] Sacharoff op cit note 142 at 251.

adds little to the government's overall knowledge. That production, therefore, would not count as testimonial.'[203]

Which of these opposing, alternative, doctrines should apply depends on whether the foregone conclusion doctrine applies to the *device* and knowledge of password when presented with a password prompt to decrypt the device (i.e. device only at password prompt), or to the *contents* of the device. This debate has further widened the split among the courts in the United States of America on what test to apply to compelled decryption cases. It appears increasingly likely that the Supreme Court will address the question.

In my view, if the court treats the device only at password prompt as the relevant scope of inquiry, that is, whether the government can independently establish that the suspect/target of the compelled decryption direction knows the password to the device – the standard may not be a difficult endeavour for the government to satisfy in many cases, especially with personal devices such as a smartphone where this is found on the suspect/target. Recently, the Massachusetts Supreme Judicial Court agreed with Kerr's password-based rule and adopted this standard. In *Commonwealth v Jones*,[204] the central legal issue concerned whether compelling the defendant to enter the password to the smartphone would violate his right against self-incrimination. The court held that when the government seeks an order compelling a suspect/target to decrypt an electronic device by entering a password, it requires the government to prove that the suspect/target knows the password beyond a reasonable doubt for the foregone conclusion exception to apply:[205]

> 'Accordingly, for the foregone conclusion exception to apply, the Commonwealth must establish that it already knows the testimony that is implicit in the act of the required production. Id. at 522-523. In the context of compelled decryption, the only fact conveyed by compelling a defendant to enter the password to an encrypted electronic device is that the defendant knows the password, and can therefore access the device. See id. See also Kerr, Compelled Decryption and the Privilege Against Self-incrimination, Tex. L. Rev. (forthcoming 2019) (manuscript at 18) ("the only assertion implied by entering the password is that the person compelled knows the password"). The Commonwealth must therefore establish that a defendant knows the password to decrypt an electronic device before his or her knowledge of the password can be

[203] Ibid at 218-19.
[204] SJC-12564 (Mass. Mar. 6, 2019).
[205] Supra note 204 at 4.

deemed a foregone conclusion under the Fifth Amendment or art. 12 [art. 12 provides that "[n]o subject shall . . . be compelled to accuse, or furnish evidence against himself"].'[206]

This means that before a suspect/target can be compelled to decrypt a device by entering a password, all that the government must demonstrate is that the suspect/target knows the password or passcode. The court's decision has been described as 'the death knell for a constitutional protection against self-incrimination in the digital age.'[207] Lenk J writing a separate concurring judgment of the court argues so because 'unlike the court' he 'thinks that compelled decryption of a cellular telephone or comparable device implicates more than just a passcode; what the government seeks is access to the files on the device, which the government believes will aid in inculpating the defendant.'[208] His application of the foregone conclusion extends the scope of inquiry beyond the device only at password prompt:

> 'Given that the foregone conclusion doctrine is a narrow exception to the constitutional privilege against self-incrimination, the government may compel a defendant's decryption of such a device only when it can show that any testimonial aspect involved in that act of production is already known to the government. In other words, the government must demonstrate, beyond a reasonable doubt, that the accused knows the passcode to the device *and* that the government already knows, with reasonable particularity, the existence and location of relevant, incriminating evidence it expects to find on that device. Because here the government met these requirements, I concur in the result. I also agree with the court that the appropriate standard of proof is beyond a reasonable doubt.'[209]

If a court were to treat the content contained on the device as the relevant scope of inquiry, the government would have to show that it knows the location, existence and authenticity of the purported evidence with reasonable particularity. While the courts do not demand that the government identify exactly the documents it requires, it does require some specificity in its requests to prevent a 'quintessential fishing expedition'.[210] In *In re Grand Jury Subpoena (Doe II)*,[211] the Eleventh Circuit rejected the government's access to files stored on

---

[206] Supra note 204 at 13-14 (footnotes omitted).
[207] Supra note 204 at 1-9 at 9, Lenk J concurring judgment.
[208] Supra note 204 at 1-9 at 1, Lenk J concurring judgment.
[209] Supra note 204 at 1-9 at 1, Lenk J concurring judgment.
[210] *Hubbell's* case supra note 156 at 42. See also *Matter of the Decryption of a Seized Data Storage Systems* U.S. Dist. Ct. No. 13-M-449 (E.D. Wis. Apr. 19, 2013 where it was held that government must demonstrate its 'knowledge of the existence, possession, and authenticity of the files on the encrypted storage devices with reasonable particularity'; *Fricosu's* case supra note 14 at 1237 it was held that the Fifth Amendment was not implicated by requiring production of unencrypted contents of computer 'where government kn[ew] of existence and location of the computer's files' although not specific content of documents, and knew of defendant's custody and control of device.'
[211] Supra note 14.

an encrypted hard drive as 'the Government has failed to show any basis, let alone shown a basis with reasonable particularity, for its belief that encrypted files exist on the drives, that [the defendant] has access to those files, or that he is capable of decrypting the files.'[212] Will it be enough for the government to demonstrate location and existence of the files it requires by the knowledge that devices such as smartphone are capable of holding such content? Probably not. This argument was rejected in *Hubbell*: '[t]he Government cannot cure this [lack of prior knowledge] deficiency through the overbroad argument that a *businessman such as respondent will always possess general business and tax records* that fall within the broad categories described in this subpoena.'[213] Therefore, on the basis of case law from the United States Supreme Court 'the Government [need not] identify exactly the documents it seeks, but it does require some specificity in its requests—categorical requests for documents the Government anticipates are likely to exist simply will not suffice.'[214]

Central to Kerr's argument on the password-based rule that the only testimony implicit in the unlocking of the device by entering the password or passcode is the 'assertion that the person knows that password.'[215] While this may be true, Lenk J[216] and Sacharoff[217] counter argue that the act of compulsion by entering a password or passcode implicates more than just that fact of knowledge of the password or passcode. The central question in their argument is: 'what message does a person implicitly communicate in entering a password to open a device?'[218] For one, it communicates that the person entering the password or passcode to unlock the device likely owns and controls the device and its contents:

> 'The difference in what messages get communicated plays out in determining how the government may satisfy the foregone conclusion doctrine. If the only message communicated is knowledge of the password, then Kerr is right: the government need only show the person knows the password. If, however, the act of opening the device also communicates that the person likely owns the device and the files on it, then the government must show that it already

[212] Supra note 14 at 1349.
[213] *Hubbell's* case supra note 156 at 45 (emphasis added).
[214] *Doe II* supra note 14 at 1347. The Eleventh Circuit held further: '[i]t is not enough for the Government to argue that the encrypted drives are *capable* of storing vast amounts of data, some of which *may* be incriminating. In short, the Government physically possesses the media devices, but it does not know what, if anything, is held on the encrypted drives. Along the same lines, we are not persuaded by the suggestion that simply because the devices were encrypted necessarily means that [the defendant] was trying to hide something. Just as a vault is capable of storing mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all' (emphasis in original).
[215] Kerr op cit note 3 at 779-785.
[216] *Commonwealth v Jones* supra note 204 at 1-9 at 1, Lenk J concurring judgment.
[217] Sacharoff op cit note 141 at 67.
[218] Ibid at 67-68

knows of and can identify with reasonable particularity the actual files it seeks, or at least a class of files such as bank records for a particular account—a higher burden.' [219]

Whether the inquiry can be limited to the question of whether suspect/target's knowledge of the password itself is sufficient to support an application of the foregone conclusion doctrine, Lenk J in his judgment argues that the protections of the right against self-incrimination 'demands even more'.[220] With reference to the doctrinal principle that although the government is not required to name every document it requires or what its contents contain, it must demonstrate, with reasonable particularity, the existence and location of some incriminating files it expects to find on the device – a departure from this constitutional doctrine states Lenk J is 'imprudent, particularly in light of the vast amount of potentially incriminating information at risk.'[221] Doing so otherwise will permit a 'quintessential fishing expedition'[222] by the government 'by ordering an individual to enter a passcode and to provide the government with unlimited, unencrypted access to a personal electronic device is precisely the sort of act against which the Fifth Amendment was designed to guard.'[223]

(ii) Compelled entry of biometric based information

Among the encryption options available for the user of devices during device setup, particularly smartphones and tablets, is the choice of protecting the device with a biometric feature such as with a fingerprint or facial recognition. Encryption based on the use of biometrics is increasingly common. I have opted for biometric protection on my devices for at least the last eight of my devices, and also for many applications installed on my devices, such as Internet banking.[224] In opting for this type of device setup, or for specific applications, which I regard

[219] Ibid.
[220] *Commonwealth v Jones* supra note 204 at 1-9 at 7, Lenk J concurring judgment.
[221] Supra note 204 at 1-9 at 7-8, Lenk J concurring judgment. See also Sacharoff op cit note 141 at 71: ''[i]n almost all cases, at least with personal devices such as a smartphone, a person's ability to open the phone will be very powerful evidence of *both* facts: that she knows the password and that the device is hers.'
[222] *Hubbell's* case supra note 156 at 42. Further at 37, referred by Lenk J in support, that it was observed that the 'right against self-incrimination, in part, was structured to prevent government from "uncover[ing] uncharged offenses."'
[223] Supra note 204 at 1-9 at 8, Lenk J concurring judgment. See also, In *re of United States District Court Northern District of California* 354 F. Supp. 3d 1010 (N.D. Cal. 2019) at 1017: 'The foregone conclusion doctrine not does not apply when the Government cannot show prior knowledge of the existence or the whereabouts of the documents ultimately produced in response to a subpoena. …Consequently, the Government inherently lacks the requisite prior knowledge of the information and documents that could be obtained via a search of these unknown digital devices, such that it would not be a question of mere surrender.'
[224] Another common option available for users of Android phones is pattern-based protections that require the user to draw a 'pattern on the screen, rather than enter a passcode. See 'Set screen lock on an Android device' available at *https://support.goo gle.com/android/answer/9079129?hl=en*, accessed 8 April 2020.

as the quickest and safest way of accessing my devices and the information contained therein, I have, of course, given little consideration to the potential implications on my legal rights. As it turns out, the legal ramifications of this choice may be significant, in the event that I am presented with a compelled decryption direction.[225]

'Unquestionably' argues Terzian 'the government can force people to produce biometric passwords like fingerprints.'[226] A review of existing precedent in a series of cases on physical characteristics akin to real evidence appears to suggest, strongly, that decryption by use of biometric based information can be compelled with little difficulty. In these cases, as referred to earlier, the state has compelled a suspect/target to perform a physical act that potentially is inculpatory. The compelled act may incriminate, however, the courts have held repeatedly that protections of the right against self-incrimination do not apply. Likewise, the argument goes that the fingerprint is a physical feature of the body, and the act of pressing my finger onto a devices' censor 'does not constitute testimonial evidence'[227] or disclose of the contents of my mind, or rely on my truthfulness as the fingerprint holder. The Minnesota Appeals Court found 'that producing a fingerprint is more like exhibiting the body than producing document' and so held 'that providing a fingerprint to unlock a cellphone is not a testimonial communication' under the right against self-incrimination:[228]

---

[225] See T Cushing 'State appeals court says unlocking a phone with a fingerprint doesn't violate the Fifth Amendment, TECHDIRT (January 2017) available at *https://www.techdirt.com/articles/20170121/08510936531/state-appeals-court-says-unlocking-phone-with-fingerprint-doesnt-violate-fifth-amendment.shtml*, accessed 14 April 2020: 'you might be better off securing your phone with a passcode than your fingerprint. While a fingerprint is definitely unique and (theoretically. . .) a better way to keep thieves and snoopers from breaking into your phone, it's not much help when it comes to your Fifth Amendment protections against self-incrimination.'

[226] Terzian op cit note 148 at 169.

[227] *Huma's* case supra note 39; *Maphumulo's* case supra note 39; *Msomi's* case supra note 39.
An act is *not* testimonial when the act provides 'real or physical evidence' that is 'used solely to measure ... physical properties' (*Dionisio's case* supra note 40 at 7) or to 'exhibit ... physical characteristics' (*Wade's* case supra note 43 at 222). The state can compel a suspect/target to act when the act presents the 'body as evidence when it may be material' (*Schmerber's* case supra note 37 at 763 (quoting *Holt's* case supra note 44)). In other words, the state may compel a suspect/target to 'exhibit himself' and present his 'features' so that it would be possible 'compare his features' with other available evidence of guilt. See also *State v Williams* 307 Minn. 191, 239 N.W.2d 222, 225–26 (1976) holding that an order to 'put on a hat found at the scene of the crime' was not testimonial because the compelled physical act was for 'the sole purpose of attempting to prove [the defendant's] ownership of [an] incriminating article.' The United States Supreme Court has drawn a distinction between the testimonial act of producing documents as evidence and the nontestimonial act of producing the body as evidence. The court first held that the compelled exhibition of the body's characteristics was not testimonial under the Fifth Amendment in *Holt*. The court explained that it would be an 'extravagant extension of the 5th Amendment' to prevent a jury from hearing a witness testify that a prisoner, who was compelled to put on clothes, did so and that the clothes fit him.

[228] *State v Diamond* 905 NW.2d 870 (Minn 2018) at 875. See also *Matter of Residence in Oakland, California*, 354 F. Supp. 3d 1010 (N.D. Cal. 2019).

> 'We reach this conclusion for two reasons. … First, the State compelled Diamond to provide his fingerprint only for the physical, identifying characteristics of Diamond's fingerprint, not any communicative testimony inherent in providing the fingerprint. The State's use of Diamond's fingerprint was therefore like a "test" to gather physical characteristics, akin to a blood sample, a voice exemplar, trying on clothing, or standing in a lineup, in an effort to unlock the cellphone. … Second, Diamond's act of providing a fingerprint to the police was not testimonial because the act did not reveal the contents of Diamond's mind. … Here, Diamond merely provided his fingerprint so that the police could use the physical characteristics of the fingerprint to unlock the cellphone. The compelled act did not require Diamond to "submit to testing in which an effort [was] made to determine his guilt or innocence on the basis of physiological responses, whether willed or not." See *Schmerber* 384 U.S. at 764, 86 S.Ct. 1826'[229]

The court concluded that '[b]ecause the compelled act merely demonstrated Diamond's physical characteristics and did not communicate assertions of fact from Diamond's mind, we hold that Diamond's act of providing a fingerprint to the police to unlock a cellphone was not a testimonial communication protected by the Fifth Amendment.'[230] However, it may not be as straightforward as it seems and modern technology offers the possibilities of modifying biometric based decryption to include some non-biometric, testimonial aspects thereby enhancing protections offered by the right against self-incrimination.[231] This possibility was acknowledged by the court in *Diamond's* case: '[t]o the extent that providing a fingerprint to unlock a cellphone might require a mental process to unlock the phone, the police did not need to rely on that mental process here. … Diamond did not need to self-select the finger that unlocked the phone. He did not even need to be conscious. Diamond could have provided all of his fingerprints to the police by making his hands available to them, and the police could have used each finger to try to unlock the cellphone.'[232] By the compulsion order, Diamond was required to 'provide a fingerprint or thumbprint as deemed necessary by the Chaska Police Department to unlock his seized cell phone.'[233]

[229] Supra note 228 at 875-77. The court also referred to *Baust's* case supra note 173 at 4, that providing a passcode was testimonial, but providing a fingerprint was not, because '[u]nlike the production of physical characteristic evidence, such as a fingerprint, the production of a password force[d] the Defendant to disclose the contents of his own mind.'
[230] Supra note 228 at 878.
[231] Cohen and Park op cit note 141 at 208-09.
[232] Supra note 228 at 877.
[233] Supra note 228 at 872.

What if what was required to unlock the device was not just 'a fingerprint or thumbprint' and required the use of multiple fingers to be placed in a particular order? Would that be considered 'mentally taxing' to the mental level of a password or passcode, and therefore testimonial? It is also a generally acknowledged feature of certain devices, in particular smartphone devices, that there are times when the device will not accept the biometric based feature and require the user to type in the password or passcode to unlock the device. For example, a password or passcode is generally required when a device has been restarted, inactive, or has not been unlocked by the user for a certain period of time, certainly as a security feature to ensure that someone without the passcode cannot readily access the contents of the device.[234] The question that arises: if a user cannot be compelled to provide a passcode because it is a testimonial communication, should it be the case that a user cannot be compelled to provide one's finger, thumb, iris, face, or other biometric feature to unlock that same device as the proposed use of biometric features *is* also testimonial?[235] The United States District Court Northern District of California thought so. In *re of United States District Court Northern District of California*, the court took the view that the use of a biometric feature to unlock an electronic device 'is not akin to submitting to fingerprinting or a DNA swab, because it differs in two fundamental ways':[236]

> 'First, the Government concedes that a finger, thumb, or other biometric feature may be used to unlock a device in lieu of a passcode. In this context, biometric features serve the same purpose of a passcode, which is to secure the owner's content, pragmatically rendering them functionally equivalent. …Second, requiring someone to affix their finger or thumb to a digital device is fundamentally different than requiring a suspect to submit to fingerprinting. A finger or thumb scan used to unlock a device indicates that the device belongs to a particular individual. In other words, the act concedes that the phone was in the possession and control of the suspect, and authenticates ownership or access to the phone and all of its digital contents. Thus, the act of unlocking a phone with a finger or thumb scan far exceeds the "physical evidence" created when a suspect submits to fingerprinting to merely compare his fingerprints to existing physical evidence (another fingerprint) found at a crime scene, because there is no comparison or witness corroboration required to confirm a positive match. Instead, a successful

[234] In *re of United States District Court Northern District of California* supra note 223 at 1015.
[235] Supra note 223 at 1015. See also *Matter of Search of [Redacted] Washington, D.C.*, 317 F. Supp. 3d 523 (D.D.C. 2018).
[236] Supra note 223 at 1015.

finger or thumb scan confirms ownership or control of the device, and, unlike fingerprints, the authentication of its contents cannot be reasonably refuted.'[237]

The court referred to a similar situation in *In re Application for a Search Warrant* where it was observed that '[w]ith a touch of a finger, a suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents.'[238] The Northern District of California also gave preference to an aspect of Brennan J's opinion of the court in *Schmerber's* case where it was noted that the courts have usually held that it offers no protection against compulsion to submit to a blood sample, provide a palm print, or finger prints, or a voice exemplar, submit to an operation, provide a handwriting sample, to stand in a line-up, or to wear a particular set of clothing, walk or make a particular gesture.[239] The distinction which has emerged in law (as also in South African law), albeit expressed in different ways, is that the privilege against self-incrimination protects against compelling 'communications' or 'testimony' but that a suspect/target may be compelled to provide 'real or physical' evidence since the privilege does not apply to real evidence.[240] While the distinction provides 'helpful framework for analysis' Brennan J noted that '[t]here will be many cases in which such a distinction is not readily drawn.'[241] He referred to testing such as lie detector tests 'measuring changes in body function during interrogation' and held: '[t]o compel a person to submit to testing in which an effort will be made to determine his guilt or innocence on the basis of physiological responses, whether willed or not, is to evoke the spirit and history of the Fifth Amendment. Such situations call to mind the principle that the protection of the privilege "is as broad as the mischief against which it seeks to guard".'[242] On this analysis, the Northern District of California concluded: 'a biometric feature is analogous to the nonverbal, physiological responses elicited during a polygraph test, which are used to determine guilt or innocence, and are considered testimonial.'[243]

The proposals suggested by Cohen and Park adds to the analysis that biometric based technology potentially blurs the doctrinal principles in precedent and the established distinction between testimonial (enter/reveal the passcode) and non-testimonial (biometric based). One

[237] Supra note 223 at 1015-16.
[238] 236 F.Supp.3d 1066, 1073 (N.D. Ill. 2017).
[239] Supra note 37 at 764.
[240] Supra note 37 at 764.
[241] Supra note 37 at 764.
[242] Supra note 37 at 764-5, with reference to *Counselman v Hitchcock* 142 U.S. 547, 562.
[243] Supra note 223 at 1016.

such proposal involves the user choosing a 'secret finger' or multiple fingers, to be placed in a particular sequence on the sensor, to enable decryption of the decryption.[244] Is it the case that 'knowledge of which finger or fingers to use' is indistinguishable from 'the contents of the user's mind, even though the fingerprint itself would still be purely physical evidence'?[245] The courts are not in agreement as to whether compelled entry of biometric based information should follow the distinction which has emerged in law that compulsion which makes a suspect/target the source of real evidence, in this instance biometric information, should be regarded as an act that is *not* testimonial that does not violate the privilege against self-incrimination.[246] These are interesting developments to follow and could pose yet more complex challenges for the law if biometric based information is coupled with technology that, for example, erases all data on the device or directs the decryption to 'decoy' content.[247] The main issue for South African law and facing the courts is that technology is outpacing the law as there will be many cases where the rudimentary distinction testimonial and non-testimonial will be challenged by technology. A recognition of this reality of the information age will require an adaption of existing doctrinal principles in the context of the right against self-incrimination.[248]

IV DEVELOPING A SOUTH AFRICA APPROACH

With careful consideration of both technology and precedent, the modern realities of the information age will require a rethinking of the doctrinal principles of the right against self-incrimination to adequately safeguard individual rights having regard to the role of passwords or passcodes in protecting our electronic information, balanced against the use of encryption as an obstacle to legitimate needs of law enforcement and the state and security agencies. Whether this can be applied with some level of consistency by the South African courts remains to be seen. Some key lessons can be drawn from the above analysis. That the doctrine of

[244] Ibid at 209. The other proposals considered include location-based decryption, situation-dependent decryption and voice command recognition.
[245] Ibid.
[246] The court in *Diamond* acknowledged *In re Application for a Search Warrant* 236 F.Supp.3d 1066, 1073–74 (N.D. Ill. 2017) where it was held that the right against self-incrimination barred the compelled production of a fingerprint to unlock a phone because the act produced the contents of the phone. The court responded at 877: '[e]ven if providing a fingerprint *did* reveal the contents of the mind, because the act of providing evidence of physical characteristics has no testimonial significance … Diamond's act would still be nontestimonial.'
[247] Ibid, as noted similar modifications could be applied to passcode based encryption.
[248] The United States Supreme Court has recently instructed courts to adopt rules that 'take account of more sophisticated systems that are already in use or in development.' See *Carpenter* supra note 135 at 2218-19 quoting *Kyllo v United States* 533 US 27, 36, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001).

compelled decryption must take cognisance of the manner of the compelled act sought by the state in addition, of course, to the facts of the particular case. This chapter referred to two scenarios in particular, namely, (i) compelled disclosure of a user's passcode (reveal/enter the passcode); and (ii) compelled entry of a biometric based information (by placing a finger on a device or by facial recognition).

In traditional cases, the jurisprudence of the South African courts has been rather rudimentary on the distinction between self-incriminating testimonial communications and incriminating non-testimonial real evidence. This means that when a physical item or feature, akin to real evidence, is the object of the compelled decryption direction, the almost seemingly natural outcome is to compel decryption.[249] The most obvious illustration is the potential lower protection afforded to the right against self-incrimination available for biometric based encryption such as fingerprints. The opposite applies in cases involving compelled disclosure of a passcode or compelled production of encrypted data. When the state seeks compelled decryption to access a decrypted device, or computer of file, that is already in its possession, the manner in which the suspect/target of a decryption direction is required to furnish that information becomes significant. Much of the complexity, as illustrated by international case law, relates to the nature of 'testimonial' introduced by variations in modern technology.

I believe that the courts in South Africa should be reluctant to interpret the right against self-incrimination to be more demanding in the context of compelled disclosure of a password or passcode. The impact of new technology means that bypassing encryption is a challenge for law enforcement and the security and intelligence agencies, and not simply an opportunity to access personal and private information in the context of compelled entering of a password or passcode.[250] Essentially, they are seeking, through a compelled decryption direction, access to an encrypted device or information to enable a search pursuant to a warrant. They are not seeking compelled decryption because they want testimony, they are seeking compelled decryption because there is no other way to execute what would have been a routine search two decades ago. This is a consequence of the information age, not the evidence they want to access. [251] The information age has now inserted 'powerful password gates.' [252] The technological shift in the widespread use of encryption in the information era, means rather than technology expanding the state's power in ways that call for new rules to avoid an

[249] *Matemba's* case supra note 38.
[250] See Kerr op cit note 3 at 794-5.
[251] Ibid at 795.
[252] Ibid.

Orwellian Big Brother or Bentham's panopticon, encryption now limits the powers of the state to execute otherwise lawful searches.[253] I do not believe that this requires higher standards of application for the right against self-incrimination. In terms of RICA 2002, the state can already compel the suspect/target of an encryption direction to (a) disclose the decryption key; or (b) provide decryption assistance.[254] This is a considerable investigative power of the state to access encrypted devices and information. It is often likely that law enforcement and the security and intelligence agencies will know the decryption holder who knows or can provide the passcode, and they can obtain a decryption direction compelling them to do so.[255] In terms of RICA 2002, a decryption holder, or employee of a decryption holder who fails to comply with a decryption direction is guilty of an offence and subject to penalties, including fines and/or imprisonment.[256] The decryption holder may decide to enter the password or passcode, and potentially incriminate themselves. This may not work in every investigation. The decryption holder may refuse to do so, or mislead by entering the incorrect password (they will likely have knowledge that a certain number of incorrect tries may lock the device forever), and would rather accept the offence and penalties than comply with a decryption direction. Some may claim to be forgetful, cannot be traced or dead. While most compelled decryption cases to date have involved illicit images, possession or distribution thereof, the widespread use of encryption also means a range of challenges for the state including data synced to encrypted cloud storage and computing, including encrypted communications and other more novel applications such as digital currencies and blockchain platforms.[257] The suggested doctrinal approach to the right against self-incrimination in compelled decryption cases, in light of the impact of widespread use of encryption in the information age, arguably should not leave

[253] Ibid at 796. However, see P Swire & K Ahmad 'Encryption and globalization' 13 (2012) *Columbia. Science & Technology LR* 416 at 420 arguing that technology, including encryption 'is actually enabling 'a golden age of surveillance.'

[254] Section 29(1).

[255] See Kerr op cit note 3 at 798-799. See Sacharoff op cit note 142 at 208 for the argument of the inference of ownership/possession in relation to the inference that the suspect/target knows the passcode, Sacharoff agrees that in almost all cases, especially those involving smartphones, the ability of the suspect/target to decrypt a device 'will be very powerful evidence of both facts' – that the suspect/target knows the passcode and the device belongs to him/her. That the compelled act of decrypting the device 'implicitly communicates ownership or control of the device and the files on it, argues Sacharoff: 'the government should have to show, under the foregone conclusion doctrine, that it knows the person possesses these particular files, or class of files, and can identify them with reasonable particularity. Even then, the government should be entitled to identify those files only.'

[256] Section 51(4).

[257] Sacharoff op cit note 142 at 210.

law enforcement and the security and intelligence agencies helpless in being able to access decrypted devices or information.[258]

The counter argument is that state access to our electronic information can be very invasive. The impact of new technologies means that law enforcement and security agencies can have access to more information than previously possible, most of which will be irrelevant to any investigation. The United States Supreme Court in *Riley v California*[259] referred earlier in the thesis, recognised that a device, such as a smartphone 'contains in digital form many sensitive records' and 'also contains a broad array of private information'[260] all in one's pocket or bag. Roberts CJ observed that the data stored on a smartphone is distinguishable from other physical objects that may be found on a person 'in both a quantitative and qualitative sense.'[261]

Does this mean that the protection afforded to the right against self-incrimination should be of a higher standard as a response to the reality of the impact of new technologies in the information age?[262] No, the preferable approach is that the 'basic principles of human rights' and notions of basic fairness and justice must be applied to the facts of a case. This necessarily involves considerations of public interest in determining whether the trial is rendered unfair, especially in cases involving serious infringement of constitutionally guaranteed rights', balanced against public interest that crime should be detected and the perpetrators punished. The primary concern should be the right to privacy which should be vigorously invoked. This potentially allows for more scope to justify the infringement of the privilege against self-incrimination or interpret the content of the right more narrowly.

As argued in earlier chapters, there should be restrictions on the ability of the state to access our electronic information. These robust protections should come into play in the context of search warrants that restrict searches of encrypted devices seized by law enforcement and the state and security agencies, with a key goal the protection of 'a principle against government fishing expeditions in which agents conduct vast, exploratory searches for unsuspected, new crimes against suspects or even non-suspects.'[263] The Supreme Court in *Riley* is an example of the judiciary's willingness to have new doctrinal principles apply to search of electronic devices, such that in the absence of 'more precise guidance from the

[258] See Kerr op cit note 3 at 795.
[259] 573 U.S. ___ (more) 134 S. Ct. 2473; 189 L. Ed. 2d 430 at 2490.
[260] Supra note 259 at 2490.
[261] Supra note 259 at 2490.
[262] See Kerr op cit note 3 at 796.
[263] Sacharoff op cit note 142 at 251.

founding era' the court indicated that it was willing to perform a balancing test for cases involving information found on electronic devices and limit the scope of execution warrants on such devices.[264] I believe this will be an important direction for developing a rule for the protection of passwords and passcodes.

The testimonial aspects of entering a passcode to decrypt a device or information should be seen as separate and distinct from the evidence that the decrypted device or folder may reveal.[265] The response to higher protections needed for electronic information should be placed elsewhere, not in the form of the right against self-incrimination acting as an absolute barrier to state access.[266] For example, there must be safeguards in South African legislation on storing, accessing, examining, using and destroying electronic information after it has been obtained by the state, such that it provides adequate safeguards against abuse of treatment of personal data and thus serve to protect individuals' personal integrity and highly sensitive information integral to the right to privacy. The current framework in RICA 2002 is lacking in this regard. This is an opportune moment, in view of the constitutional challenges on RICA 2002, to rectify the lack of safeguards and ensure that when a suspect/target has been compelled to decrypt a device that law enforcement and the state and security agencies cannot search anywhere, every file, folder, applications, deleted files and communications data. I find Sacharoff's proposed rule of particularity agreeable in this context:

> 'It will assure a suspect that law enforcement limits its search to documents relevant to the crime by limiting it to those documents. The suspect will not have to worry that law enforcement will, having gained access to the device, scour its entirety looking at unrelated photos and videos, even if only out of curiosity. Instead, the suspect will *know* precisely which files the government has access to. It will similarly provide the suspect with an accounting of the files accessed. This will both give the suspect control and help make the people "secure in their … papers."'[267]

While decryption is often regarded as a right against self-incrimination question, the balancing of interests within a search and seizure framework cannot be ignored. It avoids an all-or-nothing approach in terms of which the compelled entering of a password infringes the

[264] Supra note 259 at 2478. See generally OS Kerr 'Ex ante regulation of computer search and seizure' 96 (2010) *Virginia LR* 1241 for a debate on whether to impose ex ante restrictions or rely on ex post judicial review and approving ex ante limits.
[265] See Kerr op cit note 3 at 797.
[266] Ibid.
[267] Sacharoff op cit note 142 at 248 (emphasis in original text, footnotes omitted).

right against self-incrimination as this would impose too high a burden on the state.[268] Practically, a suspect/target either decrypts the entire device (all-) or none of it (-or-nothing). However, Sacharoff's proposed rule of particularity avoids the all-or-nothing approach, giving law enforcement and the state and security agencies access to electronic information it can identify with reasonable particularity.[269] In this regard, legal authorisation for access to such information should impose strong protections on obtaining a search warrant with limits on the resulting searches, having regard to the unprecedent ability of the state to greater access to more and more of our information that did not exist two decades ago. It must guard against unreasonable searches and general warrants. Moreover, the doctrinal approach suggested will act as a limit to 'fishing expeditions' by law enforcement and the state and security agencies, and prevents them from exploratory searches of 'vast repositories' of personal information contained in devices, without limits.[270] Privacy advocates may not agree, but I believe that it should provide some assurance that law enforcement and the state and security agencies will not sift through the entirety of our personal devices after being compelled to acts of decryption. Therefore, this approach that enables law enforcement and the security and intelligence agencies to only access electronic information it can identify with reasonable particularity, also means that compelled decryption of a suspect/target's biometric based information cannot be viewed in isolation in terms of searches. The South African courts must be willing to rethink familiar and well-established constitutional doctrines in view of technological advancements.

As it transpires, our Constitution has included the exclusionary rule, in s 35(5), but it does not apply to all evidence improperly obtained, only to evidence obtained in a manner that violates any right in the Bill of Rights. The court must exercise its discretion and this is precisely the approach which has been adopted in the Constitution in s 35(5) in relation to criminal trials: evidence obtained by the state as a result of a deliberate and conscious violation of constitutional rights of an accused person should be excluded 'save where there are "extraordinary excusing circumstances".'[271] Although the courts are more likely to admit real evidence obtained as a result of a violation, due to its existence independently and irrespective of the violation, in each case the court will engage in a balancing exercise in terms of s 35(5) to determine whether the exclusion would render the trial unfair or be detrimental to the

[268] See D Terzian 'The Fifth Amendment, encryption, and the forgotten state interest' 61 (2014) *UCLA LR Discourse* 298 at 309-10.
[269] Sacharoff op cit note 142 at 248. See also B Folkinshteyn 'A witness against himself: a case for stronger legal protection of encryption' 30 (2013) *Santa Clara High Technology LJ* 375 at 411–412.
[270] Sacharoff op cit note 142 at 208.
[271] McCall J in *Naidoo's* case supra note 86 at 499.

interests of justice. [272] The arguments would appear to indicate that the ascertainment of bodily features will seldom infringe the right against self-incrimination. However, this does not exclude the possibility that in certain circumstances they might unjustifiably infringe the right to privacy or some other constitutional right. Further, when real evidence is obtained as a result of self-incriminating testimonial communications, justification for the admission of derivative evidence becomes tempered, and the evidence may be excluded as to admit it may render the trial unfair or otherwise be detrimental to the administration of justice.[273]

In developing a South African approach an important distinguishing feature of the legal regime between the United States of America and South Africa, is that the former has a relatively inflexible judicially created exclusionary rule together with a very narrow limitations jurisprudence. In the United States, subject only to certain exceptions, evidence obtained in violation of the Constitution is excluded.[274] Unlike South Africa (and Canada), the United States does not have an explicit constitutional device for limiting rights. Section 36 of the South African Constitution which allows for the justifiable limitation of rights, effectively means that the South African courts can afford a more generous approach to the contents of a right. Cases involving the compelled disclosure of a user's passcode (reveal/enter) may well be considered by our courts to be testimonial and therefore an infringement of the right against self-incrimination. However, provided the 'compulsion' is authorised by a law of general application then the validity of that law, must be adjudged in accordance with the provisions of the limitation clause.[275] If the limitation is justifiable, evidence acquired as a result of such a breach will not fall to be excluded in terms of the right (to privacy and, in particular, the privacy of communications) can be limited by a law of general application as enunciated in s 36, which must be applied before the constitutional exclusionary rule in s 35(5).[276]

Although the provisions of RICA 2002 in relation to compelled decryption are not necessarily unconstitutional, the solution perhaps to the issue of compelled decryption and the impact of new technologies in particular the scenarios referred, is to be found in new legislation that meets the requirements of the limitations clause. This means that if the infringement of

[272] *Pillay's* case supra note 115.
[273] *Tandwa's* case supra note 84.
[274] As expressed in cases such as *Mapp v Ohio* (1961) 367 US 643 and *Miranda v Arizona* 384 US 436.
[275] See earlier at 136, 138..
[276] For a useful account of these cases see *Naidoo's* case supra note 86 at 491-98 for the general approach adopted in South Africa prior to 1994, that if the evidence was obtained in breach of a constitutional right, it should be excluded unless the breach was justified in terms of s 33(1) of the interim Constitution.'

rights is justified in terms of the limitation clause, then s 35(5) insofar as it relates to unconstitutionally obtained evidence does not apply.

V CONCLUSION

Encryption in 2020 is everywhere. It is almost routine for ordinary users to use encryption to protect the contents of communications, computers, tablets, and especially smartphone devices. If the password or passcode is strong, the encrypted data or device is 'all but unbreakable'.[277] Compelling decryption is one option available to law enforcement and the security and intelligence agencies. As demonstrated in the above analysis, a nuanced understanding of the interaction between modern technology and legal doctrine will be integral in the development of doctrinal principles and robust approaches of the courts in compelled decryption cases. Such an approach asks the courts to look beyond precedent, and the rather rudimentary distinction between self-incriminating testimonial communications and incriminating non-testimonial real evidence, to the implications of such doctrinal approach in a technologically advanced context: what is the appropriate standard for how the right against self-incrimination should apply in cases of compelled decryption where encryption is commonplace? There is little consensus as regards the correct approach. Encryption presents an increasing obstacle to the legitimate needs of law enforcement and the approach suggested represents a balance of interests. The South Africa courts should interpret the right against self-incrimination in compelled decryption cases such that modern technology does not dramatically shift the balance of power against the public interest in preventing and detecting criminal activity. The limitations clause in this regard will certainly be in the reckoning, such that an infringement may be justified in terms of s 36 of the Constitution, if it is reasonable and justifiable in an open and democratic society, having regard to the factors specified therein. I do not expect that mine will be the final word on the issues identified and the suggested doctrinal approach for South African courts, but rather only a first step in stimulating much needed debate on compelled decryption cases in South African law.

The final chapter of the thesis, chapter five, is a consideration of issues in relation to admissibility of electronic evidence in criminal proceedings.

[277] *Riley's* case supra note 259 at 12-13.

CHAPTER FIVE

RETHINKING ADMISSIBILITY AND EVIDENTIAL WEIGHT OF ELECTRONIC EVIDENCE IN THE INFORMATION ERA

I INTRODUCTION

The introduction of electronic evidence in criminal legal proceedings raises unique challenges in the South African law on evidence. This chapter identifies two separate issues in this regard: (i) admissibility of electronic evidence and (ii) its weight. In doing so, analysis of relevant provisions of the Electronic Communications and Transactions Act 25 of 2002[1] are considered. Part II focuses on the provisions in the ECT Act 2002 dealing with the admissibility and evidential weight of electronic evidence. Part III considers electronic evidence in the context of the rules applicable to documentary, hearsay and real evidence. Part IV reconsiders the evidential weight of electronic evidence and new rules on and the business records exception, including authenticity and integrity. Part V completes the chapter with concluding remarks on rethinking admissibility and evidential weight of electronic evidence in the information era.

II ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002

Chapter III of the ECT Act 2002 explicitly deals with the law of evidence, specifically s 15 under the heading 'admissibility and evidential weight of data messages' In terms of its sphere of application s 4 of the ECT Act 2002 states: 'this Act applies in respect of any electronic transaction or data message.' As the ECT Act 2002 is largely based on an electronic commerce model law that only applies to commercial activities,[2] are there any concerns for the scope and application of the ECT Act 2002 in criminal proceedings? Arguably, on a strict interpretation of the Model Law on Electronic Commerce[3] on which the ECT Act 2002 is based, the MLEC only applies to commercial matters, and as such chapter III should not extend to matters outside the commercial sphere, that is, non-commercial civil or criminal matters. However, to restrict the scope and application of chapter III to only commercial matters would be particularly problematic in the law of evidence, and contrary to the purposes of the ECT Act 2002 as an

[1] Hereafter 'ECT Act 2002'.
[2] See UNCITRAL MLEC article 1: 'This Law applies to any kind of information in the form of a data message used in the context of commercial activities".
[3] *UNCITRAL Model Law on Electronic Commerce* (1996) available at *http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html*, accessed 1 August 2019 (hereafter MLEC).

enabling Act which partly states in its long title: 'to provide for the facilitation and regulation of electronic communications and transactions.' The MLEC is not restrictive in this regard and does not prevent an enacting State from extending the scope of the MLEC to cover the use of electronic commerce outside the commercial sphere.[4] Footnote *** in article 1 of the MLEC provides options for enacting States that would consider it appropriate to extend the scope of the Model Law beyond the commercial sphere.[5] Although the ECT Act 2002, does not expressly state for the application of chapter III to matters outside the commercial sphere, to interpret otherwise would 'leave a serious lacunae in South African law and, in particular, in the South African law of evidence.'[6] Nonetheless, the currently fragmented legal framework to admissibility of electronic evidence in criminal proceedings, based on an electronic commerce model law and commercial activities, has created challenges in South African law.

The term 'electronic evidence' is not referred to in any law governing the admissibility of evidence. As with the MLEC, the ECT Act 2002, refers to the output of information by/in an electronic medium as 'data message' or 'electronic transaction'. To the extent appropriate these terms will be used interchangeably with the preferred term 'electronic evidence'. Section 1 of the ECT Act 2002 sets out definitions of inter alia 'data message', 'automated transaction' as an electronic transaction and other relevant key terms:

> '"data" means electronic representations of information in any form;
>
> "data message" means data generated, sent, received or stored by electronic means and includes – (a) voice, where the voice is used in an automated transaction; and (b) a stored record;'
>
> "automated transaction" means an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment.'

Since coming into law almost two decades ago, the scope and significance of electronic evidence in criminal proceedings is broader than initially envisaged in the ECT Act 2002. Having regard to the types of devices now in frequent use, the medium of electronic evidence

---

[4] See United Nations Commission on International Trade Law *Model Law on Electronic Commerce with Guide to Enactment* (1996) with additional art 5bis adopted by resolution of General Assembly 51/162 of 6 December 1996 at 31 available at *https://www.uncitral.org/pdf/english/texts/electcom /05-89450_Ebook.pdf*, accessed 3 March 2020 (hereafter 'MLEC *Guide to Enactment*').
[5] Ibid at 3.
[6] J Hofman 'South Africa' in S Mason (ed) *Electronic Evidence: Disclosure, Discovery and Admissibility* (2007) 459 at 462.

has now far surpassed computers.[7] The information age necessitates the expansion of the scope of electronic evidence to recognise the realities of a modern fast-paced environment of technological advancements.[8] There are specific offences where evidence will typically be available exclusively in electronic form, which is particularly transient in nature. For example, this is the case for cyber-related crimes.[9] The modern categorisation of electronic evidence often distinguishes between two types of electronic evidence. The first emphasises the relationship between electronic evidence and telecommunication service providers.[10] The second type relates to traditional evidence electronically stored, processed and transmitted that is specific to the case in question.[11] This second type of electronic evidence is recognised in the ECT Act 2002 by the definition of 'data message' above, where the storage of data is a defining component. A definition of electronic evidence needs to be broad enough to recognise network activities that are also necessary as evidence in criminal investigations or criminal proceedings: '[d]ata held by providers of internet infrastructure services, such as domain name registrars and registries and privacy and proxy service providers, or regional internet registries for internet protocol addresses, may be of relevance for criminal proceedings as they can provide traces allowing for identification of an individual or entity involved in criminal activity.'[12] RICA 2002 does this to an extent in the context of investigatory powers, but within

---

[7] See E Casey *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 2ed (2004) at 12 defined electronic evidence as 'any data stored or transmitted using a computer that support or refute a theory of how an offence occurred or that address critical elements of the offence such as intent or alibi.'

[8] H Wu & G Zheng 'Electronic evidence in the blockchain era: New rules on authenticity and integrity' 36 (2020) 105401 *Computer Law & Security Review* 1.

[9] See AA *Gillespie Cybercrime: Key Issues and Debates* 2ed (2019).

[10] See Wu & Zheng op cit note 8 at 3 referring to the example in Chinese law, in 2015, in which the Supreme People's Court defined electronic evidence in article 116 of the Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law '[e]lectronic data shall include e-mails, electronic data inter-change, online chatting records, blog, micro-blog, SMS, electronic signatures, domains and other information formed or stored in electronic media.'

[11] Wu & Zheng op cit note 8 at 3 also provide an example of this type of electronic evidence as decreed by the Supreme People's Court: '[e]lectronic data are data that are formed in the process of occurrence of a case, stored, processed, and transmitted in digital form, and can prove the case facts. Electronic data include but are not limited to the following information and electronic documents: (1) [i]nformation published through such network platforms as webpages, blogs, microblogs, moments, post bars, and network disks. (2) [c]ommunicatio**n** information in such network application services as SMS, email, instant messaging, and communication groups. (3) [i]nformation including user registration information, identity authentication information, electronic trading records, communication records, and logon logs. (4) [e]lectronic documents including documents, pictures, audio and video records, digital certificates, and computer programmes. The testimony of witnesses, victim statements, and confessions and arguments of criminal suspects or defendants recorded in digital forms and other evidence are not electronic data. Where it is really necessary, these provisions may apply, mutatis mutandis, to the collection, taking, transfer, and examination of the relevant evidence.'

[12] European Commission *Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters* Strasbourg, 17.4.2018 COM (2018) 225 final at 14 available at *https://eclan.eu/files/attachments/.2504/L_Proposal _Regulation_e_evidence _2018.pdf*, accessed 20 April 2020.

the definition of 'data message' as electronic evidence in the ECT Act 2002. Arguably, advancements in technology in the information age demands more, and for the recognition of electronic evidence beyond 'voice' and a 'stored record' in the definition of 'data message' in the Act.

In relation to the first type of electronic evidence referred to above, the European Commission in recently proposed regulations for electronic evidence in criminal matters, defines 'electronic evidence' in article 2 as 'evidence stored in electronic form by or on behalf of a service provider at the time of receipt of a production or preservation order certificate, consisting in stored subscriber data, access data, transactional data and content data.'[13] Although the term 'evidence' is not defined as such, the definition refers to four types of data which might constitute of evidence: subscriber data, access data, transactional data (these three categories commonly referred to jointly as 'non-content data')[14] and stored content data.[15] 'Content data' means 'any stored data in a digital format such as text, voice, videos, images.'[16]

When assessing the relevance and admissibility of evidence, the provision of a broader definition of electronic evidence allows some flexibility to the courts as to how to take them into account especially with regard to authenticity and integrity. In this chapter, I addresses the specific problem created by the volatile nature of electronic evidence. Admissibility and evidential weight of electronic evidence is addressed in s 15 of the ECT Act 2002:

> '(1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence-
>
> *(a)* on the mere grounds that it is constituted by a data message; or
> *(b)* if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

[13] Ibid at 39.
[14] Ibid at 39 where the following definitions are provided: 'subscriber data' means 'any data pertaining to the identity of a subscriber or customer such as the provided name, date of birth, postal or geographic address, billing and payment data, telephone, or email' including inter alia the type of service and its duration; 'access data' means 'data related to the commencement and termination of a user access session to a service, which is strictly necessary for the sole purpose of identifying the user of the service, such as the date and time of use, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the user of a service, data identifying the interface used and the user ID' and 'transactional data' means 'data related to the provision of a service offered by a service provider that serves to provide context or additional information about such service and is generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression, unless such data constitutes access data.'
[15] Ibid at 14.
[16] Ibid at 39.

(2) Information in the form of a data message must be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard must be had to-

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the integrity of the data message was maintained;

(c) the manner in which its originator was identified; and any other relevant factor.

(4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of facts contained in such record, copy, printout or extract.'

The corresponding equivalent of s 15 of the ECT Act 2002 in the MLEC is article 9. The MLEC *Guide to Enactment* states that its purpose 'is to establish both the admissibility of data messages as evidence in legal proceedings and their evidential value.'[17] On admissibility, article 9 establishes that data messages 'should not be denied admissibility as evidence in legal proceedings on the sole ground that they are in electronic form.'[18] With regard to the assessment of the evidential weight of a data message, the MLEC *Guide to Enactment* provides useful guidance as to how the evidential value of data messages should be assessed, for example, depending on whether they were 'generated, stored or communicated' in a reliable manner.[19]

The admissibility of electronic evidence in criminal proceedings, situated in a law based on an electronic commerce model law and commercial activities raises interesting questions in the law of evidence, particularly, its interaction with other statutory provisions on admissibility of evidence. The meaning and application of s 15, insofar as it applies to electronic evidence as hearsay or real evidence, or both, is a key and controversial issue. Does s 15 prescribe a rule of admissibility for *all* electronic evidence, irrespective of hearsay representations contained therein? In other words, is electronic evidence exempt from the evidential rules on hearsay by virtue of s 15? Or does s 15 prevent hearsay representations in electronic evidence from being treated like real evidence, the latter which needs only to be relevant to be admissible? Or is it

[17] MLEC *Guide to Enactment* op cit note 4 at 44.
[18] Ibid para 70.
[19] Ibid para 71.

the case for real evidence that in order for electronic evidence to be admissible, authenticity is a pre-requisite for admissibility? Electronic evidence must according to s 15(2) be given 'due evidential weight'. Electronic evidence has very different characteristics to ordinary documentary or material evidence. Such evidence can be easily subject to errors in code or software and hardware functionality, alteration, deletion and modification. Yet authentication and integrity of electronic evidence is often based on the application of rules as they relate to documentary evidence. For example, documents that fall within exceptions to the exclusionary rule against hearsay, such as the business records exception, directly translated for electronic records in my view has now created a problematic presumption in the context of electronic evidence of business records. An examination of authenticity and integrity of electronic evidence should require a consideration by the courts through the whole process of electronic evidence from the time of its creation to the time of being admitted into evidence.[20]

III ADMISSIBILITY OF ELECTRONIC EVIDENCE

(a) Does s 15 make all electronic evidence exempt from the evidential rules regulating hearsay?

In terms of s 3(4) of the Law of Evidence Amendment Act 45 of 1988[21] hearsay evidence is defined as 'evidence, whether oral or in writing, the probative value of which depends upon the credibility of any person other the person giving such evidence.' Section 3(1) provides that hearsay evidence is inadmissible and will only be admitted if one of the following three conditions is met: (i) consent is given by the party against whom it is sought to be admitted; (ii) the person on whose credibility the probative value of the evidence depends will testify later and (iii) admission would be in the interests of justice.

For the purposes of the discussion on electronic evidence, I believe that there is little to be gained by examining the history of the formulation of the evidentiary rule excluding hearsay, including all the exceptions. Suffice to add that the primary reason for excluding hearsay was its '*general* unreliability – the fact that it rested for its evidential value on the untested memory, perception, sincerity and narrative capacity of a declarant or actor who was not subjected to the oath, cross-examination or any of the other procedural devices to which our adversary system of trial procedure subjects a witness giving original evidence.'[22] The

[20] Wu & Zheng op cit note 8 at 5.
[21] Hereafter 'LEA Act 1988'.
[22] DT Zeffertt & DT Paizes *The South African Law of Evidence* 2ed (2003) at 400 (emphasis in original text).

traditional approach was to exclude evidence in the absence of a recognised exception 'not because a court could not be assured of its reliability, but that its reliability was effectively unknowable due to the absence of an ability to cross-examine.'[23] If objections to exclusionary rule were overcome, then the rationale for the exclusion no longer applied.[24]

The application of the principles of the exclusionary rule on hearsay to electronic evidence is complex and, as will be seen from the analysis below, raises 'unique issues that will often make electronic evidence stand apart from other forms of evidence.'[25] There is no reference to 'data message' or 'electronic' evidence in s 3(4). What does this mean for s 15, specifically for the application that 'the rules of evidence must not be applied so as to deny the admissibility of a data message'? Is a data message hearsay within the meaning of the LEA Act 1988? If yes, does s 15 override the normal rules applying to hearsay evidence to make data message exempt from the exclusionary rule on hearsay? Or is a data message subject to the exclusion within the meaning of s 3 of the LEA Act 1988?

One interpretation of s 15, a generous and wide interpretation, would allow admissibility for *all* electronic evidence, irrespective of hearsay representations contained therein, and a court's discretion would merely relate to an assessment of evidential weight based on the factors enumerated in s 15(3).[26] An alternative interpretation is that s 15 allows for admissibility of electronic evidence, subject to the ordinary rules of evidence including those applicable to hearsay. The approach of the South African courts has been to favour the latter. I am in favour of the former inclusionary approach. If fact-based issues of authenticity and integrity can be 'substantively satisfied' then hearsay as an exclusionary rule of evidence should no longer be warranted for electronic evidence based on the scope of inquiry in s 15(1) to (3).[27] Schwikkard and Van der Merwe, in an earlier edition, noted: '[t]he definition of 'data message' is sufficiently broad to include hearsay evidence and accordingly the section subjugates the hearsay rule in so far as the admissibility of computer printouts are concerned The courts appear to have no discretion in respect of the admissibility of a data message but rather they are required to exercise their discretion when they assess the weight to be attached

[23] C Gallavin & D Seng 'Hearsay' in S Mason & D Seng (eds) *Electronic Evidence* 4ed (2017) 70 at 73. In *S v Molimi* 2008 (3) SA 608 (CC) para 65, the Constitutional Court stated that '[t]he rationale of excluding hearsay as inadmissible is a recognition of the unreliability and unfairness emanating from such evidence. Its unreliability and susceptibility is said to be based on the so-called "hearsay damages" of insincerity and defective memory, perceptive powers and narrative capacity.'
[24] Zeffertt & DT Paizes op cit note 22 at 400.
[25] Gallavin & Seng op cit note 23 at 71.
[26] See *S v Ndiki and Others* 2008 (2) SACR 252 (Ck).
[27] See Gallavin & Seng op cit note 23 at 71.

to the evidence.'[28] However, in a subsequent edition they discarded this interpretation and noted: '[t]he exact meaning of this provision requires close consideration of the established principle that the law excludes documents as hearsay because of doubts about the reliability of their content. Therefore, should s 15(1) be given too wide an interpretation by making all data messages admissible then it would undermine the established law which governs manuscript documents.'[29]

I am not unopposed to the approach of the South African courts, after all, emerging case law at the time in its 'inclusionary as opposed to exclusionary'[30] approach to the ECT Act 2002 sought to rectify the exclusion electronic evidence in the form of computer printouts on the reasoning that the disputed documents contained information 'obtained after treatment by arrangement, sorting, synthesis and calculation by the computer.'[31] Indeed, as the court in *S v Brown*[32] noted: '[c]learly, the overall scheme of the ECTA is to facilitate the admissibility of data messaging as electronic evidence.' In 2020 we have now moved beyond the challenges of exclusion of electronic evidence simply because information contained therein had been processed by the computer. Whether the continued approach to either apply traditional rules of evidence to electronic evidence or to adjust the rules as deemed necessary is the central issue. I begin by considering the interpretation of s 15 of the ECT Act 2002 favoured by the courts.

Zeffertt and Paizes suggest that a 'data message' 'is clearly hearsay within the meaning of s 3(4) whenever it is tendered in evidence in circumstances where the probative value of the evidence depends, *in this sense*, on the credibility of such a person.'[33] The 'in this sense' referred to by the authors concerns the case where the probative value of the evidence depends on the credibility of the person who programs the computer system or software to accurately register and process information contained in the computer printout.[34] This raises the question

---

[28] PJ Schwikkard & SE van der Merwe in collaboration with DW Collier, WL de Vos, A St Q Skeen and E van der Berg *Principles of Evidence* 2ed (2002) at 385, acknowledging that provisions of the ECT Act 2002 are an improvement 'on the prior, muddled, state of affairs and it is anticipated that the provisions will allow for a more equitable approach to computer generated evidence.'

[29] Schwikkard, PJ & SE van der Merwe *Principles of Evidence* 4ed (2015) at 441-43.

[30] *Ndiki's* case supra note 26 at 258. See also *S v Brown* 2016 (1) SACR 206 (WCC) at 213: '[t]he ECTA follows an inclusionary rather than an exclusionary approach to the admission of electronic communications as evidentiary material.'

[31] *S v Mashiyi and Another* 2002 (2) SACR 387 (Tk) at 390. At 393, Miller J concluded: 'All that I can do is add my voice to the call that this lacunae in our law be filled and for new legislation relating specifically to computer evidence in criminal cases be considered and promulgated.' Legislative intervention eventually came, seven years later, in the form of the ECT Act 2002. See also *S v Harper* 1981 (1) SA 88 (D).

[32] Supra note 30 at 213.

[33] Zeffertt & DT Paizes op cit note 22 at 394 (emphasis added).

[34] See *La Consortium & Vending Cc T/A La Enterprises v MTN Service Provider (Pty) Ltd* 2011 (4) SA 577 (GSJ) at 591.

of the effect of applying s 15 to the admissibility electronic evidence – is it to be regarded as expansive in accordance with 'the purpose of the legislature … to free as much computer-generated evidence from the hearsay trap as could be justified without doing violence to the important values served by the exclusionary rule'[35] on the basis that s 15(1) provides that 'the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence'? If so, what does this mean in a situation where the evidence tendered is processed and generated by a computer, and not merely utilised for storing information? If it is accepted that such evidence is prima facie hearsay, can s 15 be used to admit it?[36] Yes, it can, potentially on the basis of s 15(1) if the only hurdle to its admissibility is 'on the mere grounds that it is constituted by a data message.'

Another interesting issue that arises is: what if the evidence sought to be admitted is not 'constituted by a data message'?[37] The application of s 15 of the ECT Act 2002 and its relationship with s 3 the LEA Act 1988 was first considered in *Ndlovu v Minister of Correctional Services and Another*,[38] in which the court was asked to consider electronic evidence in the form of a two page computer generated printout in diary form, from the computer system of Community Corrections (a section of the Department of Correctional Services). The electronic evidence showed that various violations of the plaintiff had been recorded by several different persons. On the testimony of two persons who recorded entries, the court held that their entries did not amount to hearsay. Entries by other persons who were not called to give evidence was held by the court to be hearsay. The evidence was ruled admissible by the court based on discretion to do so in terms of s 3 the LEA Act 1988, without being prejudiced by authenticity and original forms rules for documentary evidence. On the application of s 15 of the ECT Act 2002, the court took the view that the ECT Act 2002

[35] Zeffertt & Paizes op cit note 22 at 394.
[36] Ibid.
[37] Ibid at 395, the authors advocate an approach that 'would leave all the work—as far as hearsay is concerned—to the other exceptions, a conclusion that is not indefensible in view of the wide sweep of section 3(1)(c) of the Law of Evidence Amendment Act 45 of 1988 which allows for the reception of hearsay if the court is of the view, after considering the stipulated factors, that its admission would be in the interests of justice.' Further, at 394: '[t]o answer this question, one has to ask what it would be if it were not constituted by a data message. If it were to be regarded as direct oral evidence furnished by a person upon whose credibility the probative value of the evidence depends, it would clearly not be hearsay and would be admissible. But if it were to be regarded as evidence tendered by a witness other than the person upon whose credibility the probative value of the evidence depends, it would still be hearsay and would, to be admissible, have to satisfy the requirements of section 3 of the 1988 Act or some other exception to the hearsay rule (such as section 221 or section 222 of the Criminal Procedure Act).'
[38] [2006] 4 All SA 165 (W).

facilitates admissibility, but the rules relating to hearsay and documentary evidence have not been excluded entirely by s15:

> 'The provisions of section 15 require closer scrutiny. *Subsection (1)(a) appears, on a quick reading, to render a data message admissible without further ado. However, it would be anomalous if that were the case, since the ECT Act would then elevate a data message evidentially above an ordinary document.* Rather, on a proper reading, section 15(1)(a) prohibits the exclusion from evidence of a data message on the mere grounds that it was generated by a computer and not by a natural person, and section 15(1)(b) on the mere grounds that it is not in its original form. … Where the probative value of the information in a data message depends upon the credibility of a (natural) person other than the person giving evidence, *there is no reason to suppose that section 15 seeks to override the normal rules applying to hearsay evidence*. On the other hand, where the probative value of the evidence depends upon the "credibility" of the computer (because information was processed by the computer), section 3 of the Law of Evidence Amendment Act 1988 will not apply, and there is every reason to suppose that section 15(1), read with sections 15(2) and (3), intend for such "hearsay" to be admitted, and due evidential weight to be given thereto according to an assessment having regard to certain factors.'[39]

The court found support of this approach with reference to Zeffertt & Paizes[40] in that 'the purpose of the legislature was probably to free as much computer-generated evidence from the hearsay trap as could be justified without doing violence to the important values served by the exclusionary rule.'[41] In *La Consortium & Vending Cc T/A La Enterprises v MTN Service Provider (Pty) Ltd*,[42] the court adopted the preferred reasoning in *Ndlovu*. It was argued by the appellant that the computer generated documents created by a computer software system and relied upon by the respondent constituted hearsay evidence and consequently inadmissible. Having regard to the provisions of the LEA Act 1998 the court had to 'determine whether the "data messages" relied upon should be admitted despite their containing hearsay evidence.' Although the court ultimately determined that the electronic evidence constituted real evidence, and was correctly admitted into evidence, it expressed its interpretation of s 15 as follows:

> 'The definition of "data message" in s 1 is sufficiently wide to include not only real, but also hearsay, evidence. This follows from the wide description of "data" as the "electronic representations of information in any form", but also from the definition of "data message" as

[39] *Ndlovu's* case supra note 38 at 172-73 (emphasis added).
[40] Zeffertt & Paizes op cit note 22 at 394.
[41] *Ndlovu's* case supra note 38 at 18.
[42] Supra note 34. See also *Sublime Technologies (Pty) Ltd v Jonker and Another* 2010 (2) SA 522 (SCA).

> "data generated, sent, received or stored by electronic means", including "(a) voice, where the voice is used in an automated transaction; and (b) a stored record". *This, however, does not mean that hearsay is admissible just because it is contained in a data message. The principle of "functional equivalence" does not free data messages from the normal strictures of the law of evidence,* but only from those referred to in s 15(1). *It follows that, despite the very wide words of s 15(4), any hearsay contained in a data message must pass the criteria set out in s 3 of the Law of Evidence Amendment Act 45 of 1988.*'[43]

A similar approach to s 15 was also supported by the Supreme Court of Appeal in *Firstrand Bank Limited v Venter*.[44] As regards electronic evidence in the form of bank statements as proof of an overdrawn account, the court held that s 15 'facilitates the use of and reliance on a data message.'[45] The interpretation of the ECT Act 2002 that 'follows an inclusionary rather than an exclusionary approach to the admission of electronic communications as evidentiary material' was also taken in *S v Brown*.[46] The court was required to determine whether images found on a mobile phone were admissible as evidence. The images in question were downloaded from the mobile phone, reproduced in hard copy paper form and enlarged. It was contended by the accused that the images amounted to inadmissible hearsay evidence. Bozalek J held:

> 'Section 3(4) of the Law of Evidence Amendment Act 45 of 1988 defines hearsay evidence as evidence, whether oral or in writing, the probative value of which depends upon the credibility of any person other than the person giving such evidence. The three images which the state seeks to introduce as evidence are photographs, apparently of the accused, and, subject to proof of his identity and bearing in mind the limited purpose for which they are tendered, their probative value stands or falls by that simple fact. In this sense, at least, the images are more akin to being 'real evidence', but, however they are classified, they do not constitute hearsay evidence.'[47]

The approach of the courts is also reflective of the 'enabling character'[48] of the ECT Act 2002 'by ousting [previous] evidence rules which would exclude electronic evidence purely because of its electronic origin.'[49] This follows from s 15(1)*(a)* which states that 'admissibility of data messages' must not be denied 'on the mere grounds that it is constituted

[43] Supra note 34 at 592-93 (emphasis added).
[44] 2012 JDR 1676 (SCA).
[45] Supra note 44 para 19.
[46] Supra note 30 at 213.
[47] Supra note 46 at 216.
[48] Schwikkard & Van der Merwe op cit note 28 at 443.
[49] Ibid at 442 with reference to the decision in *Ndlovu's* case supra note 38.

by a data message.' The MLEC *Guide to Enactment* in article 5 on 'legal recognition of data messages' states the following: '[i]nformation shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.'[50] Hofman argues that the basis of s 15 is the 'form in which information is kept' and not the content of the message.'[51]

In terms of the prevailing interpretation of s 15 any hearsay representations contained in electronic evidence triggers s 3 of the LEA Act 1988 and must pass the criteria set out therein for admissibility purposes. However, if it is accepted – as I submit it must be – that *form* of electronic evidence in a year 2020 information age has become the norm in criminal legal proceedings, can it be argued that the ECT Act 2002 should make *all* electronic evidence admissible? Potentially, yes. I take the position that the ECT Act 2002 can be interpreted so as to make electronic hearsay evidence generally admissible. The definition of 'data message' in s 1 would be sufficiently wide to include not only real evidence, but to also include hearsay evidence by reference to 'data generated, sent, received or stored'.[52] The key issue is whether s 15 overrides the provisions of s 3 of the LEA 1988 when the evidence in issue is 'constituted by a data message'. In *Ndiki's* case, Van Zyl J noted that '[t]here is nothing specifically in the ECT Act 2020 that says that it does not.'[53] In other words, electronic evidence, real or hearsay, could be admissible as evidence in terms of s 15(2) and the court's discretion would simply relate to an assessment of the evidential weight in terms of s 15(3). Therefore, if fact-based issues of authenticity and integrity can be 'substantively satisfied' the hearsay rule need no longer be warranted for electronic evidence. This is based on the scope of inquiry in s 15(1) to (3) and due evidential weight to be given according to an assessment having regard to certain factors.[54]

---

[50] *MLEC Guide to Enactment* op cit note 4 at 5. At 31: 'Article 5 embodies the fundamental principle that data messages should not be discriminated against, i.e., that there should be no disparity of treatment between data messages and paper documents. … By stating that "information shall not be denied legal effectiveness, validity or enforceability solely on the grounds that it is in the form of a data message", article 5 merely indicates that the form in which certain information is presented or retained cannot be used as the only reason for which that information would be denied legal effectiveness, validity or enforceability. However, article 5 should not be misinterpreted as establishing the legal validity of any given data message or of any information contained therein.'

[51] J Hofman 'South Africa' in S Mason (ed) *Electronic Evidence: Disclosure, Discovery and Admissibility* (2007) 459 at 466. This is based on the definition in the ECT Act 2002, aligned to the MLEC: 'data' is 'electronic representations in any form' and 'data message is defined as 'data generated, sent, received or stored by electronic means.' See s 1, ECT Act 2002.

[52] *Ndiki's* case supra note 26 at 258.

[53] Supra note 26 at 258.

[54] See Gallavin & Seng op cit note 23 at 71.

The MLEC was adopted by the Commission at its twenty-ninth session, in June 1996. The ECT Act 2002 came into law in 2002. The interpretation of the ECT Act 2002 favoured by the courts, and also in academic scholarship, is sensible and must be seen in the context of particular legislation at the time that excluded electronic evidence because of its electronic origin. The corresponding equivalent of s 15 of the ECT Act 2002 in the MLEC is article 9. The functional equivalence approach, we are told, does not apply to s 15/article 9: 'A data message, in and of itself, cannot be regarded as an equivalent of a paper document in that it is of a different nature and does not necessarily perform all conceivable functions of a paper document.'[55] Hofman argues differently, as have the South African courts, rejecting the position that s 15 makes all electronic evidence admissible stating that 'it would go against the functional equivalence between data messages and documents by treating their evidential value differently.'[56] Similarly, in *Ndlovu's* case it was observed that the aim of s 15 'appears to be to place electronic information on the same footing as traditional paper-based transactions.'[57]

The difference between the wording of s 15 (2), (3) and (4) and its article 9 equivalent in the MLEC is where I also find support for my argument. Section 15(4) has no equivalent in the MLEC. A literal wording of the section counters the doctrine of functional equivalence that should apply between electronic evidence and documentary evidence.[58]

Section 15(2), (3) and (4) states:

'(2) Information in the form of a data message must be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard must be had to-

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the integrity of the data message was maintained;

(c) the manner in which its originator was identified; and any other relevant factor.

(4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary

[55] *MLEC Guide to Enactment* op cit note 4 at 21.
[56] Hofman op cit note 51 at 464. In addition, he states: 'it would go beyond the purpose of the ECT Act which is to regulate electronic commerce and not reform the law of evidence' and 'it would attribute to Parliament the intention to use detail buried in the ECT Act to bypass the wider debate about the admissibility of documentary evidence.'
[57] *Ndlovu's* case supra note 38 at 174.
[58] Hofman op cit note 51 at 472 argues for a 'restrictive interpretation' to the words 'in the ordinary course of business.'

proceedings under any law, the rules of a self regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of facts contained in such record, copy, printout or extract.'

Article 9 states:

'(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) on the sole ground that it is a data message; or,

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.'

The formulation of s 15(4) was most likely influenced by ss 221 and 236 of the Criminal Procedure Act 51 of 1977.[59] Section 221 provides for admissibility of certain trade or business records 'in criminal proceedings in which direct oral evidence of a fact would be admissible, *any statement contained in a document* and tending to establish that fact shall, upon production of the document, be admissible as evidence' provided that certain conditions are present.[60] The definition of 'document' in s 221(5) 'includes any device by which information is recorded or stored' and '"statement" includes any representation of fact whether made in words or otherwise.' Section 236 allows for the admissibility of accounting records and documents in the possession of a bank, including a computer printout or device that recorded or stored the document,[61] subject to the requisite supporting affidavits,[62] including an affidavit by a person stating that (a) they are in the service of the bank; (b) such accounting records and documents are the records of the bank; (c) the said entries or document have been made compiled, printed

[59] Hereafter 'CPA 1977'.
[60] As set out in s 221(1)*(a)* and *(b)* (emphasis added). For certain trade or business records to be admitted into evidence as proof of their contents if (a) the document is compiled in the course of that trade or business from information supplied by persons who have personal knowledge of the matters dealt with in the information supplied; and (b) the person who supplied the information recorded in the statement is dead, or is outside the country, or is unfit by reason of physical or mental condition to attend as a witness, or cannot be identified or found or cannot reasonably be expected to have any recollection of the matters dealt with in the information supplied.
[61] In terms of s 236(6), '"document" includes a recording or transcribed computer printout produced by any device by means of which information is recorded or stored.'
[62] Section 236(1) and (2).

or obtained in the usual and ordinary course of the business of the bank; and (d) such accounting records or documents are in the custody or under the control of such bank.

Although below I address concerns about the effect of s 15(4), and propose that it should be changed to incorporate a specific requirement that there must be some evidence of basic facts to demonstrate why a court should accept 'a data message made by a person in the ordinary course of business' that is 'certified to be correct' by an 'officer' of the business as 'proof of facts contained in such record, copy, printout or extract' – this is done so in the context of a consideration of evidential weight, not at the stage of admissibility. After all s 15(4) has the effect of making electronic hearsay evidence 'in the ordinary course of business' generally admissible, irrespective of hearsay representations contained therein. Hofman argues that if s 15(4) is interpreted as a broad exception for the admissibility of data messages, doing so would be contrary to the functional equivalence that 'should apply' between data messages and documents, and in his view 'Parliament would not have used detail in the ECT Act to make such a significant change to the law of evidence.'[63] Perhaps so on a restrictive interpretation. Although arguably, and more plausible, is that Parliament did so purposefully as s 15(4) goes beyond the 'safe harbour'[64] of the MLEC. Electronically stored information falling within the defined meaning of 'data message in s 1 of the ECT Act 2002 is admissible in evidence in terms of s 15 of the Act. As noted in *ABSA Bank Ltd v Le Roux And Others*: '[s]ection 15(4) has a twofold effect. It creates a statutory exception to the hearsay rule and it gives rise to a rebuttable presumption in favour of the correctness of electronic data falling within the definition of the term "data message".'[65] The court held that 'a proper construction' of subrule 32(2) of the Uniform Rules of Court 'does not preclude the deponent to the supporting affidavit from relying on hearsay evidence *to swear positively to the facts* when he could permissibly, as a matter of law, adduce such hearsay evidence for the purpose of proving the facts at a trial of the action.'[66] The court found that 'support of such a construction is made even stronger when there is a statutory presumption in favour of the correctness of such evidence':

> 'Thus, if the deponent to a supporting affidavit in summary judgment proceedings were to be able to aver that he is (i) an officer in the service of the plaintiff, (ii) that the salient facts—which should be particularised—are electronically captured and stored in the plaintiff's records, (iii) that he had regard thereto, (iv) that he is authorised to certify and has executed a certificate

[63] Hofman op cit cit note 51 at 472.
[64] Ibid at 471.
[65] 2014 (1) SA 475 (WCC) at 485.
[66] Supra note 65 at 485.

certifying the facts contained in such record to be correct, and (v) on the basis thereof is able to swear positively that the plaintiff will—having regard to the provisions of s 15(4) of Act 25 of 2002—be able to prove the relevant facts at the trial of the action by producing the electronic record or an extract thereof, the requirements of subrule 32(2)) [of the Uniform Rules of Court] would be satisfied.'[67]

In *Director of Public Prosecution v Modise*,[68] the court was also prepared to interpret s 15 as being widely stated in its intent:

'The sections in question (Section 212 of the Criminal Procedure Act [proof of certain facts by affidavit or certificate] and Section 15 of the Electronic Communications and Transactions Act) in their terms *are designed to and do allow evidence in the form of the facts and opinions contained in a document which complies with the section in question to be admitted in evidence at a trial* notwithstanding that the person who listed the facts and formed the opinions in the document is not called as a witness. This is the key which unlocks and solves the problem. The documents are not designed to be expert notices containing information designed to inform opposing parties of what the evidence to be led at the trial is. These sections are specifically designed to enable the state to avoid the need to lead the evidence of a witness by way of producing him and then leading viva voce evidence. The facts and matters in a document are the evidence. The evidence is admissible if the provisions of this section are complied with. Nothing more is required.'[69]

Notably while these two judgments apply to specific contexts of summary judgment and s 212 affidavits, I argue that the merits of the approach can be applied in general to the admission of hearsay electronic evidnece. Such a construction of s 15 of an inclusionary approach to electronic hearsay evidence, in my view, is significant and would certainly be advantageous in a year 2020 information age where the form of evidence in an electronic medium has now become widespread, not only in business but in every aspect of our daily lives. Doing so enables the state to easily produce evidence which will generally be of a formal and uncontested nature and to place it in documentary form before a criminal court without the need to call the witness. The advantage for criminal proceedings is immediately apparent by avoiding the 'concomitant waste of money and time' by having experts give evidence which is generally uncontested.[70] While a robust consideration of authentication is required, I believe

[67] Supra note 65 at 485. Cf *La Consortium & Vending* supra note 34 at 592, the court adopted a restrictive interpretation to s 15(4): '[i]t follows that, despite the very wide words of s 15(4), any hearsay contained in a data message must pass the criteria set out in s 3 of the Law of Evidence Amendment Act 45 of 1988.'
[68] 2012 (1) SACR 553 (GSJ).
[69] Supra note 68 at 557 (emphasis added).
[70] Supra note 68 at 557.

that it should not be subject stringent tests that makes it difficult for authentic electronic evidence to be admitted into evidence. As I shall attempt to show when I deal with electronic evidence as real evidence.

(b) Electronic evidence as real evidence

The central issue in a number of cases appears to be whether of electronic evidence should be dealt with as documentary evidence or as 'real evidence'. If s 15 does not make all electronic evidence admissible, and electronic evidence is considered the functional equivalent of documentary evidence, then in adopting this approach, the ordinary requirements of South African law of evidence for the admissibility of such evidence is that the document itself must be produced, which document, ordinarily speaking, must be the original, and the authenticity of the document must be proved.[71] These requirements are, of course, qualified by specific provisions of ECT Act 2002. For example, s 15(1)*(b)* gives electronic evidence an exemption from the requirements of producing the original 'if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.' In *Ndiki's* case,[72] during the course of a criminal trial the state sought to introduce certain documentary evidence consisting of computer-generated printouts. Van Zyl J set out the following approach for considering the admissibility of documentary evidence: 'determine the true nature of the computer print-outs in question, the class of documents they represent and whether the admissibility thereof is sanctioned by any of the provisions in the relevant legislation dealing with the admission of documentary evidence.'

In doing so case law has drawn a distinction between 'electronically generated' and 'electronically created' records,[73] the critical difference being whether the electronic evidence was generated purely by the wholly automated operation of a computer or device, or was created based on relaying information supplied by a person.[74] The ECT Act 2002 does not make such a distinction. There are some categories of electronic evidence that do not trigger

[71] See *Brown's* case supra note 30 at 214-15.
[72] *Ndiki's* case supra note 26 at 256.
[73] Schwikkard & Van der Merwe op cit note 28 at 445 use the term 'computer-generated' and 'computer-assisted' in reference to the distinction. See also JC Smith 'The admissibility of statements by computer' [1981] *Crim LR* 387 who prefers the terms 'direct computer evidence' and 'hearsay computer evidence' to describe this distinction in analysis.
[74] The term 'real evidence' is best described in *S v M* 2002(2) SACR 411 (SCA) at 413: '[r]eal evidence is an object which, upon proper identification, becomes, of itself, evidence (such as a knife, photograph, voice recording, letter of even the appearance of a witness in the witness-box).'

hearsay as an exclusionary rule of evidence. In these cases devices may as a result of internal processes create a record without human intervention or assistance and which is admissible as real evidence.[75] In *Ndiki's* case, the court held: '[e]vidence on the other hand that depends solely upon the reliability and accuracy of the computer itself and its operating systems or programs, constitutes real evidence. What s 15 of the ECT Act does, is to treat a data message in the same way as real evidence at common law. It is admissible as evidence in terms of ss (2) and the court's discretion simply relates to an assessment of the evidential weight to be given thereto (ss (3)). The ECT Act is therefore inclusionary as opposed to exclusionary.'[76] However, if there is human intervention or assistance in the performance of such processes either at the input, output or any intermediate stage, hearsay issues may arise, although in some cases exceptions to the hearsay rule may apply in terms of s 3 of the LEA 1988.[77] Electronic evidence which falls within the definition of hearsay evidence in s 3 of the LEA 1988, the provisions of which are described as operating 'exclusionarily',[78] may become admissible under s 3(1)*(c)* if the court having regard to the factors listed in that paragraph is 'of the opinion that such evidence should be admitted in the interests of justice.'

The categorisation of evidence as real or documentary has implications for admissibility: if deemed to be real evidence, then the test for admissibility is whether it is relevant; if however it is deemed documentary evidence, the ordinary requirements in the law of evidence for the admissibility of documents applies, including hearsay considerations. In *Ndlovu's* case, Gautschi AJ stated: 'in order to be admissible in evidence, [documentary evidence] generally has to comply with three rules: (a) the statements contained in the document must be relevant and otherwise admissible; (b) the authenticity of the document must be proved; and (c) the original document must normally be produced. Section 15(1) does not, in my view, do away with these three requirements. The data message must be relevant and otherwise admissible, be proved to be authentic and the original be produced, unless (in regard to the latter aspect) section 15(1)(b) applies.'[79] The court also took the view that s 3 of the LEA

[75] A third category exists, to the extent that a record may be comprised of information that is electronically generated and electronically created. For example, a suspect in a fraud case may use an Excel spreadsheet program to process financial figures relating to a fraudulent scheme. The electronic evidence as containing the output of the Excel program would derive from both the suspect's input into the program and the mathematical operations of the program automating calculations. Another example is that of an email message, where the automatically generated header as revealing the names of the sender/recipient, including time/date and other relevant metadata constitutes the electronically generated part of the communication. The content of the communication would be relaying information supplied by a person.
[76] *Ndiki's* case supra note 26 at 257-58.
[77] Supra note 26 at 264.
[78] Supra note 26 at 258.
[79] *Ndlovu's* case supra note 38 at 165-66.

Act 1988 did not apply to electronically generated records 'where the probative value of the evidence depends upon the "credibility" of the computer (because information was processed by the computer).' [80] In *La Consortium & Vending*, the court adopted the distinction 'electronically generated' and 'electronically created' records: '[t]he Oracle computer software system is, in addition, not merely utilised for storing information. It also creates additional information such as calculations as to what the appellant owes the respondent. This is real evidence the probative value of which depends on the reliability and accuracy of the computer and its operating systems.'[81] Although the court found that the electronic evidence relied upon in the case not only constituted real evidence, but also included hearsay, having applied the considerations in s 3 of the LEA 1988, the court found that the evidence relied upon was correctly admitted as evidence.[82] The 'task' of determining the admissibility of electronic evidence by distinguishing 'between what would constitute hearsay evidence and what real evidence' is one 'that is not always without its difficulties.'[83] In particular, the central issue of whether electronic evidence should more appropriately be dealt with as documentary evidence or as real evidence has challenged the courts.

Section 221(5) of the CPA 51 of 1977 provides that a document includes any device 'by means of which information is recorded or stored.' In *Seccombe and Others v Attorney-General* it was noted that the word 'document' is 'a very wide term and includes everything that contains the written or pictorial proof of something. It does not matter of what material it is made.'[84] On this definition, a data message as envisaged in s 15 could be a document.

The jurisprudence of the courts has evolved with the transition from analog to digital, albeit resulting in differing approaches to electronic evidence as a document or as real evidence in cases involving graphics, audio and video. In *S v Mpumlo & Others* it was held that a video film, like a tape recording, 'is real evidence, as distinct from documentary evidence, and,

[80] *Ndlovu's* case supra note 38 at 173. See also *S v Mpumlo & Others* 1986 (3) SA 485 (E) (video film); *S v Ramgobin* 1986 (4) SA 117 (N) (video tape recordings); *Mdlongwa v The State* (99/10) [2010] ZASCA 82 (31 May 2010)(video footage of the bank recorded during the robbery); *Motata v Nair NO* 2009 (2) SA 575 (T); *R v Cochrane* [1993] Crim LR 48 (ATM receipts); *R v Spiby* (1990) 91 Cr APP R 186 (CA) (records of a telephone metering device); *The Statue of Liberty* [1968] 1 WLR 739 (PD) (radar trackings); *R v Dodson and Williams* (1984) 79 Cr App R 220 (security camera photographs); *R v Wood* (1983) 76 Cr App R 23 (CA) (computer calculations of metal compositions); *Kajala v Noble* (1982) 75 Cr App R 149 (DC) (video recordings of camera output); *R v Maqsud-Ali* [1965] 1 WLR 1479 (CCA) (still photographs and audio recordings); *Castle v Cross* [1984] 1 WLR 137 (intoximeter breath test machines); *R v McCarthy and Others* [1998] RTR 374 (CLA) (DVLA computer records); *R v Clarke (Robert Lee)* [1995] 2 Cr App R 435 (CA) (facial mapping by way of video superimposition); *R v Reynard* [2005] EWCA Crim 550 (date/time stamp on emails).
[81] Supra note 34 at 594.
[82] Supra note 34 at 586 and 596.
[83] *Ndiki's* case supra note 26 at 265.
[84] 1919 TPD 270 at 277.

provided it is relevant, it may be produced as admissible evidence, subject of course to any dispute that may arise either as to its authenticity or the interpretation thereof.' [85] Similarly, in *Mdlongwa v The State*, the court held that 'video footage of the robbery constitutes real evidence.'[86] In *S v Baleka (1)* Van Dijkhorst J also held: 'I agree with the conclusions of Mullins J [in *Mpumlo*] that a video tape is real evidence.'[87]

In *S v Ramgobin*,[88] the court took a different approach in relation to whether certain audio and video tape recording are admissible evidence against the accused. The court was 'unable to agree' with the basis of the finding in *Mpumlo's* case that 'a video film like a tape recording is real evidence.' [89] The court held that for audio tape recordings and video tape recordings to be admissible in evidence in a criminal trial, it must be proved that the exhibits sought to be admitted: (i) are the original recordings and (ii) that, on the evidence as a whole, there exists no reasonable possibility of 'some interference' with the recordings.[90] Further:

> 'The State must also prove that the tape recordings (and video recordings) do relate to the occasion to which it is alleged they relate, and that they are faithful and prove the identity of the speakers. These requirements overlap to some extent but they are not identical. There may be proof that the tape has not been altered, added to, edited or in any way interfered with, but the tape may not be accurate because it fails to reflect faithfully what it purports to reflect, eg because of apparatus malfunction. In regard to the need for proof of accuracy, there must be a witness to the event purportedly recorded on the tape who testifies that it accurately portrays that event. It need not be the person who made the recording, but may be anyone who witnessed the event. A further requirement is that it must be proved that the tapes are sufficiently intelligible "to be placed before the jury", ie the Court.'[91]

Zeffertt and Paizes[92] support the stringent test for admissibility laid down in *Ramgobin* reflected in the tests set out above because tape recordings, 'can be altered (and materially altered) in such a way that even experts cannot detect the alteration.' These concerns also apply

[85] *Mpumlo's* case supra note 80 at 490.
[86] Supra note 80 para 25.
[87] 1986 (4) SA 192 (T) at 197.
[88] 1986 (4) SA 117 (N).
[89] Supra note 88 at 126, specifically the following statements of Mullins J in *Mpumlo's* case: '[a]t the time I gave my ruling in the present matter that the video film was admissible, there was, and still is, no evidence as to the last whereabouts of the original video film, or as to the correctness of the copy thereof used in Court. There may or may not be such evidence forthcoming later during the State case. I am satisfied however that even the lack of any such evidence would not affect the admissibility of the video films, but only if the authenticity thereof were attacked, the weight to be attached thereto.'
[90] Supra note 88 at 135.
[91] Supra note 88 at 118.
[92] *Ramgobin's case* supra note 88 at 121.

to electronic evidence. Hofman argues that graphics, audio and video that are in a data-message form should be treated in the same way as documents, and expresses the view that to regard such material as real evidence 'is conceptually simple and appeals to those who dislike excluding any evidence.'[93] He argues:

> 'In data message form, graphics, audio and video are susceptible to error and falsification in the same way as data messages that embody documentary content. They cannot prove themselves to be anything other than data messages and their evidential value depends on witnesses who can both interpret them and establish their relevance. So long as South African law follows an exclusionary approach it would seem that graphics, audio, and video that are in data message form should be treated in the same way as documents.' [94]

In such an approach electronic evidence is said to be 'dangerous from an evidential point of view unless certain precautions are taken.'[95] In *Brown's* case, the court's approach to images found in a cellphone reflects a guarded view on the admissibility of electronic evidence. Bozalek J held: '[g]iven the potential mutability and transient nature of images such as the images in this matter which are generated, stored and transmitted by an electronic device, I consider that they are more appropriately dealt with as documentary evidence rather than "real evidence".'[96] In *Ndiki's* case, although Van Zyl J found that 'the computer through its operating system processed existing information' which 'did calculations' and '"created" additional information without human intervention' constituted real evidence, the admissibility of this evidence would be 'dependent upon the *accuracy and the reliability* of the computer, its operating systems and its processes.'[97] In *S v Koralev and Another*,[98] it was held that having regard to 'the ease with which modern technology allowed such tampering to occur, it was essential that evidence in relation to such images be approached with extreme caution' The court endorsed an approach that required proof of accuracy in the form of corroboration that the event depicted had actually taken place.[99] The court held, that the images allegedly found on the appellant's computer were not the original images, since they were either downloaded from the Internet or transferred from a digital camera. The original images, therefore, would be those contained in the camera or in the original source from which they had been loaded

[93] Hofman op cit note 51 at 472-73.
[94] Ibid.
[95] *S v Baleka (3)* 1986 (4) SA 1005 (T) at 1023, reflecting the differing conclusion in *Ramgobin's* case.
[96] Supra note 30 at 214.
[97] *Ndiki's* case supra note 26 at 265 (emphasis added).
[98] 2006 (2) SACR 298 (N).
[99] Supra note 98 at 300.

onto the Internet site.[100] The absence of corroborating evidence together with evidence that at least one image was tampered with, the court found that the images failed to meet the requirements for admissibility.

The controversy in South African case law has resulted in the issues regarding admissibility of electronic evidence being approached from the premise of authenticity and integrity as a pre-requisite to admissibility. In my view, this is not an appropriate approach. Unlike its predecessor, the repealed Computer Evidence Act 57 of 1983 which required proof of authenticity as a condition of admissibility, the ECT Act 2002 does not require electronic evidence to be authenticated as a condition of admissibility. The approach of the ECT Act 2002 is preferred where issues regarding authenticity and integrity of the electronic evidence is central to an assessment of evidential weight, rather than its admissibility. In *S v Baleka (3)*[101] the court had the opportunity to consider the ruling on the admissibility of certain audio and video tape recordings in *Ramgobin*. Van Dijkhorst J stated: 'I deal with tape recordings as I would deal with any other type of real evidence tendered where its admissibility is disputed. The test is whether it is relevant. It will be relevant if it has probative value. It will only have probative value if it is linked to the issues to be decided.'[102] The court found that the stringent approach advocated by Milne JP in *Ramgobin* 'leads to the unacceptable situation that a court refuses to consider relevant evidence because it might be fabricated, where the correctness of that evidence is not even placed in issue in cross-examination, but only its admissibility.'[103] Further, as it was not put to any witness at any stage in the case that the tape recordings were not a true reflection of what had happened, or that the tape recordings had been tampered with, the court held that 'to exclude this evidence from consideration' would 'lead to a miscarriage of justice.'[104] In *S v Nieuwoudt*,[105] the Appeal Court endorsed the approach in *Baleka (3)*. The court had to determine whether it is necessary, for the admission in evidence of audio tape recordings, to prove the authenticity of the tape recording. The court held that although it can be accepted that interferences (deliberate or otherwise) are seemingly a cause for suspicion, and even though the evidential value thereof might be less than what it otherwise would have been, there can be no objection to the admissibility of the recording.[106]

[100] Supra note 98 at 300.
[101] Supra note 95.
[102] Supra note 95 at 1026.
[103] Supra note 95 at 1023.
[104] Supra note 101 at 1023.
[105] 1990 (4) SA 217 (A). See also *S v Fuhri* 1994 (2) SACR 829 (A).
[106] Supra note 105 at 232-33.

This preferred approach is aligned to the ECT Act 2002, which does not require as a condition of admissibility that electronic evidence be authenticated. Stringent tests relating to authenticity, integrity and truth or reliability of any information recorded in or reflected by the electronic evidence ought not apply for admissibility purposes.[107] I disagree with the view that graphics, audio and video in the form of electronic evidence should be treated in the same way as documentary evidence, and to be admissible it should be produced, be original and be authenticated. In the cases referred to earlier, records created by devices as a result of their own processes, without human intervention or assistance, constituted real evidence, however, there were differing outcomes on the need for proof of accuracy and the reliability as requirements for admissibility. I also disagree with the conclusions that where such electronic evidence is regarded as real evidence it should be subject to an approach inherent in the stringent test for admissibility as laid down by Milne JP in *Ramgobin*, because it is considered 'dangerous evidential material' due to the fact that it 'can be altered (and materially altered) in such a way that even experts cannot detect the alteration.'[108] Milne JP held that before the tape recording would be admissible the state had to prove beyond reasonable doubt: (i) that the recordings before court related to matters alleged in the indictment; (ii) by way of testimony of a witness who saw and heard the events allegedly recorded, that the recording accurately reflects the purported events; and (iii) that the tape recordings are the original recordings and have not been interfered with in any way, whether by mistake or otherwise, since the original recordings were made.[109]

In my view, the better approach to admissibility of electronic evidence is by Van Dijkhorst J in *Baleka (3)* who provided the following response and analysis to the advocated approach of Milne JP in *Ramgobin*. On the first test, it was agreed that to be admissible as real evidence, the electronic evidence must be relevant to the matter. However, that 'relevancy must be proved beyond reasonable doubt' was rejected – all that is needed in this respect, at admissibility stage of the proceedings, is that it be shown that prima facie the material tendered as evidence has some probative force.[110] On the second test of witness testimony, the view that, before a tape recording is admissible, a witness had to testify that he saw and heard the events allegedly recorded and that the recording accurately reflected those events, was also rejected as not correct. Van Dijkhorst J held that there was no apparent reason why that proof of

[107] See Zeffertt & DT Paizes op cit note 22 at 434.
[108] *Ramgobin's case* supra note 88 at 121.
[109] *Baleka (3)* supra note 95 at 1023, in summary by Van Dijkhorst J.
[110] Supra note 95 at 1023.

reliability and accuracy could only be furnished by viva voce evidence of a witness who saw and heard the events recorded – circumstantial evidence, after all, might, in a given case, lead to the same conclusion.[111]

On the third test, the view that, at the stage where admissibility was to be decided upon, it had to be proved beyond reasonable doubt that the tape recordings were originals, relates to the tape recordings being treated as documentary evidence.[112] Van Dijkhorst J found that the proposition that it has to be proved that the tapes have not been interfered with in any way, whether by mistake or otherwise, since the original recording was made, was too widely stated.[113] If this proposition applied, held Van Dijkhorst J it would lead to the whole tape being inadmissible, without any room for the court to determine whether this interference materially affected the recording as a whole.[114] It would be absurd, for example, to exclude a recording from which part of a conversation had been accidentally erased solely because of such defect. The better approach is that the remaining part of a recording from which a part has been erased without distorting the rest of the recording, may still admissible evidence (unless it is inadmissible on other grounds), even though the evidential value thereof might be less than what it otherwise would have been.[115]

Van Dijkhorst J concluded that the approach advocated by Milne JP in *Ramgobin* effectively 'leads to the unacceptable situation that a court refuses to consider relevant evidence because it might be fabricated' and 'where the correctness of that evidence' is 'placed in issue' only on its admissibility.[116] In keeping with my earlier submissions, s 15 should thus be interpreted in favour of its 'apparently expansive purpose'[117] as creating a single test of admissibility for all electronic evidence, whether in the form of documentary, hearsay or real evidence. The court's discretion would therefore be based on the scope of inquiry in s 15(1) to (3) and due evidential weight to be given to such evidence according to an assessment thereto having regard to certain factors.

[111] Supra note 95 at 1024-25.
[112] Section 15(1)(b) of the ECT Act 2002 now provides an exemption for the requirement of original.
[113] Supra note 95 at 1025.
[114] Supra note 95 at 1025.
[115] *Nieuwoudt's* case supra note 105.
[116] *Baleka (3)* supra note 95 at 1023.
[117] Zeffertt & DT Paizes op cit note 22 at 434.

IV EVIDENTIAL WEIGHT: NEW RULES ON AUTHENTICITY AND INTEGRITY

The basic requirements of admissibility for documentary evidence are not easily transferred to electronic evidence. They are production of the original document and authenticity. 'Authentication' involves demonstrating that the evidence sought to be adduced is what it purports to be. It requires:

> 'satisfying the court that (a) the contents of the record have remained unchanged, (b) that the information in the records does in fact originate from its purported source, whether human or machine, and (c) that extraneous information such as the apparent date of the record is accurate. As with paper records, the necessary degree of authentication may be proved through oral and circumstantial evidence, if available, or via technological features in the system or record.'[118]

Prior to the ECT Act, to authenticate electronic evidence in criminal proceedings it was necessary to demonstrate that the computer system or process that generated the evidence was working properly at all material times. Amongst other things that required proof of reliability, the proponent relying on electronic evidence was required to prove beyond reasonable doubt that at all material times the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation, was not such as to affect production of the document or accuracy of its contents before evidence from a computer could be admitted into evidence.[119] The ECT Act has altered the landscape, the focus of the debate is now on the long ignored issues relevant to establishing probative value or evidential weight of electronic evidence.

(a) The admissibility of business records in terms of s 15(4) – a problematic presumption?

Section 15(4) creates a statutory exception to hearsay as an exclusionary rule in favour of electronic evidence by making provision for 'a data message made by a person in the ordinary course of business' or for 'a copy or printout of or an extract from such data message' to be 'admissible in evidence' *and* creates a rebuttable presumption of 'proof of facts contained in such record, copy, printout or extract' as 'certified to be correct'. As noted earlier, the formulation of s 15(4) is most likely influenced the business records exceptions in s 221 (business records) and s 236 (banking records) of the CPA 51 of 1977. The application and

[118] C Reed & L Davis 'Electronic Commerce' in C Reed and J Angel (eds) *Computer Law* (2000) 303 at 308.
[119] Prior to the ECT Act 2002, electronic evidence in South African law was regulated by Computer Evidence Act 57 of 1983.

interpretation of s15(4) by the courts can be described as straightforward and uncomplicated.[120] It was observed in *Ndlovu's* case that s 15(4) provides for two situations in which electronic evidence, on its mere production, may be admissible:

> 'Section 15(4) provides an exception to the manner of proof and evidential weight ordinarily to be accorded to a data message. Section 15(4) provides for two situations in which a data message may on its mere production be admissible in evidence. *The first is "a data message made by a person in the ordinary course of business"*, which, juxtaposed with the words that follow, clearly refers to an original data message, and is required to have been made "in the ordinary course of business". *The second is a copy or printout of or an extract from such data message which is certified to be correct by an officer in the service of such person* (being a person who made the data message in the ordinary course of business). *Once either of these two situations is present, the data message is on its mere production admissible in evidence and rebuttable proof of the facts contained therein.* Section 15(4) appears to be self-contained, and does not admit of or require a qualitative enquiry to be made in terms of sections 15(2) or (3) in regard to the weight to be attached thereto. It provides for its own weight, namely that the facts contained therein will be rebuttable proof, ie if not rebutted, then they will stand as evidence.'[121]

If s 15(4) is regarded as 'self-contained' such that 'the fact contained therein will be rebuttable proof' and 'if not rebutted' the electronic record 'will stand as evidence', arguably the presumption may be difficult to rebut because the party seeking to contest the presumption will often not be in a position to challenge or offer substantial evidence to the contrary. [122] Generally it is difficult to overcome the presumption, and assertions by the proponent seeking to rebut the presumption by casting doubt on the 'correctness' of 'proof of facts' relied upon, are often made without providing any foundation for the allegations.[123] In most cases, the party facing the challenge will be in full control of the computer software or systems.[124] In the absence of evidence to the contrary, the court will generally rely on the correctness of the record, copy, printout or extract. Understandably the aim of the presumption seeks to address the previous situation in law that sought to exclude electronic evidence because the disputed

---

[120] In *Golden Fried Chicken (Pty) Ltd v Yum Restaurants International (Pty) Ltd* 2005 BIP 269 (T) at 272: '[i]n terms of s 15(4) of that Act a printout of a data message can constitute prima facie proof if the data message was made by a person in the ordinary course of business and if the printout is certified to be correct by 'an officer in the service of such person.'

[121] *Ndlovu's* case supra note 38 at 172-73.

[122] S Mason 'Electronic evidence: A proposal to reform the presumption of reliability and hearsay' 30 (2014) *Computer Law and Security Review* 80 at 81.

[123] *La Consortium's* case supra note 34 at 594.

[124] See S Mason 'The presumption that computers are "reliable"' in S Mason & D Seng (eds) *Electronic Evidence* 4ed (2017) 101.

documents contained information which had been processed by a computer. The rationale for the presumption also alleviates the need to prove every item of evidence produced 'in ordinary course of business' to save 'the time and expense of proving the obvious.'[125] However, it does not necessarily follow that the function 'by a person in the ordinary course of business' is always performed correctly or as one would normally expect in a situation where the function is mediated by electronic systems and software.[126] Van Buskirk and Liu argue that such a presumption is often difficult to rebut and note the following implications of an approach akin to an 'aura of infallibility':[127]

> 'Unless specific evidence is offered to show that the particular code at issue has demonstrable defects that are directly relevant to the evidence being offered up for admission, most courts will faithfully maintain the Presumption of Reliability. But because most code is closed source and heavily guarded, a party cannot audit it to review its quality. At the same time, however, source code audits are perhaps the best single way to discover defects. This difficulty gives rise to an important question: if a party cannot gain access to source code without evidence of a defect, but cannot get evidence of a defect without access to the source code, how is a party to rebut the Presumption? Rather than wrestle with, or even acknowledge, this conundrum, most courts simply presume that all code is reliable without sufficient analysis.'[128]

Specifically on the application of s 15(4), Hofman also raises the following concerns, including potential constitutional law challenges:

> '(a) First, an exception for communications made 'in the ordinary course of business' is much wider than the previous business record exceptions. Taken at face value, this exception could apply to any email or even a recorded voice message made in the course of business.
>
> (b) Second, s 15(4) is not only wider in scope than the previous business records exceptions, it differs from all of them (although not the exceptions for banking records) in making data messages not only admissible as evidence but also rebuttable proof of facts they contain. Attaching a probative value to bank records is acceptable because banks are regulated and supposedly responsible institutions whose records can be assumed to be reliable in much the way as the records of a public body. However, s 15(4) applies to records of any business is no guarantee that the records of that business are kept accurately or honestly.

[125] Ibid at 102 quoting *Holt v Auckland City Council* [1980] 2 NZLR 124 at 128.
[126] Ibid at 107.
[127] DW Elliott 'Mechanical aids to evidence' 1958 *Criminal LR* 5 at 7.
[128] E van Buskirk & VT Liu 'Digital evidence: Challenging the presumption of reliability' 1.1 (2006) *Journal of Digital Forensic Practice* 19 at 20 (footnotes omitted).

(c) Third, s 15(4) requires a certificate 'by an officer in the service of such person' for data messages to be admissible. This imposes less responsibility than the affidavit previously required for banking exceptions. There is also no need for the certificate to assert, as required in an affidavit, that the records have been under the control of the business.

(d) Fourth, if the person wanting to submit this form of evidence does not control the computer system which contain it, it may be difficult to get the certificate required to make the evidence admissible.

(e) Fifth, the wide range of evidence that s 15(4) makes admissible could lead courts to being asked to consider much larger volumes of evidence than at present.

(f) Sixth, when applied in a criminal prosecution, for which s 15(4) explicitly provides, the presumption of truth the section creates is open to constitutional challenge as an unjustified shifting of the onus of proof onto the accused.'[129]

These are valid concerns raised by Hofman. On his first and second point, the s 15(4) presumption is particularly relevant with regard to banking and also illustrates the nature of the problem. As set out by Mason: '[t]hat a bank benefits from the presumption that its computers and networks … puts an impossible burden on the customer. For a customer in dispute with his bank to challenge this presumption, he will require significant knowledge of the computers, systems and networks operated by the bank, how they work, and where the vulnerabilities might lie, including the results of relevant audits, both internal and external – a task well beyond the vast majority of customers, including most lawyers without the benefit of expert advice, which in itself is difficult to obtain.'[130] The nature of the problem is not limited to banking, as s 15(4) as a business exception applies to electronic records 'made in the ordinary course of business' – of *any* business.

Another problem with the s 15(4) presumption that deems electronic records made 'in the ordinary course of business' that is 'certified to be correct by an officer' of a business, admissible as 'proof of facts contained in such record, copy, printout or extract' is that there is no authoritative guidance to the meaning of the words 'certified to be correct' in the context of electronic evidence. It is presumed that because a 'record, copy, printout or extract' contains information that the 'officer' of a business might expect to see, it follows that the information recorded is 'certified to be correct'. However, information contained in 'such record, copy,

[129] Hofman op cit note 51 at 471-72 (footnotes omitted). See also Zeffertt & Paizes op cit note 22 at 434 and 852 who also address the concerning constitutional issues of s 15(4).
[130] Mason op cit note 124 at 158.

printout or extract' does not necessarily demonstrate that the information recorded is 'correct' and therefore to be readily accepted and trusted by the courts. 'This is an important issue' argues Mason 'bearing in mind that the presumption is a presumption without the requirement of proof of a basic fact.'[131] As also rightly noted by Hofman there 'is no guarantee that the records of that business are kept accurately or honestly.'

On Hofman's sixth point and the shifting of the onus of proof to the accused in criminal proceedings, a problematic issue with the presumption in s 15(4) is that it 'asserts something positive.'[132] The presumption acts to place an evidential burden on an opposing party, in this instance, an accused person contesting reliance on the presumption. It can be difficult to raise sufficient evidence to shift the burden. Can the opposing party seeking to challenge the presumption in s 15(4) convince a court to order the production of the relevant electronic evidence, including software code and operating system, if the 'certified to be correct' electronic evidence is to be tested properly? The opposing party is 'required to prove a negative in the absence of relevant evidence from the program or programs that are relied upon.'[133] In criminal proceedings, for an accused person 'this has the unfair effect of undermining the presumption of innocence.'[134]

However, does s 15(4) shift the onus of proof or does it merely place an evidential burden on the party against whom the evidence is admitted? There is clear authority in our jurisprudence for the view that the presumption of innocence will be infringed whenever there is the possibility of a conviction despite the existence of a reasonable doubt.[135] While several rebuttable presumptions of law which placed a burden of proof on the accused have been declared unconstitutional,[136] a distinction must be drawn between placing an evidential or legal burden on the accused. The Consititutional Court has held that an evidentiary burden does not create the possibility of conviction despite the existence of a reasonable doubt, and therefore

[131] Ibid at 172.
[132] Ibid at 183.
[133] Ibid.
[134] Ibid.
[135] See *Prinsloo v Van der Linde and Another* 1997 (3) SA 1012 (CC); *Minister of Safety and Security v Sekhoto and Another* 2011 (1) SACR 315 (SCA); *S v Coetzee and Others* 1997 (3) SA 527 (CC).
[136] In *S v Zuma and Others* 1995 (1) SACR 568 (CC), the Constitutional Court held that the effect of the presumption contained in s 217(1)*(b)(ii)* of the CPA 51 of 1977 to place a burden on the accused to prove a fact on a balance of probabilities, breached the constitutional right to be presumed innocent. In *S v Bhulwana; S v Gwadiso* 1996 (1) SA 388 (CC), the Constitutional Court found unconstitutional the presumption contained in s 21(1)*(a)(i)* of the Drugs and Drug Trafficking Act 140 of 1992. In *S v Ntsele* 1997 (2) SACR 740 (CC), s 21(1)*(b)* of the Drugs and Drug Trafficking Act was held unconstitutional; in *S v Mello and Another* 1999 (2) SACR 255 (CC) s 20 of the Drugs and Drug Trafficking Act was struck down by the Constitutional Court. In *S v Mbatha; S v Prinsloo* 1996 (1) SACR 371 (CC) the Constitutional Court held s 40(1) of the former Arms and Ammunition Act 75 of 1969 unconstitutional.

will not infringe the presumption of innocence.[137] Arguably, if the wording in s 15(4) that 'a data messge … is on its mere production … admissible in evidence against any person and rebuttable proof of facts contained' therein were to be generally considered as imposing no more than an evidentiary burden on the accused, then such an evidentiary burden merely requies 'evidence sufficient to give rise to a reasonable doubt to prevent conviction'[138] which unlike a legal burden does not create the possibility of conviction despite the existence of a reasonable doubt.[139]

A particular challenge in applying the s 15(4) presumption is that the working accuracy of a computer or similar devices used to create a 'a data message made by a person in the ordinary course of business' is also presumed. Where a proponent is seeking to rely on the s 15(4) presumption they would not need to lead evidence that the computer or similar devices used to create the electronic evidence 'made by a person in the ordinary course of business' was working properly at the time in question, unless there was evidence that it may not have been, in which case the proponent will need to prove that it was working properly. What this means is that in the absence of evidence to the contrary, the court will be asked to rely on the correctness of the 'proof of facts contained in such record, copy, printout or extract' that had been made 'in the ordinary course of business' as it was 'certified to be correct by an officer' of the business. The s 15(4) presumption appears to be reflective of the Latin expression 'omnia praesumuntur rite esse acta' which means 'all acts are presumed to have been done rightly and regularly' or 'all things are presumed to have been done regularly and with due formality until the contrary is proved.'[140] As noted earlier, it was observed in *Ndlovu's* case that s 15(4) 'appears to be self-contained, and does not admit of or require a qualitative enquiry to be made in terms of sections 15(2) or (3) in regard to the weight to be attached thereto.'[141] The idea of 'certified to be correct by an officer' of the company relies on the assumption that concerns about the proper operation of the computer or similar devices are 'reasonably rare'.[142] This view is problematic as being 'incomplete' and 'misleading' because 'accurate computer output depends not just on the proper operation of computers, but also proper human use (or abuse) of computers.'[143]

---

[137] *Scagell and Others v Attorney-General of the Western Cape and Others* 1997 (2) SA 368 (CC).
[138] Supra para 12.
[139] Schwikkard & Van der Merwe op cit note 28 at 555-56.
[140] Ibid at 83.
[141] *Ndlovu's* case supra note 38 at 173.
[142] Mason op cit note 124 at 113.
[143] DB Seng 'Computer output as evidence' (1997) *Singapore Journal of Legal Studies* 130 at 167.

The presumption in s 15(4) should be reconsidered. A rethinking of the articulation of the 'in the ordinary course of business' presumption should be linked to evidential foundations of the presumption in order to be 'certified to be correct'. In other words, for such a presumption to be recognised, it should be necessary for the proponent seeking to benefit from the presumption to adduce sufficient evidence, that is proof of basic facts, to warrant the introduction of such a presumption.[144] In non-presumption cases involving electronic evidence, the courts have referred to computer software system reliability. For example, in *La Consortium & Vending*, the court accepted the 'correctness' of 'an accounting software package known as the Oracle Accounting System.'[145] The court was satisfied with testimony 'as to the integrity of the system [and that] the system was audited on a regular basis by both the respondent's internal auditors as well as external auditors.'[146] The court's assessment of the electronic evidence concluded as follows:

> 'The Oracle software system, manages a particular customer (in this instance the appellant) at every step of the process. The respondent led evidence concerning the reliability of the manner in which the data messages was generated, stored or communicated; the reliability of the manner in which the integrity of the data messages was maintained; the manner in which its originator was identified. These aspects were not challenged by the appellant under cross-examination, and no evidence was led by the respondent in this regard. The Oracle computer-software system is, in addition, not merely utilised for storing information. It also creates additional information, such as calculations as to what the appellant owes the respondent. This is real evidence, the probative value of which depends on the reliability and accuracy of the computer and its operating systems. Nor does there appear to be any cogent reason to suppose that any of the computer entries relating to, for example, the orders placed, were incorrect.' [147]

I believe that the presumption in s 15(4) should not operate as a 'self-contained' section.[148] Consideration must be given to more fully understanding meaning of the words 'certified to be correct'. This means that a party seeking to rely on the presumption in s 15(4) should establish what they mean by electronic evidence 'certified to be correct' made 'in the ordinary course of business'. In *Castle v Cross*,[149] Stephen Brown LJ's preference for the presumption was in the cited formulation in *Cross on Evidence* which 'requires the basic fact

[144] Mason op cit note 124 at 112.
[145] Supra note 34 at 580. Part V below expands further on new rules for authenticity and integrity of electronic evidence.
[146] Supra note 34 at 580.
[147] Supra note 34 at 594.
[148] *Ndlovu's* case supra note 38 at 172-73.
[149] [1984] a WLR 1372.

– proof that the instrument be one of a kind which is common knowledge that they are more often than not in working order – to be established before the presumption could operate.'[150] The prosecution sought to rely on the presumption that intoximeter breath test machines were in order when they were used:

> 'A presumption which serves the same purpose of saving the time and expense of calling evidence as that served by the maxim omnia praesumuntur rite esse acta is the presumption that mechanical instruments were in order when they were used. In the absence of evidence to the contrary, the courts will presume that stopwatches and speedometers and traffic lights were in order at the material time; *but the instrument must be one of a kind which it is common knowledge that they are more often than not in working order*.' [151]

It is not my intention in the suggested rethinking of the s 15(4) presumption that the proponent seeking to benefit from the presumption will be required to prove the authenticity and integrity of every item of evidence produced 'in ordinary course of business'. The suggested proposal of rethinking the presumption in s 15(4) will be useful for cases involving electronic evidence that originates from complex networked systems, or where such evidence is several times removed from the device.[152] Just because a business or an industry such as banks rely on electronic records 'made in the ordinary course of business' where the function is mediated by operating systems and software does not necessarily mean that the courts should readily accept the 'certified to be correct' by the 'officer' of the business as 'proof of facts contained in such record, copy, printout or extract'. A failure to provide for proper scrutiny of 'such record, copy, printout or extract' and emphasis on the s 15(4) presumption by relying on the assurances of 'an officer' of a business effectively means that 'certified to be correct' cannot be readily challenged in South African courts.

It is argued that s 15(4) should be changed to incorporate a specific requirement that there must be some evidence of basic facts to demonstrate why a court should accept 'a data message made by a person in the ordinary course of business' that is 'certified to be correct' by an 'officer' of the business as 'proof of facts contained in such record, copy, printout or extract'. Evidence of 'correctness' will not always be required. However, suitable procedural mechanisms can be put in place to allow a party to require relevant evidence of 'correctness'

---

[150] Mason op cit note 124 at 110.
[151] Supra note 149 at 1377 citing *Cross on Evidence* (1979) (emphasis added). Cf *R v Governor Ex p Osman (No 1), sub nom Osman (No 1), Re* [1989] 3 All ER 701, Lloyd LJ stated: '[w]here a lengthy computer printout contains no internal evidence of malfunction, and is retained, e.g. by a bank or a stockbroker as part of its records, it may be legitimate to infer that the computer which made the record was functioning correctly.'
[152] Mason op cit note 124 at 110.

where it is challenged and argued that the proponent of the evidence should not benefit from the presumption in s 15(4).[153]

(b) Evidential weight of electronic evidence

A data message must according to s 15(2) of the ECT Act 2002 be given 'due evidential weight'. In assessing the evidential weight of a data message, s 15(3) of the Act requires that regard must be had to 'the *reliability* of the manner in which the data message was generated, stored or communicated'; 'the reliability of the manner in which the *integrity* of the data message was maintained'; 'the manner in which its originator was identified' and 'any other relevant factor.' The manner in which the technology is operated may have an impact on the weight to be attributed to its output such that the evidential value thereof might be less than what it otherwise would have been. As such, the probative value of the electronic evidence is applicable to the s 15(3) considerations particularly those relating to the manner in which the electronic evidence 'was generated, stored or communicated' and the reliability of the manner in which its integrity was maintained.[154] As regards the assessment of the evidential weight of a data message, the use of terms such as 'integrity' and 'reliability' referred to in s 15(3) to an extent go beyond a simple showing chain of custody to demonstrating that the electronic evidence was 'generated, stored or communicated' within a reliable system or process:

> '*Integrity*: this relates to how sound the data is, such as whether the data is damaged in some way, and whether it is complete, in that it possesses all the necessary parts and links. Integrity is not an absolute condition, but is a state of relationships, and whether the burden of proof will be achieved in any individual case will depend on the strength of the relationships to the data.
>
> *Reliability*: this is the capacity of a digital object to stand for the facts to which it purports to attest, which in turn is linked to ensuring sufficient procedural and technical attributes (including a combination of preventative measures, such as to prevent unauthorized amendments and changes, and verification measures to provide for a degree of assurance as to the identity of users and the provision of audit trails to the document when data is viewed and manipulated) are in place and working to provide for a degree of assurance that the digital

[153] Ibid at 192.
[154] See *La Consortium & Vending* supra note 34.

object can be deemed to be reliable. In essence, reliability is associated with the degree of control exercised over the procedures that permit the data to be created. It is not absolute.'[155]

In *Firstrand Bank Limited v Venter*, the court considered s 15(3) of the ECT Act 2002, the appellant (the bank) sued the respondent (Mr Venter) in the magistrate's court for the balance of an overdrawn current account together with interest.[156] The bank relied on the evidence of the bank manager who allegedly concluded an oral agreement to open the respondent's current account. Its only other witness was Ms Cawood, a commercial recovery analyst, employed by the bank in the recoveries department, and who produced and spoke to a certificate signed by herself in purported compliance with s 15(4) of the ECT Act 2002.[157] The magistrate gave judgment for the bank. Mr Venter appealed, successfully, to the North Gauteng High Court. The principal findings of the court a quo included inter alia: (i) the bank manager was 'not a credible witness at all. He blatantly lied at stages and he was evasive and vague on aspects he as bank manager should have been acquainted with'; (ii) the bank did not 'succeed in proving the correct amount of its claim against Mr Venter either as to capital or interest'; and (iii) the evidence of Ms Cawood was 'confusing' and 'insufficient to identify Mr Venter's bank account or the entries in it, and did not establish that the bank statements on which the bank relied had been prepared by any person on its behalf or had been computer-generated as contemplated in the Act.'[158] On appeal by the bank, the order of the court a quo in favour of Mr Venter was set aside, and it was held that 'the magistrate's approach … was correct and the appeal to the high court should not have succeeded.'[159] In assessing the weight to be attached in the application of s 15(3))*(a)*, *(b)* and *(c)*, the Supreme Court of Appeal Court found the following of relevance to the Bank successfully establishing the quantum of its claim as computed: '(1) the bank sent monthly statements detailing the state of the account to Mr Venter; (2) [Mr Venter], as he conceded, received the statements and perused them carefully; he did not testify that the statements differed in any way from those proved by Ms Cawood nor did he claim that any part was overlooked or unintelligible to him; (3) each month's statement contained details of all debits and credits including his overdraft limit, bank costs, credit and debit interest rates on balances, VAT, service fees, ATM charges and cash handling and deposit

[155] S Mason & A Stanfield 'Authenticating electronic evidence'in S Mason & D Seng (eds) *Electronic Evidence* 4ed (2017) 193 at 195-96 (emphasis in original text).
[156] Supra note 44 para 3.
[157] Supra note 44 para 3.
[158] Supra note 44 para 4.
[159] Supra note 44 para 17.

fees; (4) the defendant did not query any aspect of the account until long after the event, subject to what I shall have to say below.'[160]

A valid challenge to evidential weight may render the electronic evidence inadmissible, just as a robust defence of evidential weight of electronic evidence may preserve its admissibility.[161] Challenges to evidential weight can include that the records have not remained 'complete and unaltered' from 'the time when it was first generated in its final form'[162] as evidence; concerns regarding the reliability of the system or process that 'generated, stored or communicated' [163] the electronic evidence; or disputing the identity of the author or 'originator'[164] of the electronic evidence.[165] In assessing evidential weight in terms of s 15, a court may well rely on expert evidence.[166] The court may also take upon the role of setting out instructions, in detail the nature of the action, a proponent of electronic evidence ought to undertake to establish evidential weight of electronic evidence. For example, the instructions set out, in a United States District Court, by Catoe MJ in *Koosharem Corporation v SPEC Personnel, LLC*[167] are a useful guide. The court ordered a forensic examination of business and personal computers in a lengthy and detailed 20-point court issued protocol as a result of incomplete responses to discovery requests and contentions of irregularities in the emails that were produced that called into question the authenticity of the documents. The defendants produced approximately 1,936 pages of emails in response to the plaintiffs' discovery requests. According to the plaintiffs, many emails were missing their attachments and further it was contended 'that not a single email produced by the defendants was an accurate copy of the original email, as the date and time stamp on every email had been modified to reflect the dates the emails were compiled rather than the dates they were sent.'[168] The court agreed with the plaintiff's motion for a forensic analysis and set out, inter alia, the following procedure for conducting the requested discovery and forensic analysis: (a) forensic analysis and data recovery to be conducted by an expert forensics firm; (b) the expert will conduct a search or run other appropriate programs to determine whether any emails or documents have been

[160] Supra note 44 para 7.
[161] Mason & Stanfield op cit note 155 at 196.
[162] Section 14, ECT Act 2002.
[163] Section 15(3)*(a)*, ECT Act 2002.
[164] Section 15(3)*(c)*, ECT Act 2002.
[165] Mason & Stanfield op cit note 155 at 196-97.
[166] See *Jafta v Ezemvelo KZN Wildlife* (2009) 30 ILJ 131 (LC) where the court considered the evidence of experts in the context of s 15 of the ECT Act 2002.
[167] United States District Court, D. South Carolina, Greenville Division Sep 29, 2008 Civil Action No. 6:08-583-HFF-WMC (D.S.C. Sep. 29, 2008).
[168] Supra note 167 at 3-4.

deleted, destroyed, altered, or otherwise compromised and whether any programs have been installed that would alter, destroy, erase, modify, or otherwise compromise any portion of each computer or its contents for the specified period; (c) the expert will securely maintain the original data recovered in order to establish a chain of custody; (d) the expert will recover only the documents and email account or accounts used by individuals identified; (e) defendants' counsel will review the data to identify any privileged or personal emails that it seeks to withhold from document production.[169]

In certain defined circumstances, proof of facts by way of affidavit or certificate may also assist the court in assessing evidential weight. Some guidance can be obtained from South African case law dealing with accuracy and reliability of instruments such as those involving speed-trapping and breathe analyses. There are conflicting decisions, for example, as to how the accuracy of a gas chromatograph may be proved, and if the state may prove the accuracy of a gas chromatograph by way of a certificate in terms of s 212(4) of the CPA 51 of 1977. In *S v Ross*,[170] Bozalek J held that proof of the proper calibration of the measuring instrument used could not be proved in terms of a 212(4) affidavit. In *S v Van der Sandt*,[171] the court took a more judicious approach with a finding that s 212 (4) allows for the admission of an affidavit or certificate as prima facie proof of the facts stated therein:

> 'The section does not contain any indication that the requirements of proof of trustworthiness and correctness have thereby been jettisoned. There is no reason to do so. The purpose of the section is to obviate viva voce evidence in every case where this type of evidence is necessary, not to introduce a new type of evidence, viz expert factual evidence of a result without explanation or clarification. As stated in *S v Dickenson* (supra at 96A – C) this is not opinion evidence where the facts upon which the opinion is based must be set out with such detail as to enable the court to draw its own conclusion. Nevertheless an expert who utilises an instrument of measurement which is outside the scope of judicial notice should name it and explain its operation and why it is trustworthy. Proof of reliability can be dispensed with in cases where there is a high degree of likelihood that the machine is accurate or because it has been tested. Where the test entails the use of a yardstick, proof that it has been assized is normally accepted as evidence of correctness thereof. *S v Mthimkulu* (supra at 763G – 764G).'[172]

[169] Supra note 167 at 3-4.
[170] 2013 (1) SACR 77 (WCC).
[171] 1997 (2) SACR 116 (W).
[172] Supra note 171 at 133.

On the issue of whether the certificate must deal with the calibration of the instrument used against assized units of measure, Van Dijkhorst J held:

> 'A court of law should be practical. If a court can take judicial notice of hearsay evidence about assized scales, as was done in *S v Mthimkulu* (supra), there can be no serious objection to judicial notice of the fact that there is a high likelihood that scientists in designated government laboratories when calibrating their instruments will do so against correct standards. The mere allegation of proper calibration will in my view be adequate prima facie proof thereof. This conclusion is in conformity with the wording of s 212(4) which requires no more than that the process be set out.'[173]

The interpretation by Van Dijkhorst J is correct, and was appropriately followed in *S v Eke*.[174] The appellant on a charge of drunk driving challenged the accuracy and reliability of the blood specimen measurement process; namely, whether the instruments used to analyse the blood sample (gas chromatographs) had been properly calibrated before the sample was analysed. The appellant's challenge was dismissed in the absence of evidence to rebut or challenge the certificate, its contents, having been prima facie proof, became conclusive proof.[175] The court held that appellant must adduce evidence to counter the prima facie value of evidence provided by the state.[176] The court noted that s 212 provided three cogent routes to do so: (a) she could have applied to the court below to exercise its discretion in terms of s 212(12) to have the analyst subpoenaed to give oral evidence; (b) she could have herself subpoenaed the analyst to testify; and (c) if she had a factual basis to cast doubt on the accuracy of the result (that it could not be accurate because she consumed no alcohol at the time) she could have testified or called witnesses.[177]

The court may also rely on technical processes as a means of assessing integrity and reliability. In determining whether the proponent of electronic evidence has met the evidential

---

[173] Supra note 171 at 136.
[174] 2016 (1) SACR 135 (ECG).
[175] In *S v Britz* 1994 (2) SACR 687 (W), Eloff JP held that the mere fact that the appellant challenged the correctness of a s 212(4) certificate 'is not sufficient to affect the prima facie value of the certificate', and that the weight of the s 212(4) certificate 'is only affected if there is proof to the contrary. The appellant has to adduce evidence to counter the prima facie value of the certificate.' (at 690).
[176] As referred in support in *Eke's* case, in *Ex parte the Minister of Justice: In re R v Jacobson and Levy* 1931 AD 466 at 478-79, Stratford JA held: 'Prima facie evidence in its usual sense is used to mean prima facie proof of an issue, the burden of proving which is upon the party giving that evidence. In the absence of further evidence from the other side, the prima facie proof becomes conclusive proof and the party giving it discharges his onus.' Further, in *S v Veldthuizen* 1982 (3) SA 413 (A) at 416, Diemont JA held that the words 'prima facie evidence' used in s 212(4) were not to be 'brushed aside or minimised' and that they meant 'that the judicial officer will accept the evidence as prima facie proof of the issue and, in the absence of other credible evidence, that that prima facie proof will become conclusive proof.'
[177] *Van der Sandt's* case supra note 171 at 146-47.

foundations of authenticating the evidence, a range of factors may need to be taken into account by the court, covering some or all of the technical processes associated with the preservation of electronic information.[178] Authentication rests on being able to prove that the electronic evidence is what it purports to represent 'and that it has not been altered or corrupted in such a way as to invalidate its evidential meaning.'[179] The technical aspects of proving the evidential weight of electronic evidence on Rothenberg's 'archival principle of provenance' means to provide 'evidence of their origin, authorship, and context of generation, and then by proving that the records have been maintained by an unbroken chain of custodianship in which they have not been corrupted.'[180] Rothenberg's proposition is based on two conditions: 'first, that an unbroken chain of custodianship has been maintained; and second, that no inappropriate modifications have been made to the records during that custodianship.'[181] He points to the challenges:

> 'The first of these conditions is only a way of supplying indirect evidence for the second, which is the one that really matters. An unbroken chain of custodianship does not in itself prove that records have not been corrupted, whereas if we could prove that records had not been corrupted, there would be no logical need to establish that custodianship had been maintained. However, since it is difficult to obtain direct proof that records have not been corrupted, evidence of an unbroken chain of custodianship serves, at least for traditional records, as a surrogate for such proof.' [182]

On the second of the two conditions above, that 'no inappropriate modifications' have been made to electronic evidence, a question that arises in the court's assessment of evidential weight: will circumstantial indicators of authenticity suffice, or is more conclusive proof required for evidential weight in the assessment of reliability as it relates to the manner in which the electronic evidence was 'was generated, stored or communicated' and 'the manner in which the integrity' of electronic evidence was maintained?[183] In my view, the threshold for evidential weight must be the same as for any other form of evidence: there must be prima facie evidence to support the claim.[184] It is an issue that must be determined on the fact of each case, after all, the nature of evidence available to a court to make a determination on evidential

[178] Mason & Stanfield op cit note 155 at 199.
[179] J Rothenberg 'Preserving authentic digital information' (2000) available at *https://www.clir.org/pubs/reports/pub92/rothenberg/*, accessed 21 July 2019.
[180] Ibid at 57.
[181] Ibid at 57.
[182] Ibid.
[183] As envisaged in s 15(3) of the ECT Act 2002.
[184] Mason & Stanfield op cit note 155 at 233.

weight will differ from case to case: [f]or instance, the print-out from a mainframe computer will demand a different approach in comparison to the data held on a personal computer; this in turn will be different if data is stored with a cloud service provider. The mainframe computer cannot be removed, so reliance must be placed on the print-outs and relevant expert evidence, which in turn raises the question of how is the reliability of the mainframe to be tested.'[185] It is not always necessary to obtain 'intricate details' of a computer or similar device and its operating system before electronic evidence may be accepted into evidence, and the means by which the evidence is authenticated may not necessarily require the evidence of a qualified expert.[186]

Proving evidential weight of electronic communications is possible through the use of compelling circumstantial evidence. Circumstantial evidence of the evidence itself has been frequently used to authenticate email, as the content of what the email says can often authenticate it.[187] Another way of locating circumstantial evidence of the electronic evidence itself is by certain technical processes associated with the record. This involves unique identifiers attached to electronic information which also provides distinguishing information about the electronic evidence that can be used to verify, or challenge claims of reliability and integrity. This includes, for example, hash marks and time/date-stamps.[188] To an extent, the

[185] Ibid at 277.

[186] Ibid at 216. As in the case of *DPP v Brian Meehan* 1 [2006] IECCA 104, [2006] 3 IR 468, the Republic of Ireland Court of Appeal was satisfied that electronic evidence in the form of records of telephone calls made and received was authenticated by appropriate witnesses. Kearns J stated: '[w]hen the telephone numbers on the computer printout were checked against the names who had registered each of the telephone numbers the identity of the users of each of the mobile phones was established clearly from the direct evidence which had been given by the various witnesses identified by the court.' See also *R v Shephard* [1993] AC 380 at 387, Lord Griffith: 'I suspect that it will very rarely be necessary to call an expert and that in the vast majority of cases it will be possible to discharge the burden by calling a witness who is familiar with the operation of the computer in the sense of knowing what the computer is required to do and who can say that it is doing it properly.'

[187] See *In the Interest of FP, a Minor* 878 A.2d 91 (Pa Super 2005) where transcripts of instant messages between the defendant and the victim were held properly authenticated after considering the following facts: the defendant identified himself by first name and threatened physical violence against the victim in the transcripts, the victim reported the threats to school authorities, staff at the school met with the defendant regarding the threats, the defendant sent another instant message regarding that school meeting, and the defendant's brother testified that he saw the defendant assault the victim. The court rejected arguments for a 'whole new body of law' for authentication of electronic evidence.

[188] Communications data, for example, with its distinctive characteristics linked to date/time-stamps and identity of creator, can also be used for authentication purposes. Other common technical solutions for reliability and integrity include embedded features in the electronic evidence itself such as 'watermarks' and digital signatures which are only of any real use for authentication purposes if the public key infrastructure (PKI) associated with the creation of the signature is outside the control of the proponent seeking to adduce the record as evidence. See S Fischer-Dieskau & D Wilke 'Electronically sighed documents: Legal requirements and measures for their long-term conservation' (2006) 3 *Digital Evidence and Electronic Signature Law Review* 38 and T Kunz, S Okunick and U Viebeg 'Long-term security for signed documents: Services, protocols and data structures' in AU Schmidt, Me Kreutzer & R Accorsi *Long-term and dynamical aspects of information security: Emerging trends in information and communication security* (2007) at 125.

technical focus of proving evidential weight 'is to have checks and balances in place to demonstrate the history of how the data have been managed, which leads to the assertion that the data have not been modified, replaced or corrupted and must, therefore, be trustworthy.'[189] Although these technical processes are not without risks and standing alone may not be proof of wrongdoing,[190] the information linked to electronic evidence can be an effective means of supporting an assertion that the electronic evidence has not been altered in any way.

An argument often made in support of heightened standards for admissibility of electronic evidence is that any modifications or alterations to electronic evidence is difficult, if not impossible, to detect. As regards the use of digital images for example, it has been argued that 'new authentication standards tailored to compensate for the susceptibilities inherent in digital imaging technology'[191] should be adopted because '[t]he lack of an "original" for comparison with the offered image reduces the opportunity to verify that the image has not been altered or has only been altered in an acceptable manner, thereby increasing the likelihood that changes will not be discovered unless the proponent of the image reveals them.'[192] This may not create much concern for evidence in a conventional paper-based format, which can be stored and retrieved as it was originally created. Electronic evidence, by nature of its computerised medium, may be transferred to another storage media or migrated to another form of software causing the evidence to undergo changes. This illustrates the need to pay careful attention to the manner in which electronic evidence is authenticated, more than whether it is the original or copy of the original.

This is not a problematic issue in South African domestic law because whether or not an original exists 'the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence … if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.'[193] Section 14 of the ECT Act 2002 provides that electronic evidence satisfies the requirements of original form if it meets the conditions set out in that section. These are in terms of s 14(1)*(a)* that 'the

---

[189] Mason & Stanfield op cit note 155 at 196.
[190] See E Casey *Digital Evidence and Computer Crime: Forensics Science, Computers and the Internet* (2004) at 477 noting that electronic evidence on its own can rarely conclusively prove that someone in a specific place at a specific time sent an email message, or that someone downloaded a pornographic image from the Internet. After all, IP addresses or any such technical information are linked to computers, not people and investigators will almost always have to combine this technical information physical evidence to strengthen a case.
[191] J Witkowski 'Can juries really believe what they see? New foundational requirements for the authentication of digital images' (2002) 10 *Journal of L and Policy* 267 at 294.
[192] Ibid at 272-73 (footnotes omitted).
[193] Section 15(1)*(b)*.

integrity of the information from the time when it was first generated in its final form as a data message' has passed assessment in terms of s 14(2) and, secondly, in terms of s 14(1)*(b)*, 'that information is capable of being displayed or produced to the person to whom it is to be presented.' As regards the first requirement, s 14(2) provides that the integrity of electronic evidence must be assessed: '(a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display; (b) in light of the purpose for which the information was generated; and (c) having regard to all other relevant circumstances.' The terms of a s 14(2)*(a)* assessment aligns with definitions of integrity that refer to electronic evidence that 'has not been altered in an unauthorised manner since the time it was created, transmitted, or stored by an authorised source.'[194] The integrity of electronic evidence as such refers to the soundness and completeness of the evidence over time, or in transit, and whether it can be considered to be unaltered and uncorrupted in all material aspects. [195] The integrity of electronic evidence may also be demonstrated by records found embedded in the evidence itself or embedded in the accompanying communications data.[196]

In order for integrity to exist and be demonstrated in terms of the statutory framework, it should not require that the electronic evidence be exactly the same 'from the time when it was first generated in its final form' as electronic evidence.[197] In other words, integrity should not be absolute. For example, traditional physical paper documents with the passage of time may subject the physical features of the paper document to deterioration and loss (e.g. faded signatures or print). However, while the physical integrity of the paper document may be compromised, the paper document is essentially completed and uncorrupted if the articulation of the content of the document and any required annotations remain the same.[198] Similarly with electronic evidence based in a computerised medium, technological obsolescence and media fragility may affect the features of the evidence 'in the normal course of communication,

[194] AJ Menezes, PC van Oorschot & SA Vanstone *Handbook of Applied Cryptography* (1997) at 24.
[195] See C Lynch 'Authenticity and integrity in the digital environment: An exploratory analysis of the central role of trust' (2000) available at *https://www.clir.org/pubs/reports/pub92/lynch/*, accessed 21 July 2019.
[196] See *Brown's* case supra note 46 at 215-16 regarding images found on a mobile phone, where the court conducted an assessment in terms of s 14 of whether the images satisfied the requirements of original form in terms of the conditions in that section. The court was satisfied with the 'undisputed evidence' on chain of custody of the device, the absence of evidence of tampering of the device or images and that the software used prevented tampering of the images. As regards authenticity of the images, the court was also satisfied with the testimony of the state's witness whom established the authenticity of the images in relation to integrity and security which were well documented, and not disputed by the accused.
[197] InterPARES Project 'Requirements for assessing and maintaining the authenticity of electronic records' (2002) at 1 available at *http://www.interpares.org/book/interpares_book_k_app02.pdf*, accessed 21 July 2019.
[198] See Lynch op cit note 195 at 3.

storage and display.[199] This does not affect the integrity of electronic evidence. If there has been any change to the electronic evidence, the assessment of integrity is whether the evidence has remained materially complete and unaltered. In essence, the ability to prove evidential weight 'is not [about] proving that an "original" exists'…[t]he issue is about trust, or the lack of trust.'[200] It means 'providing sufficient evidence to convince an adjudicator that the object that has been retrieved is a faithful representation of what is claimed to be the "original" or a reliable representation of the object that was relied upon by the originator.'[201]

V CONCLUSION

Notwithstanding the issues raised above, South African law has achieved its 'enabling character'[202] in the ECT Act 2002 'by ousting evidence rules which would exclude electronic evidence purely because of its electronic origin.'[203] The introduction of electronic evidence in criminal legal proceedings raises unique challenges in the South African law on evidence. The meaning and application of s 15, insofar as it applies to electronic evidence as hearsay or real evidence, or both, is a key and controversial issue. I am of the view that a proper construction of s 15 should not preclude a rule of admissibility for *all* electronic evidence, irrespective of hearsay representations contained therein. Support of such a construction is made even stronger by the the application of s 15(4) as a rebuttable presumption of law in terms of which an assumption which is demanded by law must be accepted by the court in the absence of evidence or proof to the contrary.[204] If fact-based issues of authenticity and integrity can be 'substantively satisfied' then hearsay as an exclusionary rule of evidence should no longer be warranted for electronic evidence based on the scope of inquiry in s 15(1) to (3). The issue of whether electronic evidence should more appropriately be dealt with as documentary evidence or as real evidence has challenged the courts. To an extent, it has resulted in the issues regarding admissibility of electronic evidence being approached from the premise of authenticity and integrity as a pre-requisite to admissibility. I have argued that this is not an appropriate approach. The preferred approach is aligned to the ECT Act 2002, which should not require as a condition of admissibility, that electronic evidence be authenticated. Stringent tests relating

[199] Section 14(2)*(a)*.
[200] Mason & Stanfield op cit note 155 at 230.
[201] Ibid.
[202] Schwikkard & Van der Merwe op cit op cit note 28 at 443.
[203] Ibid at 442, describing the decision in *Ndlovu's* case supra note 38.
[204] *ABSA Bank Ltd v Le Roux And Others* supra note 65 at 485.

to authenticity, integrity and truth or reliability of any information recorded in or reflected by the electronic evidence should not apply for admissibility purposes. I have proposed for the presumption in s 15(4) of the ECT Act 2002 to be reconsidered in South African law. Consideration must be given to more fully understanding meaning of the words 'certified to be correct'. This means that s 15(4) should be changed to incorporate a specific requirement that there must be some evidence of basic facts to demonstrate why a court should accept 'a data message made by a person in the ordinary course of business' that is 'certified to be correct' by an 'officer' of the business as 'proof of facts contained in such record, copy, printout or extract'.

On matters of evidential weight, given the different format and applications in which electronic evidence exists, there is no 'one-size-fits-all' approach to weight that will work and a range of evidential issues may arise depending on the nature of the evidence and source of its origin. The concept of 'original' and circumstantial indicators for reliability of electronic evidence itself provide useful tools for a court's assessment of evidential weight of electronic evidence. It is hoped that statutory reform initiatives will provide detailed guidelines and technical procedures for the judiciary and practitioners alike on the type of evidence that may be produced to establish the authenticity and integrity of electronic evidence. It is argued that while authentication standards for electronic evidence appear to vary from a moderate approach to a 'most demanding', calls for heightened standards of admissibility in relation to accuracy and authenticity should be rejected. While a robust consideration of authentication is required, I believe it should not be subject to stringent tests that makes it difficult for authentic electronic evidence to be admitted into evidence. The necessary safeguards after all are to be found in the determination of what evidential weight is to be accorded to the electronic evidence.

CONCLUSION

I INFORMING THE DEBATE

A central premise of the thesis is that evolving technological phenomena can and do present challenges to existing legal concepts on evidence and the investigatory powers of law enforcement and the security and intelligence agencies to obtain electronic evidence and for its admissibility in criminal proceedings. In the analysis I have critically described the legal, factual and technological debates of certain key investigative powers and evidential issues in the context of whether South African law has developed appropriately in response to advancements in technology or in ways that are cause for concern.

In doing so, I have analysed through key themes and arguments the challenges of regulating investigative powers and electronic evidence in an era of evolving technological phenomena: (i) how those investigative powers are used in practise by law enforcement and security and intelligence agencies, with a focus on interception (chapter two), acquisition and retention of communications data (chapter three), and access to encrypted information (chapter four); (ii) issues relating to transparency and oversight in the legal framework that governs the use of those powers; (iii) the importance of privacy in the information age, ensuring safeguards and necessary and proportionate limitations; (iv) technology, by considering the information age and a modern fast-paced environment of technological advancements as the setting in which the law currently operates, from new capabilities in relation to encryption, communication, connectivity, devices and data; and (v) a consideration of what the law could be. I also considered interesting questions in the law of evidence on the impact of electronic evidence in criminal proceedings in terms of two issues, admissibility and its weight (chapter five). In the final analysis, the debates feature arguments for 'more and fewer capabilities, more and fewer safeguards.'[1] As observed by Bartlett:

> 'On one side there are civil liberties groups demanding increased privacy and transparency; on the other there are securocrats and law-enforcement spokesmen, under pressure to keep us safe and facing a bewildering array of security threats, insisting they need to monitor more of our online behaviour ... The debate is lurching between these nightmarish poles: we can choose a

[1] D Anderson QC *A question of trust report of the Investigative Powers Review* (2015) Independent Reviewer of Terrorism Legislation available at *www.gov.uk/government/publications*, accessed 17 May 2016 at 245.

dystopia where our every move is secretly monitored, recorded and analysed, or a world where criminals are able to do what they like.'[2]

Albeit, the exaggerated rhetoric of Bartlett, if one thing is certain: technology has exposed the current frameworks in South African law in the context of the investigative powers of law enforcement and security and intelligence agencies to obtain electronic evidence, and its subsequent admissibility in criminal proceedings. Access to information is unprecedented and intelligence is shared in ways that neither the state nor the public predicted. Disturbingly, in ways that have been found to be unlawful and unconstitutional. Despite being brought to light by commissions, committees, the courts and civil rights organisations, both international and local, including significant findings of 'unlawful and unconstitutional'[3] surveillance practices, reports of such unlawful activities continue to emerge in post-democratic South Africa.[4] Informed discussion continues to be hampered by indications that the intelligence agencies appear to remain hopelessly politicised,[5] with weak accountability, excessive secrecy, with the added failure of the state to implement changes in law despite concerns of illegalities brought to its attention.

The benefits, and harm, of controversial and intrusive capabilities now available to law enforcement and security and intelligence agencies triggers a range of issues and challenges for individual rights, including how those capabilities are used in investigative activities, the scale of their use, the extent to which such capabilities intrude on privacy rights, legislative authority for their use and safeguards that constrain and regulate such new technological capabilities. The silence of the majority of the state is no longer defensible, nor can the necessity of further law reform continue to be ignored. Several aspects of Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002[6] have now been found by the High Court of South Africa to be 'deficient in meeting the threshold required by s 36 of the Constitution to justify the subtraction of the rights in ss 14 [privacy], 16(1) [rights to freedom of expression and of the media], and 34 [rights of access

[2] Ibid at 245 quoting J Bartlett *Orwell vs Terrorists: Crypto-wars and the future of surveillance* (2015).
[3] See 'Ministerial Review Commission *Intelligence in a Constitutional Democracy* 10 September 2008 Final Report to the Minster for Intelligence Services, the Honourable Mr Ronnie Kasrils MP (hereafter 'The Matthews Commission') at 180 available at *http://www.lse.ac.uk/international-development/Assets/Documents/PDFs/csrc-background-papers /Intelligence-In-a-Constitutional-Democracy.pdf*, accessed 05 January 2016.
[4] See earlier chapter 1 at 32 for incidents cited by amaBhungane Centre for Investigative Journalism in its legal challenge to the constitutionality of RICA 2002.
[5] See also chapter 2 at 91 where the Supreme Court of Appeal in *Zuma v Democratic Alliance and Others* 2018 (1) SA 200 (SCA) noted with 'unsettling' concern 'that different law enforcement agencies of government appear to be spying upon each other.'
[6] Hereafter 'RICA 2002'.

to a court] and 35(5) [rights to a fair trial] of the Constitution.'[7] Bulk surveillance activities was declared unlawful and invalid 'for want of a law authorising it to take place.'[8] Those aspects of RICA declared inconsistent with the Constitution included: ss 16(7), 17(6), 18(3)*(a)*, 19(6), 20(6), 21(6) and 22(7) in that it failed to prescribe procedures for user notification;[9] the definition of 'designated judge' in that it failed to prescribe an appointment mechanism and terms which ensure independence of the designated judge;[10] s 16(7) for its failure to adequately provide a system of appropriate safeguards to deal with orders that are granted *ex parte*;[11] ss 35 and 37 for their failure to prescribe proper procedures for handling, destruction and retention arrangements for data obtained through interceptions;[12] and ss 16(5), 17(4), 19(4), 21(4)*(a)*, and 22(4)*(b)* for their failure to prescribe procedures for the protection of sensitive information, including legal privilege and journalistic information in relation to sources.[13] Therefore, at the very least, legislative amendments to RICA 2002 or new legislation will have to remedy the above defects in law.

The rest of the chapter contains a summary of my proposals for change that have been detailed in the preceding chapters. Below I reiterate my proposals for a legislative solution with a focus on the overall importance of clear and accessible laws that avoids different sets of rules in different legislation covering essentially the same intrusive power. It is proposed that such powers should only be exercised when it is strictly necessary in fulfilment of a legally prescribed mandate. Clearly drafted legislative provisions should provide a unified approach to bulk surveillance measures: in doing so special care must be taken to minimise the impact on the constitutional rights of individuals, especially those whom are in no way implicated in an operation. There should be enhanced safeguards and procedures when sensitive rights are in issue such as the rights of journalists not to disclose their sources and the rights of lawyers/clients in privileged legal communications. It is essential that there is a clear and comprehensive system for the independent authorisation, transparency and oversight of the use of any measure that restricts constitutional rights. Individuals whose constitutional rights have been infringed must be able to seek an effective remedy. I have expressed the view that

[7] *amaBhungane Centre for Investigative Journalism NPC and SP Sole v Minister of Justice and Correctional Services and Others* Case No: 25978/2017 (16 September 2019) para 167, subject to confirmation by the Constitutional Court. The declaration of invalidity is suspended for two years to allow Parliament to cure the defects in law, and in some instances, interim relief was proposed by the court.
[8] See chapters 1, 2, and 3. Supra note 7 paras 143-166.
[9] Supra note 7 paras 41-54.
[10] Supra note 7 paras 55-71.
[11] Supra note 7 paras 72-83.
[12] Supra note 7 paras 84-108.
[13] Supra note 7 paras 109-142.

notification to a suspect/target of an interception direction should be by default, which would allow such individuals to pursue a challenge of legality retrospectively even in circumstances where exercise of such investigative power was deemed within rights limitations. Although my proposals below in Part II are done in the context of acquisition and retention of communications data, the key principles identified would equally apply across the other types of investigative powers identified.

II A FORWARD-LOOKING AND TRANSPARENT LEGAL FRAMEWORK IN SOUTH AFRICAN LAW

(a) Principles for a new legal framework

Policy debates in the context of the challenges of continued technological advancements and the complexity of electronic evidence frequently lack clarity. Underlying most of the criticisms of existing investigative powers is a fundamental concern regarding their scope and breadth in an environment dominated in the information age by connectivity, data and devices. The volume of information and data now being generated has the potential to give law enforcement and the security and intelligence agencies unprecedented access to personal information from a wide range of individuals, most of whom are unlikely to be of interest in any criminal matter, unless privacy protections and safeguards are robust in the modern technology environment.

Successive governments in South Africa from 1994 onwards have supported the compulsory retention of communications data by telecommunication service providers. A key lesson for South African law from European jurisprudence is that 'discretion afforded' to the state in operating an electronic surveillance regime 'must necessarily be narrower.' There can no longer be untargeted and indiscriminate mandatory retention of communications data, without suspicion and for everyone. Specifically on retention of communications data, I propose that there should be the introduction of targeted retention orders in a new legal framework. In other words, any direction for data retention must be linked to a legitimate aim and not have blanket application. A legitimate purpose may include, the interests of disruption, detection and investigation of criminal activity, specifically of serious offences or in the interests of national security or compelling national economic interests. In the joined cases of *Digital Rights Ireland Ltd* (C-293/12) and *Kärntner Landesregierung and*

Others (C-594/12),[14] the court was explicit in its view that that the retention of data by the adopted European Union Directive 'constituted a particularly serious interference with those rights' of privacy and data protection.[15] The court provided a number of reasons. First, while the court noted that the obligation in terms of the Directive 'does not permit the retention of the content of the communication or of information consulted using an electronic communications network' it regarded that '[t]hose data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.'[16]

Second, the court found that the 'the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives.'[17] Furthermore, as the directive 'covers all subscribers and registered users' it effectively 'entails an interference with the fundamental rights of practically the entire European population.'[18] Third, while seeking 'to contribute to the fight against serious crime' the directive 'does not require any relationship between the data whose retention is provided for and a threat to public security.' and, in particular, it is not restricted to a retention in relation 'and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime' or 'to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.'[19] Fourth, the court spoke of the need for 'clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data.'[20] The court found that the need for such safeguards was 'all the greater', as in the adopted directive, where 'personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data.'[21] Finally, 'as far as concerns

[14] CJEU (08 April 2014) para 26-27 (emphasis added). See chapter 3 at 111-13
[15] Supra note 14 para 39.
[16] Supra note 14 para 27.
[17] Supra note 14 para 56.
[18] Supra note 14 para 56.
[19] Supra note 14 para 57.
[20] Supra note 14 para 54.
[21] Supra note 14 para 55.

the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks' the court was concerned that the directive did not 'lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality.'[22]

In considering a new legal framework for the compulsory retention of communications data by telecommunication service providers, the South African state could address the above list of shortcomings by the European Court of Justice and ensure that any new law in this regard provides various safeguards against unauthorised access to and use of communications data. This will include safeguards on storing, accessing, examining, using and destroying communications data, such that it provides adequate safeguards against abuse of treatment of personal data and thus serve to protect individuals' personal integrity. These safeguards would equally apply to intercepted data, targeted and in bulk. This could similarly be the state's response to the outcomes of the *amaBhungane* case referred earlier. The state 'could take a superficial view'[23] of both decisions, and regard it as cases in which the European Court of Justice and High Court of South Africa found provisions in Directive 2006/24 and RICA 2002 respectively to be incompatible with various rights because it did not provide sufficient safeguards against unlawful access to that data or impose adequate limitations on data retention. Effectively, it would be 'a superficial response to a superficial reading'[24] to both case judgments. As Roberts argues, the judgment of the European Court of Justice 'has wider significance.'[25] I agree, and so too does the decision of the High Court of South Africa. Both judgments address the 'fundamental questions regarding the acceptable limits of mass surveillance and the function of the right to privacy, and we need to consider how it might be understood in this broader context and its implications for the relationship between the state and citizens (rights-holders).'[26] A key balancing principle is that investigative powers need to be limited in the interests of privacy rights.

[22] Supra note 14 para 66.
[23] A Roberts 'Privacy, data retention and domination: Digital Rights Ireland Ltd v Minister for Communications (2015) 78.3 *The Modern Law Review* 535 at 539-40.
[24] Ibid at 544.
[25] Ibid at 540.
[26] Ibid.

I therefore propose that the outcomes of both decisions reflect a fundamental concern regarding the scope and breadth of these investigatory powers in a modern fast-paced environment of technological advancements, and need for safeguards against 'arbitrary interference.'[27] Lord Sumption in United Kingdom case of *R (P) v Secretary of State for Justice* concluded that the need for safeguards against 'arbitrary' interference with individual rights, is a reference 'to safeguards essential to the rule of law because they protect against the abuse of imprecise rules or unfettered discretionary powers.'[28] Earlier in the judgment he noted:

> '... An excessively broad discretion in the application of a measure infringing the right of privacy is likely to amount to an exercise of power unconstrained by law. It cannot therefore be in accordance with law unless there are sufficient safeguards, exercised on known legal principles, against the arbitrary exercise of that discretion, so as to make its application reasonably foreseeable.'[29]

This is an opportunity for the South African state to not only address 'declarations of invalidity' of certain provisions in RICA 2002, but to do so within the context of the 'wider significance' of the relationship between the state and its citizens in investigative powers legislation.[30] It is not enough to say 'trust us'.[31] Concerns about the use of arbitrary power by law enforcement and security and intelligence agencies are well documented. Reports indicate that unlawful surveillance practices are only revealed by accident, or by information leaks, public interest litigation or whistleblowing. As such, the need for transparency and clear legal powers are fundamental as a new legal framework is being considered by the state, or at the very least legislative amendments to RICA 2002. Some of the intrusive investigative powers by law enforcement and security and intelligence agencies, specifically bulk surveillance, do not find clear and explicit basis for their use in RICA 2002 or any other legislation. This will need to be rectified. Different safeguards and authorising mechanisms based on types of data deemed less intrusive than others, and therefore more easily accessible by law enforcement and security and intelligence agencies, as set out in RICA 2002, will also need to be reconsidered. A legal framework designed in 2002 may have survived almost two decades through a technology neutral approach that ensured flexibility and agility in meeting the investigatory

[27] *Roman Zakharov v Russia* EctHR 47143/06 (4 December 2015) para 230. See also *The Queen (on Application of National Council for Civil Liberties (Liberty) v Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs* [2019] EWHC 2057 (Admin) para 224, and *Big Brother Watch & Ors v United Kingdom* 58170/13 (13 September 2018) para 306.
[28] [2019] UKSC 3; [2019] 2 WLR 509 para 41. See also *Liberty's* case supra note 27 paras 83-86.
[29] Supra note 28 para 31.
[30] Roberts op cit note 23 at 548.
[31] Anderson op cit note 1 at 214.

capability requirements of the information age. However, technology in the information age has now allowed law enforcement and security and intelligence agencies to have access to more sophisticated and new capabilities than appear justifiable in the existing legal framework of RICA 2002 and as demonstrated in the thesis, it carries with it safeguards that have minimal impact.[32] Where the interference with the right to privacy by the state 'is systematic rather than suspicion-based "[t]he sheer scale of the interference with privacy rights calls for a competing public policy justification of analogical magnitude", including – as a minimum – "a meaningful public account of the tangible benefits that accrue from its use."'[33]

III SUMMARY OF PROPOSALS

Shape of the new law in South Africa[34]

- A comprehensive new law should be drafted, providing clear limits and safeguards on the use of any intrusive powers that are necessary for law enforcement and security and intelligence agencies. The safeguards contained within the new law must be capable of preventing abuse of power.
- The new law clearly should provide for, inter alia: (i) types of powers allowed for obtaining data; (ii) the law enforcement and intelligence agencies permitted to obtain such data; (iii) authorisation and independent oversight mechanisms; (iv) handling criteria that apply to the use, retention, disclosure and deletion of such data, including parameters for sharing and safeguards in doing so.

Investigative capabilities[35]

- The existence of 'bulk' powers must be regulated subject to strict additional safeguards.
- The definitions of 'content' and 'communications data' must be reviewed and updated.
- The new law should close the loophole in s 205 of the Criminal Procedure Act 51 of 1977 that provides different sets of rules for essentially the same

[32] Ibid.
[33] Ibid at 256, quoting B Emmerson QC (UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism) Report to the General Assembly of 23 September 2014 para 13.
[34] Chapters 2, 3 and 4.
[35] Chapter 2 and 3.

investigative measures, which in practise is less strictly regulated under different standards of conduct to RICA 2002.

Warrants for interception[36]

- All warrants for interception should be judicially authorised.
- Where a warrant, targeted or bulk, is regarded as necessary at least in the interests of national security or for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the Republic insofar as those interests are also relevant to national security, it should involve the approval functions of a designated Minister, who is accountable to Parliament (and also in principle to the relevant courts in the fulfilment of the statutory duties imposed by the new law), by applying the principles of necessity and proportionality, and subject to judicial approval/review. In the process of ministerial/judicial approval, it must be satisfactorily established that the conduct of the investigative power authorised by the warrant is necessary to what is sought to be achieved.
- There should be a requirement that a bulk warrant application must contain in a sufficient level of detail, the description of the communications to be intercepted, and relevant to the operational purposes specified in the warrant. The requirement of operational purposes for bulk interception, similar to law in the United Kingdom, must be from a list maintained by a designated Minister and reviewed at quarterly intervals, including being presented to the parliamentary Joint Standing Committee on Intelligence after each review, and also to the President who must review the list of operational purposes at least once a year.

Independent oversight authority[37]

- The new law should create an independent oversight authority, to be supported by a team of experienced inspectors/technology experts. This oversight authority should include a body of judicial officers, whom are persons who hold or have held high judicial office, and are responsible for the judicial authorisation of all warrants.

[36] Ibid.
[37] Ibid.

- The independent oversight authority must be satisfied that there are safeguards and protections in place relating to the manner in which data is retained, copied, disclosed and destroyed.
- The independent oversight authority should also have the powers to notify the subject/target of interception surveillance after an investigation or operation has terminated, unless there is an objectively justifiable reason for maintaining secrecy.
- Other important functions, including oversight by way of audit, inspection and investigations should be central in the independent oversight authority.

Procedures for storing, accessing, examining, using and destroying the interception data[38]

- Intercepted data must be protected by appropriate technical and procedural measures against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure. This should also include measures for destroying the data if the retention of the data is no longer necessary, or ceases or is not otherwise authorised by law, and for the special handling of data in relation to legal privilege and journalists' confidential sources. There should be constraints on search criteria for examination of intercepted data.

Encryption[39]

- The modern realities of the information age will require a rethinking of the doctrinal principles of the right against self-incrimination.
- Although the provisions of RICA 2002 in relation to compelled decryption are not necessarily unconstitutional, the solution perhaps to the issue of compelled decryption and the impact of new technologies is to be found in new legislation that meets the requirements of the limitations clause of the Constitution which allows for the justifiable limitation of rights, which effectively means that the South African courts can afford a more generous approach to the contents of a right.
- There should be restrictions on the ability of the state to access our electronic information. These robust protections should come into play in the context of

[38] Ibid.
[39] Chapter 4.

search warrants that restrict searches of encrypted devices seized, with a key goal of 'a principle against government fishing expeditions in which agents conduct vast, exploratory searches for unsuspected, new crimes against suspects or even non-suspects.'[40]

Admissibility and evidential weight[41]

- A proper construction of s 15 of the Electronic Communications and Transactions Act 25 of 2002 should not preclude a rule of admissibility for *all* electronic evidence, irrespective of hearsay representations contained therein.
- A rethinking of s 15(4) business records presumption is proposed. I argued this should be linked to evidential foundations. For such a presumption to be recognised, it should be necessary for the proponent seeking to benefit from the presumption to adduce sufficient evidence, at least proof of basic facts, to warrant the introduction of such a presumption.
- On matters of evidential weight, there is no 'one-size-fits-all' approach that will work; while a robust consideration of authentication is required in the court's assessment of evidential weight of electronic evidence, it should not be subject to stringent tests that makes it difficult for authentic electronic evidence to be admitted into evidence.

IV CONCLUDING REMARKS

The rhetoric of the debate as extremes 'lurching between these nightmarish poles'[42] of one or the other may not be particularly helpful, but it reflects the fears that underlie the debates on both the benefits and harms of controversial investigative powers. If one thing is certain, it is that a new legislative framework in South African law must reflect a better balance between the extremes of the two sides. It is worth nothing that in the year 2020, the day of 4 February marked the twenty-fourth anniversary of the Constitution coming into operation. As we take stock of the key achievements in South Africa since 1996, the start of the new decade in 2020 provides an apt opportunity for the legislature and the courts to ensure that the protections enshrined in the Constitution are treated as a priority. The setup of a new legal framework for

[40] L Sacharoff 'Unlocking the Fifth Amendment: Passwords and Encrypted Devices' (2018) 87 *Fordham LR* 203 at 251.
[41] Chapter 5.
[42] Ibid.

investigatory powers, including reforms in relation to matters of evidence, should be one that responds effectively to the challenges of new technology, with minimal and justified interference of rights supported by robust oversight and accountability mechanisms. I hope the opportunity will be taken to 'build together an intricate set of modes of accountability, which involve Parliament as well as members of the government as the highest level.'[43]

[43] *The Queen (on Application of National Council for Civil Liberties (Liberty) v Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs* [2019] EWHC 2057 (Admin) para 167.

APPENDIX

Chapter Two: Interception of Communications

I REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT 70 OF 2002

(a) The meaning of interception

Section 1 of RICA 2002 sets out the following definitions and interpretation of relevant key terms:

> ‘**“intercept”** means the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the-
>
> (a) monitoring of any such communication by means of a monitoring device;
> (b) viewing, examination or inspection of the contents of any indirect communication; and
> (c) diversion of any indirect communication from its intended destination to any other destination,
>
> and **“interception”** has a corresponding meaning;
>
> **“interception direction”** means a direction issued under section 16(4) or 18(3)(a) and which authorises the interception, at any place in the Republic, of any communication in the course of its occurrence or transmission, and includes an oral interception direction issued under section 23(7);
>
> **“interception device”** means any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to intercept any communication.’

(b) Other key definitions in section 1

The definition of ‘direct communication’ is stated as follows:

> ‘**“direct communication”** means an-
>
> (a) oral communication, other than an indirect communication, between two or more persons which occurs in the immediate presence of all the person participating in that communication; or

(b) utterance by a person who is participating in an indirect communication, if the utterance is audible to another person who, at the time that the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication;

…

"indirect communication" means the transfer of information, including a message or any part of a message, whether-

(a) in the form of-

(i) speech, music or other sounds;

(ii) data;

(iii) text;

(iv) visual images, whether animated or not;

(v) signals; or

(vi) radio frequency spectrum; or

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

that is transmitted in whole or in part by means of a postal service or a telecommunication system;

…

"monitor" means to listen to or record communications by means of a monitoring device, and 'monitoring' has a corresponding meaning'.

"monitoring device" means any electrical, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to or record any communication.'

(c) Unlawful interception

Section 2 of RICA 2002 constitutes the key provision in this regard and prescribes the prohibition of interception of communications as follows:

'Subject to this Act, no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission.'

The prohibition in s 2 refers to the interception of communications 'in the course of its occurrence or transmission'. This must be read in conjunction with section 1(2)(*a*) and *(b)* of the Act which states that:

'(2) For the purposes of this Act-

(a) the interception of a communication takes places in the Republic if, and only if, the interception is effected by conduct within the Republic and the communication is either intercepted, in the case of-

(i) a direct communication, in the course if its occurrence; or

(ii) an indirect communication, in the course of its transmission by means of a postal service or telecommunication system, as the case may be; and

(b) the time during which an indirect communication is being transmitted by means of a telecommunication system includes any time when the telecommunication system by means of which such indirect communication is being, or has been, transmitted is used for storing it in a manner than enables the intended recipient to collect it or otherwise have access to it.'

Section 12 of RICA 2002 further provides as follows in relation to the prohibition of provision of real-time or archived communication-related information:

'Subject to this Act, no telecommunication service provider or employee of a telecommunication service provider may intentionally provide or attempt to provide any real-time or archived communication-related information to any person other than the customer of the telecommunication service provider concerned to whom such real-time or archived communication-related information relates.'

Section 42 of RICA 2002 provides in relation to prohibition on disclosure of information:

'(1) No person may disclose any information which he or she obtained in the exercising of his or her powers or the performance of his or her duties in terms of this Act, except-

(a) to any other person who of necessity supplies it in the performance of his or her functions in terms of this Act;

(b) if he or she is a person who of necessity supplies it in the performance of his or her functions in terms of this Act;

(c) information which is required in terms of any law or as evidence in any court of law; or

(d) to any competent authority which requires it for the institution, or an investigation with a view to the institution, of any criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act.

(2) No-

(a) postal service provider, telecommunication service provider or decryption key holder may disclose any information which he or she obtained in the exercising of his or her powers or the performance of his or her duties in terms of this Act; or

(b) employee of a postal service provider, telecommunication service provider or decryption key holder may disclose any information which he or she obtained in the course of his or her employment and which is connected with the exercising of any power or the performance of any duty in terms of this Act, whether that employee is involved in the exercising of that power or the performance of that duty or not,

except for the purposes mentioned in subsection (1).

(3) The information contemplated in subsections (1) and (2) includes information relating to the fact that-

(a) a direction has been issued under this Act;

(b) a communication is being or has been or will probably be intercepted;

(c) real-time or archived communication-related information is being or has been or will probably be provided;

(d) a decryption key is being or has been or will probably be disclosed or that decryption assistance is being or has been or will probably be provided; and

(e) an interception device is being or has been or will probably be installed.'

Section 45 of RICA 2002 in relation to the prohibition on manufacture, possession and advertising of listed equipment provides 'no person may manufacture, assemble, possess, sell, purchase or advertise any listed equipment'. Section 44(1)(*a*) defines listed equipment as 'any electronic, electro-magnetic, acoustic, mechanical or other instrument, device or equipment, the design of which renders it primarily useful for purposes of the interception of communications.'

(d) Lawful interception

S 25 (5) of RICA 2002, provides as follows:

'If a direction issued under section 23(3) or oral direction is cancelled in terms of subsection 2(2)-

(a) the contents of any communication intercepted under that direction or oral direction will be inadmissible as evidence in criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, unless the court is of the opinion that the admission of such evidence would not render the trial unfair or otherwise be detrimental to the administration of justice;'

(e) Application to a designated judge for the issuing of an interception direction

In terms of s 16(5):

'An interception direction may only be issued if the designated judge concerned is satisfied, on the facts alleged in the application concerned, that-

(a) there are reasonable grounds to believe that-

(i) a serious offence has been or is being or will probably be committed;

(ii) the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;

(iii) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;

(iv) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relation to terrorism or the gathering of information relating to organised crime or terrorism, is in-

(aa) accordance with an international mutual assistance agreement; or

(*bb*) the interests of the Republic's international relations or obligations; or

(v) the gathering of information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be there proceeds of unlawful activities is necessary;

(b) there are reasonable grounds to believe that-

(i) the interception of particular communications concerning the relevant ground referred to in paragraph (*a*) will be obtained by means of such an interception direction; and

(ii) subject to subsection (8), the facilities from which, or the place at which, the communications are to be intercepted are being used, or are about to be used, in connection with the relevant ground referred to in paragraph (a) are commonly used by

the person or customer in respect of whom the application for the issuing of an interception direction is made; and

(c) in respect of the grounds referred to in paragraph (a)(i), (iii), (iv) or (v), other investigative procedures have been applied and have failed to produce the required evidence or reasonably appear to be unlikely to succeed if applied or are likely to be too dangerous to apply in order to obtain the required evidence and that the offence therefore cannot adequately be investigated, or the information therefore cannot adequately be obtained, in another appropriate manner: Provided that this paragraph does not apply to an application for the issuing of a direction in respect of the ground referred to in paragraph (a)(i) or (v) if the-

(i) serious offence has been or is being or will probably be committed for the benefit of, or in association with, a person, group of persons of syndicate involved in organised crime; or

(ii) property is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities.'

II THE CRIMINAL PROCEDURE ACT 51 OF 1977

The relevant provisions of s 205 read as follows:

'(1) A judge of a High Court, a regional court magistrate or a magistrate may, subject to the provisions of subsection (4) and section 15 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002, upon the request of a Director of Public Prosecutions or a public prosecutor authorized thereto in writing by the Director of Public Prosecutions, require the attendance before him or her or any other judge, regional court magistrate or magistrate, for examination by the Director of Public Prosecutions or the public prosecutor authorized thereto in writing by the Director of Public Prosecutions, of any person who is likely to give material or relevant information as to any alleged offence, whether or not it is known by whom the offence was committed: Provided that if such person furnishes that information to the satisfaction of the Director of Public Prosecutions or public prosecutor concerned prior to the date on which he or she is required to appear before a judge, regional court magistrate or magistrate, he or she shall be under no further obligation to appear before a judge, regional court magistrate or magistrate.

(2) The provisions of sections 162 to 165 inclusive, 179 to 181 inclusive, 187 to 189 inclusive, 191 and 204 shall mutatis mutandis apply with reference to the proceedings under subsection (1).

(3) The examination of any person under subsection (1) may be conducted in private at any place designated by the judge, regional court magistrate or magistrate.

(4) A person required in terms of subsection (1) to appear before a judge, a regional court magistrate or a magistrate for examination, and who refuses or fails to give the information contemplated in subsection (1), shall not be sentenced to imprisonment as contemplated in section 189 unless the judge, regional court magistrate or magistrate concerned, as the case may be, is also of the opinion that the furnishing of such information is necessary for the administration of justice or the maintenance of law and order.'

The above section contains a cross-reference to s 15 of RICA 2002. The latter section reads as follows:

'(1) Subject to subsection (2), the availability of the procedures in respect of the provision of real-time or archived communication-related information provided for in section 17 and 19 does not preclude obtaining such information in respect of any person in accordance with a procedure prescribed in any other Act.

(2) Any real-time or archived communication-related information which is obtained in terms of such other Act may not be obtained on an ongoing basis.'

III THE NATIONAL PROSECUTING AUTHORITY ACT 32 OF 1998

Section 28 of the National Prosecuting Authority Act 32 of 1998[1], as amended by National Prosecuting Authority Amendment Act 61 of 2000[2], under chapter 5 in relation to 'powers, duties and functions relating to investigating directorates' provides powers to obtain 'any book, document or other object' as follows:

'(6) For the purposes of an investigation -

(a) the Investigating Director may summon any person who is believed to be able to furnish any information on the subject of the investigation or to have in his or her possession or under his or her control any book, document or other object relating to that subject, to appear before the Investigating Director at a time and place specified in the summons, to be questioned or to produce that book, document or other object;

(b) the Investigating Director or a person designated by him or her may question that person, under oath or affirmation administered by the Investigating Director , and examine or retain for further examination or for safe custody such a book, document or other object: Provided that any person from whom a book or document has been taken under this section may, as

[1] Hereafter 'NPAA 32 of 1998'.
[2] Hereafter 'NPAAA 61 of 2000'.

long as it is in the possession of the Investigating Director , at his or her request be allowed, at his or her own expense and under the supervision of the Investigating Director , to make copies thereof or to take extracts therefrom at any reasonable time.'

Chapter Three: Obtaining evidence from third part telecommunication service providers: Regulating surveillance of communication-related information (real-time or archived)

I REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT 70 OF 2002

(a) Definitions

'**"archived communication-related information"** means any communication-related information in the possession of a telecommunication service provider and which is being stored by that telecommunication service provider in terms of section 30(1)*(b)* for the period determined in a directive referred to in section 30(2)*(a)*, beginning on the first day immediately following the expiration of a period of 90 days after the date of the transmission of the indirect communication to which that communication-related information relates;

"**archived communication-related direction"** means a direction issued under section 18(3)*(a)* or 19(3) in terms of which a telecommunication service provider is directed to provide archived communication-related information in respect of a customer";

"real-time communication-related information" means communication-related information which is immediately available to a telecommunication service provider-

(a) before, during or for a period of 90 days after, the transmission of an indirect communication; and

(b) in a manner that allows the communication-related information to be associated with the indirect communication to which it relates.

"real-time communication-related direction" means a direction issued under section 17 (3) or 18 (3) in terms of which a telecommunication service provider is directed to provide real-time communication-related information in respect of a customer, on an ongoing basis, as it becomes available, and includes an oral real-time communication-related direction issued under section 23 (7).'[3]

[3] Section 1.

(b) Part 2: Prohibition of provision of real-time or archived communication-related information and exceptions (ss 12-15)

The prohibition and provision of real-time or archived communication-related information is set out in ss 12-15:

> '12 Prohibition of provision of real-time or archived communication- related information
>
> Subject to this Act, no telecommunication service provider or employee of a telecommunication service provider may intentionally provide or attempt to provide any real-time or archived communication-related information to any person other than the customer of the telecommunication service provider concerned to whom such real-time or archived communication-related information relates.'

In terms of s 13 of RICA 2002 in relation to the 'provision of real-time or archived communication-related information under real-time communication-related direction or archived communication-related direction' it is stated:

> 'Subject to this Act, any telecommunication service provider to whom a real-time communication-related direction or an archived communication-related direction is addressed, may provide any real-time or archived communication-related information to which that real-time communication-related direction or archived communication-related direction relates.'

Sections 14 and 15 completes Part 2, Chapter 2 of RICA 2002 on the '[p]rohibition of provision of real-time or archived communication-related information and exceptions' as follows:

> '14 Provision of real-time or archived communication-related information upon authorisation by customer
>
> Any telecommunication service provider may, upon the written authorisation given by his or her customer on each occasion, and subject to the conditions determined by the customer concerned, provide to any person specified by that customer, real-time or archived communication-related information which relates to the customer concerned.
>
> 15 Availability of other procedures for obtaining real-time or archived communication-related information
>
> (1) Subject to subsection *(2)*, the availability of the procedures in respect of the provision of real-time or archived communication-related information provided for in sections 17 and 19 does not preclude obtaining such information in respect of any person in accordance with a procedure prescribed in any other Act.

(2) Any real-time or archived communication-related information which is obtained in terms of such other Act may not be obtained on an ongoing basis.'

(c) Applications and issuing of a real-time or archived communication-related direction

In terms of s 17(1) 'an applicant may apply to a *designated judge* for the issuing of a real-time communication-related information direction.'[4] Further in terms of s 17(4):

(4) A real-time communication-related direction may only be issued if it appears to the designated judge concerned, on the facts alleged in the application concerned, that there are reasonable grounds to believe that-

(a) a serious offence has been or is being or will probably be committed;

(b) the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;

(c) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;

(d) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in-

(i) accordance with an international mutual assistance agreement; or

(ii) the interests of the Republic's international relations or obligations; or

(e) the gathering of information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities is necessary,

and that the provision of real-time communication-related information is necessary for purposes of investigating such offence or gathering such information.

For an archived communication-related direction, s 19(1) provides that '[i]f only archived communication-related information is required, an applicant may apply to a *judge of a High Court*, a *regional court magistrate* or a *magistrate* for the issuing of an archived

[4] Emphasis added. RICA 2002 provides for combined application and issuing of an interception direction, real-time communication-related direction and archive-related direction or interception direction supplemented by a real-time communication-related direction in terms of s 18(3)*(a)*.

communication-related direction.'[5] Similar to the grounds for a real-time communication-related information direction, an archived communication-related direction may only be issued if the 'reasonable grounds' threshold has been met.[6]

(d) Interception capability and mandatory retention of communication-related information

Continued compliance from telecommunication service providers requires technology capable of facilitating interception. Section 30 of RICA 2002 imposes duties on telecommunication service providers as follows:

> '(1) Notwithstanding any other law, a telecommunication service provider must-
>
> *(a)* provide a telecommunication service which has the capability to be intercepted; and
>
> *(b)* store communication-related information.'
>
> In terms of s 30(2), provides specifically:
>
> '(2) The Cabinet member responsible for communications, in consultation with the Minister and the other relevant Ministers and after consultation with the Authority and the telecommunication service provider or category of telecommunication service providers concerned, must, on the date of the issuing of a telecommunication service licence under the Electronic Communications Act, to such a telecommunication service provider or category of telecommunication service providers-
>
> *(a)* issue a directive in respect of that telecommunication service provider or category of telecommunication service providers, determining the-
>
> …
>
> *(iii)* type of communication-related information which must be stored in terms of subsection (1) *(b)* and the period for which such information must be stored, which period may, subject to subsection (8), not be less than three years and not more than five years from the date of the transmission of the indirect communication to which that communication-related information relates;'

Interception centres, including the establishment of Office for Interception Centres[7], is also provided for in RICA 2002 for 'the interception of communications.'[8]

[5] Emphasis added.
[6] Section 19(4).
[7] Hereafter 'OIC'.
[8] Sections 32-38.

Chapter Four: Obtaining evidence from a suspect/target of an investigation: Compelled decryption and the constitutional rights against self-incrimination

I REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT 70 OF 2002

(a) Applications and issuing of a decryption direction and entry warrant

Section 21 of RICA 2002 in relation to the application and issuing of decryption direction provides as follows:

> '(1) An applicant who-
>
> *(a)* makes an application referred to in section 16(1) may in his or her application also apply for the issuing of a decryption direction; or
>
> *(b)* made an application referred to in section 16(1) or, if he or she is not available, any other applicant who would have been entitled to make that application, may, at any stage after the issuing of the interception direction in respect of which such an application was made, but before the expiry of the period or extended period for which it has been issued, apply to a designated judge for the issuing of a decryption direction.
>
> (2) Subject to section 23(1), an application referred to in subsection (1) must be in writing and must-
>
> *(a)* indicate the identity of the-
>
> *(i)* applicant;
>
> *(ii)* customer, if known, in respect of whom the decryption of encrypted information is required; and
>
> *(iii)* decryption key holder to whom the decryption direction must be addressed;
>
> *(b)* describe the encrypted information which is required to be decrypted;
>
> *(c)* specify the-
>
> *(i)* decryption key, if known, which must be disclosed; or
>
> *(ii)* decryption assistance which must be provided, and the form and manner in which it must be provided;
>
> *(d)* indicate the period for which the decryption direction is required to be issued;
>
> *(e)* indicate whether any previous application has been made for the issuing of a decryption direction in respect of the same customer or encrypted information specified in the application and, if such previous application exists, must indicate the current status of that application;

(f) if the application is made in terms of subsection (1)*(b)*, also contain-

(i) proof that an interception direction has been issued; and

(ii) an affidavit setting forth the results obtained from the interception direction concerned from the date of its issuance up to the date on which that application is made, or a reasonable explanation of the failure to obtain such results; and

(g) comply with any supplementary directives relating to applications for decryption directions issued under section 58.

(3) A designated judge may, upon an application made to him or her in terms of subsection (1), issue a decryption direction.

(4) A decryption direction may only be issued-

(a) if the designated judge concerned is satisfied, on the facts alleged in the application concerned, that there are reasonable grounds to believe that-

(i) any indirect communication to which the interception direction concerned applies, or any part of such an indirect communication, consists of encrypted information;

(ii) the decryption key holder specified in the application is in possession of the encrypted information and the decryption key thereto;

(iii) the purpose for which the interception direction concerned was issued would be defeated, in whole or in part, if the decryption direction was not issued; and

(iv) it is not reasonably practicable for the authorised person who executes the interception direction concerned or assists with the execution thereof, to obtain possession of the encrypted information in an intelligible form without the issuing of a decryption direction; and

(b) after the designated judge concerned has considered-

(i) the extent and nature of any other encrypted information, in addition to the encrypted information in respect of which the decryption direction is to be issued, to which the decryption key concerned is also a decryption key; and

(ii) any adverse effect that the issuing of the decryption direction might have on the business carried on by the decryption key holder to whom the decryption direction is addressed."

(5) A decryption direction-

(a) must be in writing;

(b) must contain the information referred to in subsection 2*(a)*(ii) and (iii), *(b)* and *(c)*;

(c) must state the period within which the decryption key must be disclosed or the decryption assistance must be provided, whichever is applicable;

(d) may specify conditions or restrictions relating to decryption authorised therein; and

(e) may be issued for a period not exceeding three months at a time, and the period for which it has been issued may be specified therein: Provided that a decryption direction expires when the period or extended period for which the interception direction concerned has been issued, lapses.

(6) Section 16(7) applies, with the necessary changes, in respect of the issuing of a decryption direction.'

Section 22 of RICA 2002 in relation to the application and issuing of an entry warrant provides:

'(1) An applicant, who-

(a) makes an application referred to in section 16(1) may in his or her application also apply for the issuing of an entry warrant, or

(b) made an application referred to in section 16(1) or, if he or she is not available, any other applicant who would have been entitled to make that application, may, at any stage after the issuing of the interception direction in respect of which such an application was made, but before the expiry of the period or extended period for which it has been issued, apply to a designated judge for the issuing of an entry warrant.

(2) Subject to section 23(1), an application referred to in subsection (1) must be in writing and must-

(a) indicate the-

(i) identity of the applicant;

(ii) premises in respect of which the entry warrant is required to be issued; and

(iii) specific purpose, referred to in the definition of 'entry warrant', for which the application is made;

(b) if the application is made in terms of subsection (1)*(b)*, also contain-

(i) proof that an interception direction has been issued; and

(ii) an affidavit setting forth the results obtained from the interception direction concerned from the dates of its issuance up to the date on which that application is made, or a reasonable explanation of the failure to obtain such results;

(iii) comply with any supplementary directives relating to applications for entry warrants issued under section 58.

(3) A designated judge may, upon an application made to him or her in terms of subsection (1), issue an entry warrant.

(4) An entry warrant may only be issued if the designated judge concerned is satisfied, on the fact alleged in the application concerned, that-

(a) the entry of the premises concerned is necessary for a purpose referred to in the definition of 'entry warrant'; or

(b) there are reasonable grounds to believe that it would be impracticable to intercept a communication under the interception direction concerned otherwise than by the use of an interception device installed on the premises.

(5) An entry warrant-

(a) must be in writing;

(b) must contain the information referred to in subsection (2)*(a)*(ii) and (iii); and

(c) may contain conditions or restrictions relating to the entry upon the premises concerned as the designated judge deems necessary.

(6) An entry warrant expires when-

(a) the period of extended period for which the interception direction concerned has been issued, lapses; or

(b) it is cancelled in terms of section 23(11) or 25(1) or (2) by the designated judge who issued it or, if he or she is not available, by any other designated judge,

whichever occurs first.

(7) Section 16(7) applies, with the necessary changes, in respect of the issuing of an entry warrant.

(8) If an entry warrant has expired as contemplated in subsection (6)*(a)*, the applicant who made the application in respect of the entry warrant concerned or, if he or she is not available, any other applicant who would have been entitled to make that application, must, as soon as practicable after the date of expiry of the entry warrant concerned, and without applying to a judge for the issuing of a further entry warrant, remove, or cause to be removed, any interception device which has been installed thereunder and which, at the date of expiry of that entry warrant, has not yet been removed from the premises concerned.'

(b) Assistance by the decryption holder

In terms of assistance by the decryption holder, s 29 of RICA 2002 provides:

'(1) If a decryption direction or a copy thereof is handed to the decryption key holder to whom the decryption direction is addressed by the authorised person who executes that

decryption direction or assists with the execution thereof, the decryption key holder concerned must within the period stated in the decryption direction-

(a) disclose the decryption key; or

(b) provide the decryption assistance,

specified in the decryption direction concerned, to the authorised person concerned.

(2) In complying with a decryption direction, a decryption key holder-

(a) must only disclose such decryption key or provide such decryption assistance which is necessary to obtain access to the encrypted information specified in that decryption direction or to put that encrypted information in an intelligible form;

(b) may only disclose the decryption key or provide the decryption assistance to the authorised person who executes that decryption direction or assists with the execution thereof; and

(c) may not disclose any other information, which is not specified in that decryption direction, relating to the customer in respect of whose encrypted information the decryption key has been disclosed or the decryption assistance has been provided.

(3) A decryption key holder to whom a decryption direction is addressed and who is in possession of both the encrypted information and the decryption key thereto-

(a) may use any decryption key in his or her possession to provide decryption assistance; and

(b) must, in providing such decryption assistance, make a disclosure of the encrypted information in an intelligible form.

(4) A decryption key holder who, in terms of a decryption direction, is required to provide decryption assistance in respect of any encrypted information, will be regarded as having complied with that requirement if he or she-

(a) instead of providing such decryption assistance, discloses any decryption key to the encrypted information that is in his or her possession; and

(b) makes such a disclosure, in accordance with the decryption direction concerned, to the authorised person to whom, and by the time by which, he or she was required to provide the decryption assistance.

(5) If a decryption key holder to whom a decryption direction is addressed, is-

(a) not in possession of the encrypted information; or

(b) incapable, without the use of a decryption key that is not in his or her possession, to comply fully with that decryption direction,

the decryption key holder concerned must endeavour to comply, to the best of his or her ability, with that decryption direction.

(6) If a decryption key holder to whom a decryption direction is addressed, is in possession of different decryption keys, or combinations of decryption keys, to the encrypted information-

(a) it will not be necessary, for purposes of complying with the decryption direction concerned, for the decryption key holder to disclose any decryption keys in addition to those the disclosure of which, alone, is sufficient to enable the authorised person to whom they are disclosed to obtain access to the encrypted information and to put it into an intelligible form; or

(b) the decryption key holder may select which of the decryption keys, or combination of decryption keys, to disclose for purposes of complying with the decryption direction concerned.

(7) If a decryption direction is addressed to a decryption key holder who-

(a) has been in possession of the decryption key to the encrypted information, but is no longer in possession thereof;

(b) if he or she has continued to have the decryption key in his or her possession, he or she would have been required by virtue of the decryption direction to disclose it; and

(c) is in possession of any information that would facilitate the obtaining or discovery of the decryption key or the provision of decryption assistance,

he or she must disclose all such information as is in his or her possession to the authorised person who executes the decryption direction or assists with the execution thereof.

(8) An authorised person to whom a decryption key has been disclosed under this section-

(a) may use the decryption key only in respect of the encrypted information, an in the manner and for the purposes, specified in the decryption direction concerned; and

(b) must, on or before the expiry of the period or extended period for which the decryption direction concerned has been issued, with the written approval of the applicant who made the application for the issuing of a decryption direction, destroy all records of the disclosed decryption key, if in the opinion of the applicant concerned-

(i) no criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, will be instituted in connection with such records; or

(ii) such records will not be required at any such criminal or civil proceedings for purposes of evidence or for purposes of an order of court.'

(c) Offences and penalties

In terms of offences and penalties stated in s 51(4) provides as follows:

'*(a)* Any decryption key holder or any employee of a decryption key holder who-

(i) contravenes or fails to comply with section 29(1);

(ii) contravenes or fails to comply with section 29(2), (3)*(b)*, (5) or (7) or 42(2); or

(iii) performs an act contemplated in subsection (1) *(a)*(iii), (v) or (vii),

is guilty of an offence.

(b) Any decryption key holder or employee of a decryption key holder who is convicted of an offence referred to in paragraph *(a)* is liable, in the case of-

(i) a decryption holder who is a-

(aa) natural person, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years; or

(bb) juristic person, to a fine not exceeding R5 000 000; or

(ii) an employee, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years.'

Chapter Five: Admissibility of electronic evidence

I REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT 70 OF 2002

In terms of use of information in criminal proceedings, s 47 of RICA 2002 sets out the following:

'(1) Information regarding the commission of any criminal offence, obtained by means of any interception, or the provision of any real-time or archived communication-related information, under this Act, or any similar Act in another country, may be admissible as evidence in criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act.

(2) Any information obtained by the application of this Act, or any similar Act on another country, may only be used as evidence in any criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, with the written authority of the National Director, or any member of the prosecuting authority authorised thereto in writing by the National Director.'

II ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002

In terms of the legal requirements for data messages, Part 1 of the ECT Act 2002 sets out the following relevant sections:

> '11. Legal recognition of data messages
> (1) Information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message.
> (2) Information is not without legal force and effect merely on the grounds that it is not contained in the data message purporting to give rise to such legal force and effect, but is merely referred to in such data message.
> (3) Information incorporated into an agreement and that is not in the public domain is regarded as having been incorporated into a data message if such information is-
> *(a)* referred to in a way in which a reasonable person would have noticed the reference thereto and incorporation thereof; and
> *(b)* accessible in a form in which it may be read, stored and retrieved by the other party, whether electronically or as a computer printout as long as such information is reasonably capable of being reduced to electronic form by the party incorporating it.
>
> Original
> 14. (1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if-
> *(a)* the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and
> *(b)* that information is capable of being displayed or produced to the person to whom it is to be presented.
> (2) For the purposes of subsection 1*(a)*, the integrity must be assessed-
> *(a)* by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;
> *(b)* in the light of the purpose for which the information was generated; and
> *(c)* having regard to all other relevant circumstances.
>
> Admissibility and evidential weight of data messages
> 15 (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence-
> *(a)* on the mere grounds that it is constituted by a data message; or

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message must be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard must be had to-

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the integrity of the data message was maintained;

(c) the manner in which its originator was identified; and

(d) any other relevant factor.

(4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of facts contained in such record, copy, printout or extract.'