UNIVERSITY OF ZIMBABWE

FACULTY OF LAW

MASTER OF LAW DEGREE (LL.M)

"*Information Communication Technology and the Right to Privacy*"- *A critique of the current legal framework in Zimbabwe.*

By Lazarus Murinda

Supervisor: Dr. T. Mutangi

A research project submitted to the Faculty of Law, University of Zimbabwe, in partial fulfillment of the requirements of the Master of Law Degree

JUNE 2020

"*PRIVACY IS LIKE freedom: we do not recognize its importance until it is taken away...it is a personal right that we assume we have yet take for granted – until someone infringes on it.*"

David H. Flaherty '*On the utility of Constitutional Rights to Privacy and Data Protection*', 41 Case W. Res. L. Rev. 831 (1991) at 831

DECLARATION

I declare that this research project is my own work. The research project is submitted in partial fulfillment of the requirements for the degree in Master of Law, at the Faculty of Law, University of Zimbabwe. The research project has not been submitted before for any degree or examination in any other university.

.....

LAZARUS MURINDA **30 June 2020**

ACKNOWLEDGMENTS

Glory be to the ALMIGHTY GOD for affording me the gift of life and the opportunity to be a student and practitioner of the law. I would like to express my appreciation to my Supervisor Dr. T. Mutangi for guiding me through the research and for his wise counsel. I also wish to profusely thank Professor L. Madhuku for infusing the knowledge and skills that have shaped me into the person I am academically and professionally. My most profound appreciation goes to Sibusisiwe Chibaya for reviewing the first drafts of this thesis and for providing constructive feedback and encouragement. I also extend my acknowledgement to members of the Faculty of Law, University of Zimbabwe for making it a worthwhile experience as I ventured through my Master's Degree program. Last but not least, I wish to thank Linda Chaniwa for printing and binding various materials that contributed to the success of this research project.

DEDICATION

I dedicate this thesis to my wife **Tariro**, my son **Taonaishe** and my daughter **Kuzivakwashe**!

TABLE OF CONTENTS

LIST OF ACRONYMS

AIPPA	Access to Information and Protection of Privacy Act
ECHR	European Convention of Human Rights and Fundamental Freedoms
GPS	Global Positioning System
ICCPR	International Covenant on Civil and Political Rights
ICT	Information Communication Technologies
IoCA	Interception of Communications Act
POPI Act	Protection of Personal Information Act of South Africa
POTRAZ	Postal and Telecommunications Regulatory Authority of Zimbabwe
RICA	Regulation of Interception of Communications Act
SIM	Subscriber Identity Module
UDHR	Universal Declaration of Human Rights

CHAPTER 1

Overview on Information Communication Technology and Privacy

1.0 Introduction

The nexus between privacy, liberty and dignity plays a central role in defining what it means to be a human being.[1] In almost all societies, it is generally accepted that every person has a reasonable expectation of privacy in one form or another. For this reason the right to privacy, and/or the right to 'private life', is probably one of the most precious but also contentious of the universal fundamental human rights and freedoms. Although privacy has not only proved to be difficult to define but also means different things to different people, cultures, and societies, the right to privacy remains a fundamental right recognised in international human rights instruments as well as national constitutions and laws in many jurisdictions.

Despite its importance, the right to privacy finds itself in constant collision with other rights such as freedom of expression and often plays second fiddle to other societal interests such as the administration of the criminal justice system.[2] Indeed, the right to privacy has been under threat from various sources including the state and its

[1] See the minority judgment of O'Regan J. in the South African case of *NM & Ors v Smith* [2007] ZACC 6; 2007 (5) SA 250 (CC); in which the court said that the inter-relationship between privacy, liberty and dignity are the key constitutional rights which construct our understanding of what it means to be a human being.

[2] According to Foster, "[t]he right to privacy is...eternally in conflict with the power of the state to regulate individual and group conduct, and with the obligation of the state and its law to ensure that individual privacy is not enjoyed at the unreasonable expense of other rights." S. Foster, *Human Rights & Civil Liberties*, 2nd Ed. Pearson Education Limited, 2008. 560

machinery.[3] In response, the law has provided some safeguards against unwarranted invasion of privacy. However, a formidable threat to privacy has emerged in more ferocious forms with rapid developments in information and communication technologies (ICT). The emergence of highly intrusive technologies such as computers, the Internet, mobile phones, and a plethora of other 'smart' devices threaten to obliterate the essence of privacy. As postulated by Lord Hoffmann in the English case of *R v Brown*[4] 'the right to keep oneself to oneself, to tell other people that certain things are none of their business, is under technological threat.'

The primary purpose of this chapter is to provide a general overview of developments in the field of ICT and their impact on privacy. This first chapter also deals with the statement of the problem, justifications for, and objectives of, the study as well as the research questions. It also covers the research methodology and provides a brief review of relevant literature on the subject matter of the research.

1.1 Information Communication Technology and Privacy

The advent of sophisticated information and communication technologies in the turn of the century is perhaps one of the most fundamental innovations in the history of mankind. Today, technology permeates almost every facet of human life and continues to assume an increasingly important role in creating immense benefits for the society. Technology plays a critical role in delivering innovative, effective and convenient communication channels. Indeed, with these advances in novel

[3] Traditionally, the State has been perceived as a threat to individual privacy through surveillance of persons for political or other reasons such as investigation of crime. See G. M. Rehm, 'Privacy in the Digital Age: Vanishing into Cyberspace? In D. Friedmann & D. Barak-Erez (Eds) *Human Rights in Private Law*, Hart Publishing, 2001. 377

[4] *R v Brown* [1996] 1 AC 541 at 556

technologies, the world is progressively becoming interconnected and networked. It is now possible to electronically generate and seamlessly transmit information anywhere in the world at astonishing speeds. Computers are able to store massive amounts of data effortlessly, inexpensively and for inordinate periods of time.

Technology and particularly the Internet, has transformed social, legal and economic aspects of human life. People now predominantly communicate, interact and transact business on the Internet, via email, through video-conferencing, and a host of other social media platforms. In Zimbabwe, the total number of active mobile telephony subscriptions as at 30 June 2019 was approximately 12.3 million while mobile penetration rate was 84.8%.[5] In terms of data and Internet services, the total number of active Internet subscriptions was reported at 8.3 million during the same period while the Internet penetration rate was estimated at 57.2%.[6] This means that a significant proportion of the Zimbabwean populace is now actively using mobile telephony for making and receiving calls, sending and receiving messages as well as accessing the Internet.

The field of law in general, and in particular the area of human rights, has not been spared by technological developments as the world evolves into a global village. Advances in ICTs have both positively and adversely impacted on fundamental rights and freedoms. ICTs raise a gamut of legal issues relating to constitutional rights and fundamental freedoms such as the right to privacy, freedom of assembly and

[5] Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) Abridged Postal and Telecommunications Sector Performance Report: Second Quarter 2019 Report, p. 7. [Available at http//www.potraz.gov.zw]

[6] *Ibid*, at p. 16

association, freedom of expression, among others. In the first instance, ICT may be utilized in protecting and promoting constitutional rights such as the right of access to information and freedom of association and assembly. For instance, ICT may be used as an instrument for exposing and campaigning against human rights infractions.

Apart from these positive developments, another brand of 'rights' is also gradually emerging in tandem with the evolving technological revolution under the banner of "digital rights."[7] Although digital rights are not justiciable in our jurisdiction and many other jurisdictions, such rights are slowly gaining prominence elsewhere. Typical examples of so-called digital rights include but are not limited to accessibility to and availability of the Internet and right to access information on the Internet.[8] The importance of digital rights was felt when the Government of Zimbabwe shut down the internet on 15 January 2019 in order to quell the use of online social media during a mass stay away.[9]

On the other hand, increased usage of ICT also poses serious threats to, and continued erosion of, certain fundamental rights such as the right to privacy and the right to

[7] In 2012, the United Nations Human Rights Council passed a resolution to the effect that the 'same rights that people have offline must also be protected online.' See also MISA, "Digital Rights Lessons from Zimbabwe Internet Shutdown" https://misa.org/news/digital-rights-lessons-from-zimbabwes-internet-shutdown/

[8] See for instance, Articles 2 and 4 of the African Declaration on Internet Rights and Freedoms, which provide, respectively, that 'access to the internet should be available and affordable to all persons in Africa without discrimination...; 'everyone has the right to access information on the Internet'.

[9] In the case of *The Zimbabwe Lawyers for Human Rights and MISA Zimbabwe against the Minister of State for National Security & Others* (unreported) Case No: HC 265/19 applicants challenged a warrant issued by the Minister of State in the President's Office for National Security suspending internet services across all networks purportedly in terms of the Interception of Communications Act. Citizens could not access internet services, email services and social media platforms due to the shutdown and there was a huge local and international public outcry.

dignity. The proliferation of ICT devices that collect, store and transmit personal information implies that the privacy of personal information is at stake.[10] According to Solove,[11] 'every day, rivulets of information stream into electric brains to be sifted, sorted, rearranged, and combined in hundreds of different ways.' Individuals no longer have the ability to physically lock away sensitive information from curious eyes.[12] The ubiquitous use of ICT devices inevitably tends to whittle down the ability of citizens to enjoy their privacy in the absence of adequate legal safeguards.

Additionally, governments tend to resort to increased censorship, regulation and control of technologies such as the Internet in a manner that may impinge upon citizens' enjoyment of their constitutional rights.[13] ICT also comes with increased surveillance capabilities thereby threatening the privacy of citizens. The interception of private communications by law enforcement agents and increased surveillance of citizens in public places are some of the common vices associated with technological devices. In workplaces, shopping malls, airports, streets and in many other public places, surveillance cameras surreptitiously monitor human activities and incessantly collect personal information about unsuspecting citizens. Such information is

[10] A classic example in Zimbabwe on the use (or abuse) of personal information for political purposes is found in the July 2018 elections in Zimbabwe where voters' personal information (contact phone numbers) in the electronic voters' roll were allegedly accessed and used to disseminate bulk political campaign materials to citizens without their consent.

[11] D. J. Solove 'Privacy and Power: Computer Databases and Metaphors for Information Privacy', (2001) 53, *Stanford Law Review*, 1393 at 1394

[12] R. Winick 'Searches and Seizures of Computers and Computer Data' 8 *Harvard Journal of Law and Technology* 75,104 (1994)

[13] See *Zimbabwe Lawyers for Human Rights & Anor v The Minister of State in the President's Office & Ors* (unreported) Case No: HC 265/19 in which the High Court issued a provisional order setting aside a directive shutting down internet services.

transmitted to central computers in real time for processing without the knowledge and consent of the subjects.

The nation of Zimbabwe is by no means insulated from these technological developments and their attendant consequences on privacy. In 2018, the Government of Zimbabwe was reportedly mulling ideas on introducing *en masse* facial recognition technologies to improve its law enforcement capabilities and strengthen national security.[14] Such technologies have unpalatable implications for citizens' rights of privacy as they can learn unique features of individuals' facial makeup and be able to differentiate them from others. [15] Such technology may be used to carry out untrammelled surveillance on citizens with reckless abandon. Against this backdrop, a question that must inevitably exercise legal minds is whether our current legal framework is adequately geared to respond to these technological developments in defence of fundamental rights such as the right to privacy and the concomitant protection of personal information?

1.2 Statement of the Problem

Dramatic changes ushered in by developments in the ICT sector demand that the law and the legal system adapt to the changes in order to remain relevant. The corollary is

[14] See MISA Zimbabwe, 'Digest: Facial Recognition Technology and its possible impacts on Privacy Rights', http://zimbabwe.misa.org/2018/05/29/digest-facial-recognition-technology-privacy-rights/.

[15] 'Facial recognition software allows comprehensive collection of distinctive features on the surface of a face, such as the contours of the eye sockets, cheekbones, nose and chin.' See A. Atkon, 'Privacy and Data Protection in the Light of Smart TV Technology' (Unpublished Master Thesis, Tilburg Institute for Law, Technology & Society available at http://arno.uvt.nl/show.cgi?fid=140063 at page 30.

that extensive research is required in the field of ICT before calls for legal reforms can be made. According to Carr[16]

> '[i]t is trite to extol the virtues of the IT (information technology) revolution, its ability to shrink space and time, to bring people together without traversing long distances, to create new marketplaces and to contribute to global economic growth.'

While ICT brings with it many benefits, it also creates complex legal and other challenges that legal systems need to contend with. Legal complexities associated with the technological phenomena cut across every field of law including the general rubric of constitutional law and human rights. The law has always been seen as slow in keeping up with exponential developments in the field of technology thereby creating novel challenges for the legal system.[17] In the context of human rights, ICT poses a number of challenges that may require appropriate legislative responses. A number of countries have promulgated specific laws addressing issues pertaining to data protection, electronic commerce, cybercrime, and lawful interception of communications, among others.

Despite the pervasiveness of information communication technologies, limited research has been carried out in our jurisdiction to ascertain whether adequate legal safeguards exist to protect privacy rights in the digital era. In the same vein, there has been, and continue to be, apparent lack of urgency in coming up with legislative interventions to address some of the challenges emanating from the technological and

[16] I. Carr, *International Trade Law*, 5th Ed. Routledge Taylor Francis Group, 2014. 121

[17] See generally D. I. Bainbridge, *Introduction to Information Technology*, 6th Ed. Pearson Education Ltd, 2008, in which it is highlighted that information and communications technologies have posed and continue to pose novel and complex social legal problems.

information revolution.[18] In the absence of dedicated laws designed to specifically respond to peculiar challenges posed by technological advances, rights and freedoms of citizens are more likely than not to be prone to unwarranted interference. This is particularly the case where technology may be used as a formidable weapon in the hands of the state, law enforcement agents, powerful private and public institutions and powerful individuals to undermine the free enjoyment of fundamental rights and freedoms. Needless to say, research becomes necessary to unravel unique legal issues associated with the ICT phenomenon as well as identify potential gaps in the law.

The right to privacy raises fundamental questions that ought to exercise legal minds, ranging from the precise nature and scope of privacy to other pertinent issues such as the relationship between privacy and other competing rights and interests: what is the full scope of the right to privacy? To what extent does the law protect that right? Should the enjoyment of the right to privacy be limited? If so, to what extent and on what basis should the law attenuate privacy rights? To what extent has information and communication technologies made incursions into privacy interests? Is the current legal framework adequate to guarantee the full enjoyment of the right to privacy in the face of ubiquitous and invasive technological devices? Should the law intervene to provide additional safeguards in tandem with technological developments and their impact on privacy? These seemingly intractable legal questions demand answers.

[18] Proposals to promulgate cyber security and cyber crime laws, data protection legislation and electronic transaction and electronic commerce law have been in the pipeline for a long time. See Ministry of Information Communication, Postal and Courier Services website for pending bills at http://www.ictministry.gov.zw/?q=downloads

Whilst developments in the field of ICT have serious implications for privacy, the problem is that the right to privacy is generally a nebulous and multi-faceted concept. The increased intrusion on privacy necessitated by technological developments demands that we establish the extent to which the law protects the full scope of this fundamental right. This research seeks to critique the current legal framework in Zimbabwe in a bid to ascertain the extent to which the law protects the right to privacy in this digital era.

1.3 Research Questions

As highlighted above, the fundament of this thesis is to critique the current Zimbabwean legal framework in order to ascertain the extent to which it provides adequate protection (or lack thereof) to the right to privacy in the face of sustained developments in ICT and emerging facets of privacy. To this end, the research is guided by the following research questions:

(i) To what extent does the current legal framework provide for the right to privacy in Zimbabwe?

(ii) Are there any gaps in the current laws relating to the right to privacy in view of developments in the field of information and communication technologies?

(iii) How does the Zimbabwean law on privacy compare with international human rights instruments and laws of other jurisdictions?

(iv) What legal reforms (if any) are necessary to reinforce the right to privacy in Zimbabwe in the digital era?

However, the right to privacy is multifaceted and complex such that treatment of the full scope of the right may not be possible in this thesis. As such, the research will focus more on facets of privacy that have been seriously impacted on by information

communication technologies. It is important to highlight that the research is not about technology but about the state of the law on privacy in light of changes brought about by technological developments.

1.4 Research Methodology

This research predominantly adopts a 'doctrinal legal research' method. Doctrinal legal research has been defined and distinguished from non-doctrinal legal research as follows:

> 'Doctrinal legal research is defined as research into legal doctrines through analysis of statutory provisions and cases by the application of power of reasoning. It gives emphasis on analysis of legal rules, principles or doctrines. While non-doctrinal legal research is defined as research into relationship of law with other behavioral sciences.'[19]

The essence of the doctrinal research method is that it entails 'a systematic exposition, analysis and critical evaluation of legal rules, doctrines or concepts, their conceptual bases, and inter-relationship.'[20] This approach enables the researcher, according to Professor Birks,[21] 'to analyse, criticise, sift and synthesise' the law. In terms of data gathering methods, the primary source materials will include an analysis of constitutional provisions, legislation and relevant case law relating to the law of privacy in Zimbabwe. Key legislative instruments will include the Constitution of Zimbabwe[22] and other Acts of Parliaments with a bearing on privacy including (but not limited to) the Access to Information and Protection of Privacy Act,[23] Interception

[19] K. Vibhute & F. Aynalem *Legal Research Methods Teaching Material*, 2009 chilot.worldpress.com at p. 70

[20] *Ibid*, at p. 71

[21] Birks, P. "The Academic and the Practitioner", (1998) 18 *Legal Studies*, 377 at 399

[22] Constitution of Zimbabwe Amendment (No. 20) Act, 2013

[23] [Chapter 10:27]

of Communications Act,[24] and the Criminal Law (Codification and Reform) Act.[25]

Reference will also be made to leading textbooks and prominent journal articles on the subject matter of the research. In order to develop deep insights into the law of privacy as it obtains in Zimbabwe and at the regional and international plane, an analysis of key international human rights instruments will be carried out. In the same vein, a comparative perspective will be adopted by looking at privacy laws in other jurisdictions such as South Africa and the United Kingdom. These two countries have been singled out in this research for a good reason: the legal system of South Africa, like that of Zimbabwe, has its roots firmly entrenched in the Roman-Dutch Law system. In addition, English law has also influenced the legal system of Zimbabwe by virtue of the country being an erstwhile British colony.

1.5 Literature Review

Although there are growing concerns globally over the extent to which technology continues to encroach on privacy,[26] the realization that technology is a constant threat to privacy is by no means a recent phenomenon. Threats posed by mechanical devices on privacy have long been recognized. In 1890, Warren and Brandeis observed as follows in their seminal article: '*The Right to Privacy*':[27]

---

[24] [Chapter 11:20]

[25] [Chapter 9:23]

[26] See S. Davis in R. K. M. Smith & C. van den Anker (eds) *The Essentials of Human Rights*, Hodder Arnold, 2005: 288-290 at 288 who argues that 'according to opinion polls, concern over privacy violation is now greater than at any time in recent history. Uniformly, populations throughout the world report their distress about encroachment on privacy, prompting an unprecedented number of nations to pass laws that specifically protect the privacy of their citizens.'

[27] S. D. Warren & L. D. Brandeis "The Right to Privacy" *Harvard Law Review,* Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220 at 195. Available at http://www.jstor.org/stable/1321160 [Accessed: 14 November 2019]

> *'Instantaneous photographs* and newspaper enterprises *have invaded the sacred precincts of private and domestic life*; and *numerous mechanical devices* threatened to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops".' (Emphasis supplied)

The learned authors (Warren and Brandeis) lamented the invasion of privacy by "numerous mechanical devices" as way back as 1890. Since then the technological landscape has changed dramatically. The inescapable corollary is that the current technological advances signify the death knell for privacy. In 1928 Justice Brandeis in *Olmstead v United States*[28] also foretold the dangers posed by technology that have become stark reality in the present era:

> 'Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home...'[29]

Similar sentiments were expressed in 1963 in *Lopez v United States*[30] in which the court observed that 'the fantastic advances in the field of electronic communication constitutes a great danger to the privacy of the individual.' In 1977, the Privacy Protection Study Commission also echoed the same fears regarding the dangers of technology on individual liberties:

> 'The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping system, each of which alone may seem innocuous, even benevolent, and wholly justifiable.'[31]

---

[28] *Olmstead v United States*, 277 U.S. 438 (1928)

[29] *Ibid*. 474

[30] *Lopez v United States* 373 U.S. 427 (1963)

[31] See Privacy Protection Study Commission, "Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission", 1977, http://aspe.hhs.gov/datacncl/1977privacy/toc.htm cited in George Reynolds "Ethics in Information Technology", Cengage Learning

But perhaps a more succinct explanation of the modern day impact of technology on privacy are the most telling words of Lord Hoffmann in *R v Brown*:[32]

> "One of the less welcome consequences of the information technology revolution has been the ease with which it has become possible to invade the privacy of the individual. No longer is it necessary to peep through keyholes or listen under the eaves. Instead, more reliable information can be obtained in greater comfort and safety by using the concealed surveillance camera, the telephoto lens, the hidden microphone and the telephone bug. No longer is it necessary to open letters, pry into files or conduct elaborate inquiries to discover the intimate details of a person's business or financial affairs, his health, family, leisure interests or dealings with central or local government. Vast amounts of information about everyone are stored on computers, capable of instant transmission anywhere in the world and accessible at the touch of a keyboard."

The magnitude of the threat to privacy has exponentially grown with the multiplicity of computers and other devices such as mobile phones,[33] tablets, digital cameras and many other gadgets that electronically process photos, audios, videos, and messages. As observed by Stefanick:

> 'The ubiquitous use of email, cellphones, digital cameras, instant messaging, and social networking allows people to share information instantly and to connect, reconnect, and stay connected with people all over the globe in ways that were inconceivable a mere decade ago.'[34]

[32] *R v Brown* [1996] 1 AC 541 at 556

[33] One author highlighted that "[t]he ubiquitous smartphone, above and beyond a communication device, is a device which can maintain a complete record of the communications data, photos, videos and documents, and a multitude of other deeply personal information, like application data which includes location tracking, or financial data of the user." See Centre for Internet & Society (2014), "Search and Seizure and the Right to Privacy in the Digital Age: A Comparison of US and India downloaded from <https://cis-india.org/internet-governance/blog/search-and-seizure-and-right-to-privacy-in-digital-age >

[34] L. Stefanick, *Controlling Knowledge: Freedom of Information and Privacy Protection in a Networked World*, AU Press, Athabasca University, 2011. 187

Wicker[35] posits that 'cellular technology allows service providers to compile activity and location records of ever finer granularity, records that reveal users' behavior, beliefs and preferences.'[36] These devices are increasingly interconnected and can transmit information anywhere in the world in a matter of seconds. Similarly, various search engines and social media platforms continue to sprout, facilitating the exchange of inordinate amounts of personal data and information. As observed by one author:

> 'Search engines and social media platforms simultaneously allow access to information that individuals may wish to keep "private" or secret, such as news articles about past crimes, embarrassing old photos, or sex videos posted by ex-partners.'[37]

The above synopsis of literature suggests that threats posed by developments in technology to privacy are more than real. Although extensive literature on the interface between technology and privacy abound in other developed jurisdictions, a dearth of literature is available on the subject in Zimbabwe. According to the Stakeholder Report on the Right to Privacy in Zimbabwe:[38]

> 'As innovations in information technology have enabled previously unimagined forms of collecting, storing, and sharing personal data, the right to privacy has evolved to encapsulate state obligations related to the protection of personal data.'

The authors of the Stakeholder Report on the Right to Privacy in Zimbabwe argue that 'despite constitutional recognition of the right to privacy and Zimbabwe's international obligations to uphold the right to privacy, few protections for privacy

---

[35] S. B. Wicker 'Cellular Convergence and the Death of Privacy' Oxford University Press, 2013

[36] *Ibid*. p. 4

[37] See Article 19, 'The "Right to be Forgotten": Remembering Freedom of Expression', 2015, Free Word Centre, available at http://www.article 19.org, p. 4

[38] Stakeholder Report Universal Periodic, 26th Session, "The right to privacy in Zimbabwe" (March, 2016) submitted by the Zimbabwe Human Rights NGO Forum, the Digital Society of Zimbabwe, the International Human Rights Clinic at Harvard Law School, and Privacy International, p. 3

exist in Zimbabwe's domestic law.' [39] The same authors opine that although Zimbabwe enacted the Access to Information and Protection of Privacy Act in 2002 'the Act's title is a misnomer, as it does not serve to protect privacy, but instead allows the government to control aspects of the media, through measures such as the accreditation of journalists.'[40] In the same vein, the authors of the Stakeholder Report on the Right to Privacy in Zimbabwe lament the lack of data protection legislation in Zimbabwe.

1.6 Structure of the Thesis

This thesis is divided into six chapters dealing with various issues relating to the law of privacy. Chapter 1 provided a general overview of developments in the field of ICT and their impact on privacy. The first chapter also covered the background to the research, statement of the problem, justifications and objectives of the study as well as the research questions. It also dealt with the research methodology and provided a snapshot of literature review on the subject matter of the research.

Chapter 2 extensively deals with the constitutional right to privacy under Zimbabwean law. The chapter canvasses the right to privacy as provided for in the Constitution of Zimbabwe. Chapter 2 also looks at constitutional limitations on the right to privacy. Chapter 3 explores the right to privacy in Zimbabwe from a statutory law and common law perspectives. Various enactments providing for the right to privacy in Zimbabwe will be interrogated and evaluated. The chapter will also discuss common law remedies for breach of privacy.

---

[39] *Ibid*. p. 4

[40] *Ibid.* p. 4

Chapter 4 brings into the fray regional and international perspectives on the right to privacy and its various facets. An analysis of a number of international instruments encapsulating the right to privacy is carried out. These instruments include the Universal Declaration of Human Rights 1948; the International Covenant on Civil and Political Rights 1966; the European Convention on Human Rights and Fundamental Freedoms; the African Charter on Human and People's Rights as well as the African Charter on Rights and Welfare of the Child. The Chapter will also cover the UN General Assembly Resolution A/RES/69/166 of 2014 on The Right to Privacy in the Digital Age.

From a comparative standpoint, Chapter 5 explores the law of privacy as it obtains in other jurisdictions. In particular, the chapter assesses the right to privacy in South Africa and under English law. The chapter concludes by showing that different jurisdictions treat privacy interests differently although privacy is now almost universally recognized as a fundamental right.

Chapter 6 concludes this research by presenting findings, conclusions and recommendations. Recommendations will include proposed legislative reforms targeted at improving the protection of privacy interests, particularly in the area of interception of communications and data protection. Areas for further research will also be highlighted in this chapter.

1.7 Conclusion

This chapter commenced by providing a general overview of the developments in the field of ICT and possible ramifications on the right to privacy. The chapter dealt with

the background to the research, statement of the problem, research questions, and research methodology. The next chapter will carry out an in depth analysis of the right to privacy under Zimbabwean constitutional law.

CHAPTER 2

Constitutional Right to Privacy under Zimbabwean Law

2.0 Introduction

An overview on the impact of information communication technology on privacy in the digital era was provided in the preceding chapter. The primary objectives of this chapter are two-fold. The first objective is to explore the definition and nature of privacy from different perspectives. This objective is necessary as attempts to define privacy, and concomitantly its precise nature and full scope, has generally been problematic. The second objective is to interrogate the constitutional framework regulating the right to privacy in Zimbabwe.

A critique of the relevant constitutional provisions will be carried out in a bid to assess the extent to which the constitution, as the supreme law of the land, guarantees the right to privacy. The chapter endeavors to find answers to two fundamental research questions posed in Chapter 1. The first question relates to the extent to which the current legal framework provides for the right to privacy in Zimbabwe. The second question is concerned with finding any gaps in the law in view of developments in the field of information and communication technologies.

2.1 Nature and scope of the right to privacy

It is self-evident that human nature requires a certain level of privacy as a basic necessity of life. Privacy appears to be an incontrovertible 'right' that naturally accrues to every person by virtue of one being human[41] in the sense that individuals have an innate freedom to do what they want in private, away from intrusive and

[41] In *S v A & Another* 1971 (2) SA 293 (T) 297 the court confirmed that a person's right to privacy is one of 'those rights in rem related to personality, which every free man is entitled to enjoy.'

prying eyes of the public and without interference from others. Despite its recognition as a fundamental human right locally, regionally and globally,[42] privacy remains a nebulous concept defying precise definition.

A cursory review of literature on privacy evinces considerable controversy over the definitional nature and scope of the right.[43] Rengel[44] opines that 'providing a concrete definition of the notion [of privacy] has eluded social scientists, jurists, philosophers, and others seeking singular clarity on the subject.' For this reason, privacy has been variously described as 'notoriously difficult to define';[45] as both 'amorphous and elusive';[46] and as 'exasperatingly vague and evanescent.'[47] By its nature, privacy consists of a bundle of different but related rights rendering it difficult to define with any degree of precision.[48]

[42] The right to privacy is guaranteed in virtually almost all notable international human rights instruments and found in most national constitutions.

[43] See *NM & Ors v Smith & Ors* 2007 (5) SA 250 (CC)

[44] A. Rengel, Privacy as an International Human Right and the Right to Obscurity in Cyberspace, *Groningen Journal of International Law*, Vol 2(2) (2015): 37 Privacy in International Law, <https://grojil.files.wordpress.com/2015/04/grojil_vol2-issue2_rengel.pdf

[45] A. W. Bradley & K. D. Ewing *Constitutional & Administrative Law*, 15th Ed. Pearson Education Limited, 2011. 476

[46] *Bernstein & Ors v Bester & Ors* 1996 (2) SA 751: 787-788

[47] A. R. Miller, *The Assault on Privacy: Computers, Data Banks and Dossiers*, University of Michigan Press, 1971. 25

[48] K. Gormely, One Hundred Years of Privacy, 1992. *Wisconsin Law Review*, 1335 at 1339 in which it is stated that 'legal privacy consists of four or five different species of legal rights which are quite distinct from each other and thus incapable of a single definition.'

As highlighted by Rubenfeld[49] 'privacy is like obscenity: Justices might not be able to say what privacy is, but they know it when they see it.' Privacy is everything and anything rolled in one. It can be 'a situation, a right, a claim, a form of control, or a value. It relates to information, autonomy, identity, or access. Alternatively, it can be split into the aspects of confidentiality, anonymity, and data protection.' [50] The corollary is that 'privacy' as a term can be described, but not clearly defined. Be that as it may, definitions of privacy (or rather descriptions of privacy) are many and varied. Under Zimbabwean law, the term 'privacy' and what it represents has not been explicitly defined in case law or other sources of law.[51] However, according to the Stakeholder Report on the Right to Privacy in Zimbabwe:[52]

> 'The right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction, and liberty, a "private sphere" with or without interaction with others, free from arbitrary state intervention and from excessive unsolicited intervention by other uninvited individuals.'

The above definition finds support in *Khumalo & Ors v Holomisa*[53] in which the court highlighted that the right to privacy 'recognizes that human beings have the right to a sphere of intimacy and autonomy that should be protected from invasion.' Similarly, in *Bernstein & Ors v Bester NO & Ors*,[54] the court defined privacy as:

---

[49] J. Rubenfeld, The Right of Privacy, 1989. Yale Law School, Faculty Scholarship Series, Paper 1569, at 751 http://digitalcommons.law.yale.edu/fss_papers/1569. See also J. B. Young, "Introduction" In J. B. Young (ed), *Privacy 2*, 1978 where the author states that "privacy, like an elephant, is more readily recognized than described."

[50] B. C. Stahl, 'What Privacy? The Impact of the UK Human Rights Act 1998 on Privacy Protection in the Workplace' in R. Subramanian (ed) *Computer Security, Privacy and Politics, Current Issues, Challenges and Solutions*, IRM Press, (2008), 55-68

[51] At least to the knowledge of this researcher.

[52] Stakeholder Report on the Right to Privacy in Zimbabwe (n 38 above) 3

[53] *Khumalo & Ors v Holomisa* 2002 (5) SA 401 (CC)

[54] *Bernstein & Ors v Bester NO & Ors* 1996 (2) SA 751 at 789.

> '...an individual condition of life characterized by exclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has determined himself to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private.'

Protection of privacy has been portrayed as a way of drawing the line on how far society can intrude into a person's private affairs.[55] In American jurisprudence, the right to privacy is expressed in a broader sense as the '*right to be let (or left) alone*'.[56] Stefanick elucidates this broad definition by observing that privacy entails 'the right of individuals to be let alone to pursue their self-interest without observation or interference from others.'[57] Thus, the right to privacy seeks to ensure that personhood, that is, the quality or condition of being an individual person, remains inviolate.

The right to privacy is not only about individual autonomy per se but extends to various other values and interests. Indeed, the right to privacy has been described as embodying two competing and contradicting 'core ideas'. On the one hand, 'privacy is about creating distance between oneself and society, about being left alone (privacy as freedom from society), but it is also about protecting elemental community norms concerning, for example, intimate relationships or public reputation (privacy as dignity).'[58] From this perspective, one can say that:

---

[55] O. Mironenko, Body Scanners versus Privacy and Data Protection, 2011. 27. *Computer Law and Security Review* 232 -244: 235 available at www.sciencedirect.com

[56] This definition is attributed to Brandeis & Warren (n 27 above). It has been contended that the 'right to be left alone seems to be attractive and capture imaginations but it does not lend itself to clear legal (or moral) implementation.' Stahl (n 50 above) 55-68

[57] Stefanick (n 34 above). 36

[58] O. Diggelmann & M. N. Cleis, How the Right to Privacy Became a Human Right, 2014. Vol. 14 Issue 3. *Human Rights Law Review*, 441-458: 442 https://doi.org/10.1093/hrlr/ngu014

> 'privacy is a broad concept relating to the protection of individual autonomy and the relationship between an individual and society, including government, companies, and private individuals. It encompasses a wide range of rights including protections from intrusions into family and home life, control of sexual and reproductive rights, and communications secrecy.'[59]

The right to privacy does not only concern itself with aspects relating to the individual's personal attributes (such as bodily integrity) but also extends to the individual's personal property and possessions. The quintessence of privacy as viewed from the latter perspective lies in a person's right not to have their property entered without permission, arbitrarily searched, or their possessions seized.[60]

Recently, the law has evolved through data protection legislation to enable individuals to control the use and dissemination of their personal information by others. In this regard, 'information privacy' is considered an integral adjunct to, and a basic element of, the general right of privacy. This perspective is supported by Westin[61] who defines privacy as a 'claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'. Foster expounds on the notion of information privacy as follows:[62]

> 'The right to privacy may refer more specifically to the protection of information that is personal to you or an associate: the revelation of personal or family secrets or any other information that one would prefer to keep either to oneself or within a particular group of associates.'

The inescapable deduction from the foregoing is the absence of a single, universal and exhaustive definition of privacy. The nature of privacy is such that it is a multifaceted

[59] Article 19 (n 37 above). 7

[60] Section 57 of the Constitution of Zimbabwe, 2013

[61] A. F. Westin, *Privacy and Freedom*, Atheneum, 1970. 330-364

[62] Foster (n 2 above). 559-560

concept comprising a number of distinct but interrelated components. As aptly observed by Finn *et al*,[63] 'privacy is an inherently heterogeneous, fluid and multidimensional concept.' The right to privacy may be conveniently condensed into five major taxonomies,[64] namely: *bodily privacy* (or *privacy of person*); *privacy of communications*; *information privacy*; *territorial or spatial privacy*;[65] and *decisional privacy*. Finn *et al*,[66] have conceptualized privacy into seven typologies, *viz*: (i) privacy of the person; (ii) privacy of behaviour and action; (iii) privacy of communications; (iv) privacy of data and image; (v) privacy of thought and feelings; (vi) privacy of location and space; and (vii) privacy of association. Finn *et al*,[67] argue that, while other theorists lament the fact that privacy is difficult to pin down, 'an imprecise conceptualization of privacy may be necessary to maintain a fluidity that enables new dimensions of privacy to be identified, understood and addressed in order to effectively respond to rapid technological evolution.'[68] This research will endeavor to establish the extent to which some of these broad facets of privacy are protected by the laws of Zimbabwe.

2.2 Rationale behind the Right to Privacy

After all is said and done, it remains necessary to step back and reflect on why the law painstakingly seeks to protect privacy in all its different forms. Privacy encompasses a

[63] R. L. Finn, D. Wright & M. Friedewald 'Seven Types of Privacy' in P. J. A. de Hert, S. Gutwirth, S. Leenes, & Y. Poullet (Eds.) *European Data Protection: Coming of Age*, Springer, 2013.

[64] Section 57 of the Constitution of Zimbabwe seeks to protect privacy broadly in five distinct areas although these areas may not fall neatly and squarely into the above taxonomies.

[65] Stefanick (n 34 above). 11 states that 'territorial privacy concerns the establishment of limits on intrusion into a variety of physical spaces, such as the domestic space, the workplace, and the public space.'

[66] Finn (n 63 above)

[67] *Ibid*.

[68] *Ibid.*

set of innate values and principles regarded by human beings as sacrosanct. The concept of privacy is also inextricably linked to other values and freedoms such as human liberty and dignity, freedom of expression and freedom of association.[69] Foster[70] neatly summaries some of the values and principles encapsulated in the notion of privacy as follows:

> 'The right to privacy or private life: thus reflects a number of values and principles: personal autonomy and dignity; reputation and honour; bodily integrity; and the formation and continuance of personal and other relationships.'

The law therefore seeks to protect privacy in the same manner that it guarantees the protection of other concepts such as the individual's liberty and dignity. The importance of the right to privacy and the legal mechanics for its protection cannot be negated.

2.3 Right to Privacy in Zimbabwe

The right to privacy is recognized and protected from three perspectives, namely: it is enshrined in the Constitution;[71] it is protected through a number of statutory enactments;[72] as well as under the common law. Invasion of privacy may not only be actionable under civil law but may also attract sanctions under criminal law.[73] The law relating to privacy in Zimbabwe will therefore be explored from a constitutional, statutory and common law standpoints. Potential remedies available at law in the event of breach of privacy are also considered under each of the perspectives. In this

[69] Article 19 (n 37 above) 7.

[70] Foster (n 2 above). 559

[71] Section 57 of the Constitution of Zimbabwe Amendment (No. 20) Act, 2013

[72] For instance, section 95 of the Criminal Law (Codification and Reform) Act [Chapter 9:23]

[73] *S v I & Another* 1976 (1) SA 781 (RAD) 784 where Beadle ACJ stated: 'It seems to me to be a *fortiori* conclusion that if a particular invasion of privacy was not actionable at civil law, it certainly would not be punishable at criminal law.'

chapter the focus is on the constitutional framework regulating privacy rights in Zimbabwe.[74]

2.3.1 Constitutional Protection of the Right to Privacy

The constitutional framework in Zimbabwe provides for the protection of privacy as a fundamental right. Even the former constitution of Zimbabwe provided for the right to privacy in one form or another though not explicitly. The relevant provisions of the former and current constitutions are explored insofar as they related or relate to the right to privacy.

2.3.2 Provisions of the former Constitution

Historically, the right to privacy was not specifically guaranteed in the former Constitution of Zimbabwe.[75] Thus the categorical recognition of privacy as a stand alone constitutional right is a recent phenomenon introduced in 2013 by dint of section 57 of the current Constitution of Zimbabwe. The absence of a specific right to privacy in the former constitution did not detract from its importance as a fundamental right as some aspects of privacy were guaranteed.[76] For instance, section 17(1) of the former constitution provided for 'protection against arbitrary search or entry' and stipulated that:

> 'Except with his own consent or by way of parental discipline, no person shall be subjected to the search of his person or his property or the entry by others on his premises.'

---

[74] The statutory protection of privacy as well as the common law position is covered in Chapter 3.

[75] The former Constitution of Zimbabwe was published as a Schedule to the Zimbabwean Constitution Order 1979 (S.I. 1979/1600 of the United Kingdom. The former Constitution came into operation on 10 June 1981 via Constitution of Zimbabwe Amendment Act 1981 and repealed by the current Constitution of Zimbabwe Amendment (No. 20) Act, 2013.

[76] See also C. B. Ncube, 'Data Protection in Zimbabwe', in A. B. Makulilo (Ed.) *African Data Privacy Laws*, Springer International Publishing, 2016. 104

Section 17 however limited the protection against arbitrary search or entry, in the interests of defence, public safety, public order, public morality, public health or town and country planning. It also circumscribed freedom from search and entry for purposes of law enforcement where reasonable grounds existed for believing that the search or entry was necessary for the prevention or investigation or detection of a criminal offence. Section 20(1) of the former constitution also protected privacy of personal correspondence as follows:

> 'Except with his own consent or by way of parental discipline no person shall be hindered in the enjoyment of his freedom of expression, that is to say, freedom to hold opinions and to receive and impart ideas and information without interference, and *freedom from interference with his correspondence*.' (Emphasis supplied)

The above section therefore protected 'freedom from interference with correspondence' as an important facet of privacy. In *Law Society of Zimbabwe v Minister of Transport and Communications & Anor*[77] the court held that unfettered powers conferred on the President in terms of the Postal and Telecommunications Act, [78] to intercept correspondence and communications were 'too broad and overreaching to be reasonably justified in a democratic society.' The impugned sections of the Act were, rightly so, declared unconstitutional and eventually struck down.

As highlighted above, one of the glaring shortcomings of the former constitution was the absence of a distinct right to privacy per se. At best, certain aspects of privacy were subsumed in other fundamental rights such as freedom of expression. A critique of the provisions of the former constitution also reveals that protection of the full

[77] *Law Society of Zimbabwe v Minister of Transport and Communications & Anor* SC 59/2003

[78] [Chapter 12:05]

scope of the right to privacy was not guaranteed. However, these misgivings were subsequently and substantially addressed in the current Constitution of Zimbabwe.

2.3.3 Provisions of the current Constitution

The current Constitution of Zimbabwe Amendment (No. 20) Act 2013 now provides for an explicit right to privacy. Section 57 stipulates as follows in this regard:

> 'Every person has the right to privacy, which includes the right not to have –
> (a) their home, premises or property entered without their permission;
> (b) their person, home, premises or property searched;
> (c) their possessions seized;
> (d) the privacy of their communications infringed; or
> (e) their health condition disclosed.'

The import of section 57 is two-fold. Firstly, it enshrines a general right to privacy for every person without exception. Secondly, the section enumerates a host of specific infringements of privacy proscribed by its provisions, including but not limited to, unauthorised entry, search and seizure, infringement of privacy of communications and disclosure of health conditions. Accordingly, the current position of the law in Zimbabwe is that privacy is explicitly guaranteed in the Constitution as a fundamental right.

The Constitution also contains complementary provisions relating to privacy by way of exclusion from the ambit of freedom of expression and freedom of media, of 'malicious injury to a person's reputation or dignity' or 'malicious or unwarranted breach of a person's right to privacy.' [79] Thus the Constitution of Zimbabwe

[79] See section 61(5) of the Constitution

recognizes that freedom of expression and freedom of media should not be exercised to the detriment of a person's reputation, dignity and/or privacy.

In addition, although the Constitution does not specifically provide for the right to protection of personal information as part of the right to privacy (save for information relating to health conditions), it does recognize a fundamental principle of data protection in the form of the *right to correction and deletion of incorrect information*. For the avoidance of doubt, section 62 (3) of the Constitution provides:

> 'Every person has a right to the correction of information, or the deletion of untrue, erroneous or misleading information, which is held by the state or any institution or agency of the government at any level and which relates to that person.'

Albeit the right to correction or deletion of incorrect information is provided in the context of the right of access to information in the Constitution, there is no doubt that the crux of the right lies in the protection of personal information.

2.3.4 Juristic Persons and the Right of Privacy

An analysis of the pertinent constitutional provisions demonstrates the availability of the right of privacy to both natural and juristic persons. The Declaration of Rights in the Constitution of Zimbabwe does not only bind natural and juristic persons[80] but also provides for the enjoyment of the rights and freedoms by both natural and juristic persons to the extent that those rights and freedoms can appropriately be extended to them.[81] The courts have dealt with the right to privacy as it pertains to juristic persons.

[80] Section 45 (2) of the Constitution of Zimbabwe

[81] Section 45 (3) of the Constitution of Zimbabwe

In *Eto Electricals and Rewinds (Pvt) Ltd v ZESA Holdings (Pvt) Ltd*[82] the court observed that:

> 'Section 45(3) of the Constitution provides that juristic persons as well as natural persons are entitled to the rights and freedoms set out in Chapter 4 to the extent that those rights and freedoms can appropriately be extended to them...the applicant, which is an incorporated company, is entitled to the rights and freedoms set out in the constitution, just like a natural person. The right to privacy is one to which the applicant can lay claim...'

Thus the right to privacy is also conferred on juristic persons in appropriate circumstances although their privacy rights are not perceived as intense as those of natural persons on the basis that juristic persons do not possess human dignity.[83] As rightly pointed out by Du Plessis and De Ville, 'because of the highly personal, human nature of substantive privacy rights the protection they afford appears to be restricted to natural persons only, whereas juristic persons seem to have a claim to certain informational privacy rights.'[84] The corollary is that, unlike natural persons, juristic persons do not enjoy the full bouquet of privacy rights. In *Thint (Pty) Ltd v National Director of Public Prosecutions and Ors*[85] the court observed that a corporate entity 'does not bear human dignity and thus its rights of privacy are much attenuated compared with those of human beings.'

---

[82] *Eto Electricals and Rewinds (Pvt) Ltd v ZESA Holdings (Pvt) Ltd* HH 547-15

[83] *Investigating Directorate: Serious Economic Offences and Ors: In Re Hyundai Motor Distributors (Pty) Ltd and Ors v Smit NO and Ors* 2001 (1) SA 545 (CC)

[84] L. M. Du Plessis & J. R. De Ville 'Personal Rights: Life, Freedom and Security of the Person, Privacy, and Freedom of Movement' in Van Wyk *et al* D (Ed) (2004) Rights and Constitutionalism: The New South African Legal Order, Clarendon Press, Oxford Juta & Company Ltd. 243

[85] *Thint (Pty) Ltd v National Director of Public Prosecutions and Ors* [2008] ZACC 13 para [77]

2.3.5 Limitation of the right to privacy

The right to privacy, like most other fundamental rights and freedoms, is not absolute and admits of exceptions. To use the words of the court in *Bernstein* case[86] '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 *Zimbabwe Lawyers for Human Rights & Anor v President of the Republic of Zimbabwe & Anor*,[87] the court held that although rights created by the constitution are protected and guaranteed, they are not absolute and are subject to limitations that are 'designed to ensure that the enjoyment of the said rights and freedoms by any person does not prejudice the public interest or the rights and freedoms of other persons.'

In *Mr. & Mrs. "X" v Rhodesia Printing & Publishing Co. Ltd*[88] the court noted that there is a qualified right to privacy and that 'in deciding whether or not to afford relief in any particular case, a Court will often have to steer a middle course between apparently conflicting interests.' Similarly, in *S v I & Another*[89] the court observed that

> '...while every person has an inborn right...to have his privacy respected, this rule is subject to many limitations. What the limitations are in any particular case must depend on a variety of circumstances...'

[86] *Bernstein and Others v Bester and Others NNO* 1996 (2) SA 751 (CC)

[87] *Zimbabwe Lawyers for Human Rights & Anor v President of the Republic of Zimbabwe & Anor SC 12/03*

[88] *Mr. & Mrs. "X" v Rhodesia Printing & Publishing Co. Ltd* 1975 (1) SA 590 (RA) 513C-D

[89] *S v I & Another* 1976 (1) SA 781 (RAD) at 784G-H See also *Rhodesian Printing & Publishing Ltd v Duggan* 1975 (1) SA 590 (RAD)

According to Du Plessis and De Ville[90] the right to privacy can be limited by law of general application if the limitation (i) is reasonable and justifiable in an open and democratic society based on freedom and equality, and (ii) does not negate the essential content of the right. Bradley and Ewing[91] contend that where rights of privacy are restricted, there is a case for violations only where there is clear legal authority and only where there is a clear need for a legitimate purpose.

The Constitution of Zimbabwe manifestly provides for limitations on rights and freedoms in two fundamental dimensions. First, it provides that the fundamental rights and freedoms 'must be exercised reasonably and with due regard for the rights and freedoms of other persons.'[92] The second and equally important parameter is that fundamental rights and freedoms may be limited only in terms of a law of general application and to the extent that the limitation is fair, reasonable, necessary and justifiable in a democratic society.[93] The Constitution provides a host of pertinent factors that must also be taken into account in determining the fairness, reasonability, necessity and justifiability of the limitation.[94] Thus the right to privacy is not entirely sacrosanct as it is subject to certain limitations imposed by the law.

[90] Du Plessis & De Ville (n 84 above). 242

[91] Bradley (n 45 above). 477

[92] Section 86 (1) of the Constitution.

[93] See Section 86(2) of the Constitution. See also J. A. Mevedzenge 'Accessing the National Voters' Rolls through the Right of Access to Information in Zimbabwe', *Zimbabwe Rule of Law Journal* Vol. 1 Issue 1, February 2017 International Commission of Jurists and Center for Applied Legal Research (at page 16) in which the author states that 'the right of access to information may only be limited through a law of general application which applies to everyone in Zimbabwe.'

[94] See section 86(2) of the Constitution

Be that as it may, any such limitation must be reasonably justifiable in a democratic society and must constitute an acceptable derogation from the right in order to pass constitutional muster. In the case of *In re Munhumeso & Ors*[95] Gubbay CJ stated:

> 'What is reasonably justifiable in a democratic society is an illusive concept – one which cannot be precisely defined by the courts. There is no legal yardstick save that the quality of reasonableness of the provision under challenge is to be judged according to whether it arbitrarily or excessively invades the enjoyment of a constitutionally guaranteed right.'

In *Madanhire & Anor v Attorney General*[96], Patel JA observed that 'the test as to what is democratically reasonable and justifiable is not susceptible to precise legal formulation' and that 'the test may very well vary from one society to another depending upon its peculiar political organization and socio-economic underpinnings.' The courts will generally apply the proportionality test in determining whether a limitation to a constitutional right is reasonable and justifiable.[97]

In *Law Society of Zimbabwe v Minister of Transport and Communications & Anor*[98] the court noted that freedom from interference with correspondence is not absolute. Chidyausiku CJ remarked as follows:

> 'It is also clear that the protection given, under the Constitution, to freedom from interference with correspondence is not an absolute right but may be restricted, as with freedom of expression, in certain circumscribed circumstances:-
> (a) the interference with the right must be in accordance with a law;
> (b) it must be, *inter alia*, in the interest of defence, public safety, public order, the economic interests of the State, public morality or public health;
> (c) the interference must be reasonably justifiable in a democratic society.'

---

[95] *In re Munhumeso & Ors* 1994 (1) ZLR 49 (S) at 64B-C

[96] *Madanhire & Anor v Attorney General* 2014 (1) ZLR 719 (CC) at 728D-E. See also *Retrofit (Pvt) Ltd v PTC & Anor* 1995 (2) ZLR 199 (S) 211C-F; *United Parties v Min of Justice* 1997 (2) ZLR 254 (S) 269A-E

[97] *S v Makwanyane and Another*1995 (3) SA 391 (CC)

[98] *Law Society of Zimbabwe v Minister of Transport and Communications & Anor* SC 59/2003

It is therefore trite law that any restriction on a constitutional right must be provided by law of general application in order to be justifiable.[99] In addition, the restriction must be intended for the pursuance of a legitimate aim and be necessary in a democratic society. In *Mosley v News Group Newspapers Ltd*[100] the court noted that

> '[t]he judge will often have to ask whether the intrusion, or perhaps the degree of the intrusion, into the claimant's privacy was proportionate to the public interest supposedly being served by it.'

Thus once a reasonable expectation of privacy is established the next stage is to determine whether there is some countervailing consideration of public interest justifying any intrusion on privacy.[101] There is also support from case law for the proposition that invasion of privacy for purposes of obtaining evidence may be justified. Thus in *S v I & Another*[102] the court held that

> '[i]n a case where one spouse suspects the other of committing adultery, invasion of the privacy of the guilty spouse and of his paramour by the injured spouse may be justified where the injured spouse invades that privacy solely with the bona fide motive of obtaining evidence of the adultery and the invasion is no more than is reasonably necessary for the purpose of obtaining that evidence.'[103]

2.4 Critique of the Constitutional provisions on privacy

The provisions of the current Constitution must be applauded for entrenching a more encompassing and comprehensive right to privacy. In the quest to provide for an elaborate and standalone right to privacy, the current Constitution expands on aspects

---

[99] Laws of general application that restrict the right to privacy such as the Interception of Communications Act will be discussed in the ensuing chapter.

[100] *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB) at para 7

[101] *Ibid.* at para 11

[102] *S v I & Another* 1976 (1) SA 781 (RAD)

[103] See headnote on page 781

of privacy relating to protection from arbitrary search or entry and also incorporates additional privacy parameters such as the right not to have one's health condition disclosed. Notably, the current Constitution also replaces 'freedom from interference with correspondence' in the former constitution with the right not to have the privacy of one's communications infringed. Ncube[104] opines that the substitution of the term 'correspondence' with 'communication' in section 57(d) of the Constitution 'may be indicative of a broadening of the scope of protection from written communication (i.e. correspondence) to all types of communication including oral and digital forms.' However, it has been observed that 'correspondence', in its broadest meaning, involves communication with others.[105]

Unlike in the former constitution, the parlance of section 57 of the Constitution generously provides for protection of various facets of privacy. However, whether the provisions of section 57 cover the full spectrum of the right to privacy as it is commonly understood remains debatable. Indeed, section 57 does not sufficiently protect the privacy of personal data or information unless such personal information or data is deemed to be a 'communication' or the information relates to a person's health condition.

Put differently, section 57 partially protects personal information in only two fundamental respects, *viz*: through the right of a person not to have their communications infringed, and not to have their health condition disclosed. A third aspect of protection of personal information is provided in section 62 of the

[104] C. Ncube 'A Comparative Analysis of Zimbabwean and South African Data Protection Systems', 2004 (2) *The Journal of Information, Law and Technology* (JILT). 105

[105] A. Peters, "Privacy, Rechtsstaatlichkeit, and the Legal Limits on Extra-territorial Surveillance" in Miller, R. A. (Ed) Privacy and Power: A Translantic Dialogue in the Shadow of the NSA-Affair at p. 147

Constitution which deals with the right of access to information. Section 62(3) confers the right of every person to correction of personal information held by the state or other institutions of government. However, this section too does not protect personal information held by persons or institutions other than the state and institutions of government.

Thus a glaring shortcoming of the Constitution is that it does not seem to cater for the protection of the full spectrum of privacy, in particular, the protection of personal information. The Stakeholder Report on the Right to Privacy highlights that Zimbabwe lacks data protection legislation despite that 'a number of international instruments enshrine data protection principles, and many domestic legislatures have incorporated such principles into national law.'[106]

Developments in the ICT field call for alternative ways of interpreting the provisions of section 57 of the Constitution in order to ensure the enjoyment of the full scope of the right to privacy. For instance, in the digital world, the right of a person not to have 'their home, premises or property entered without their permission' should not be considered merely in the parochial sense of physically 'entering' the premises. As technology evolves physical invasion of privacy in the sense of 'entering' of premises without permission has transformed. New devices capable of accessing previously inaccessible locations now potentially threaten to erode any remnants of privacy. Again the words of Lord Hoffmann in *R v Brown*[107] are spot on:

> 'No longer is it necessary to peep through keyholes or listen under the eaves. Instead, more reliable information can be obtained in greater comfort and safety by using the concealed surveillance camera, the telephoto lens, the hidden microphone and the telephone bug.'

[106] See Stakeholder Report Universal Periodic (n 38 above). 3

[107] *R v Brown* [1996] 1 AC 541: 556

Thus the phrase 'entered without permission' requires a wider interpretation by the courts to include devices such as drones which may physically 'enter' a home, premise or property and take photos and videos in breach of one's privacy. In addition, territorial or spatial privacy is no longer limited to domestic space and public space but also applies to aerial surveillance thanks to technology. For instance, the recreational use of drones mounted with cameras hovering over private property may constitute trespassing and an invasion of privacy.[108]

Albeit every person has a reasonable expectation of privacy regarding the sanctity of their home, premises or property, the Constitution of Zimbabwe does not however specifically protect privacy of individuals outside their homes, premises or property, that is, privacy in public spaces. Yet advances in technology have resulted in invasion of privacy outside the confines of a person's home, premises or property. For instance, devices such as mobile phones increasingly encroach on the user's location privacy regardless of whether the user is in a private or public space. Blumberg and Eckersley[109] underscore the importance of location privacy as follows:

> 'Preserving locational privacy is about maintaining dignity and confidence as you move through the world. Locational privacy is also about knowing when other people know things about you, and being able to tell when they are making decisions based on those facts.'

Mobile telephony gadgets have become, to all intents and purposes, tracking devices *par* excellence, posing ominous threats to locational privacy. Typically, stalking applications can be installed easily on a person's cell phone and used to track the

[108] See B. Gonzalez, 'Drones and Privacy in the Golden State, 2017. 22 *Santa Clara High Tech. Law Journal.* 288 http://digitalcommons.law.scu.edu/chtlj/vol33/iss2/3.

[109] A. J. Blumberg & P. Eckersley, *On Location Privacy and How to Avoid Losing it Forever, Electronic Frontier Foundation*, 2009 http://www.eff.org at 7.

user's movements without their knowledge. One author amply explains the ramifications of mobile telephony on privacy as follows:

> 'Technology has made it easy for a person to track the whereabouts of someone else at all times, without ever having to follow the person. Cell phone spy software called stalking app can be loaded onto someone's cell phone or smart phone within minutes, making it possible for the user to perform location tracking, record calls, view every text message or picture sent or received, and record the URLs of any website visited on the phone. A built-in microphone can be activated remotely to use as a listening device even when the phone is turned off.'[110]

A typical case in point is *S v Chipetu*[111] in which applicant was arrested for theft of a motor vehicle. Applicant's cell phone, which he had left at a police station in Masvingo, was subsequently used to track his whereabouts after disappearing with the stolen vehicle. The police enlisted the assistance of a mobile telephone service provider for details on applicant's SIM card including outgoing and incoming calls, dates, time and geographical locations of the calls and messages. The details were used to track the applicant to Harare where he was found in possession of the stolen vehicle.

In the same vein, provisions relating to the right of a person 'not to have their person, home premises or property searched' ought to be interpreted widely to accommodate new meanings of 'search' brought about by technological developments. In other jurisdictions, courts have grappled with new forms of searches associated with technology. In *United States v Jones*[112] the court held that installation by the government of a GPS device on a vehicle to monitor the vehicle's movements,

---

[110] "High-Tech Devices Leave Users Vulnerable to Spies, Phys.org, January 5, 2012 http://phys.org/print244989742.html quoted in Reynolds, G. (2015) "Ethics in Information Technology", 5th Ed. Cengage Learning

[111] *S v Chipetu* HMA 06-17

[112] *United States v Jones* 565 U.S. (2012)

constituted a 'search'. The court highlighted that '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.'[113]

Additionally, the constitutionally guaranteed right to privacy incorporates, *inter alia*, the right of individuals not to have their 'person' searched.[114] In other words, the law protects bodily privacy from unwarranted searches. Given that bodily searches constitute grave intrusion on individuals' privacy, the law requires the search 'to be conducted with strict regard to decency and decorum.'[115] However, the meaning of 'search' as it is ordinarily understood continues to evolve due to technological advances. In high security areas like airports, persons are usually subjected to searches through the use of scanners without physical conduct with the body of the person being searched. Body scanners emit radiation used to identify hidden objects worn on the body or in the clothing of the scanned person, hence these devices have been sarcastically referred to as 'digital strip searchers'.[116]

According to Mironenko 'the use of scanners has a serious impact on passengers' rights, such as the right to privacy and data protection, as well as other fundamental rights.'[117] Body scanners have also been viewed as breaching data protection rights since the production and processing of a person's images amounts to processing of

[113] *Ibid.* p. 3.

[114] Section 57(b) of the Constitution of Zimbabwe

[115] Section 41D(3) of the Criminal Procedure and Evidence Act

[116] See generally Mironenko (n 55 above)

[117] *Ibid.*

personal data.[118] However, such security measures are usually justified in the aviation industry as necessary and reasonable in the interest of national security and public safety.

Another facet of privacy that ICT developments have impacted on relates to a person's right not to have their possessions seized.[119] Search and seizure of computers and mobile phones by law enforcement agents have serious privacy implications for citizens. The portability of cell phones means that law enforcement agents may have access to personal and sensitive information stored on cell phones without warrant in cases of search and seizure of cell phones incident to arrest. It is common for arresting officers to search and seize objects on the arrestee's person where such objects may afford evidence of the commission of crime.[120]

In Zimbabwe there is currently no clear legal safeguards against invasion of privacy during search and seizure of digital devices incident to arrest. Similarly, case law dealing with search and seizure of cell phones during arrest is conspicuous by its absence. However, the issue came close for determination in *The Prosecutor General of Zimbabwe v Mtetwa & Anor*[121] in which a lawyer was charged with obstructing the course of justice by hindering police officers from executing a search warrant at her client's premises. The lawyer allegedly took photos of the proceedings and, when the

[118] *Ibid.*

[119] Section 57(c) of the Constitution of Zimbabwe

[120] Section 51 of the Criminal Procedure and Evidence Act states that a police officer may, without warrant search any person if the person consents to the search or where the officer on reasonable grounds believes that a warrant would be issued if he applied for one and the delay in obtaining a warrant would prevent the seizure or defeat the object of the search.

[121] *The Prosecutor General of Zimbabwe v Mtetwa & Anor* HH 82-16

police officer tried to seize the phone, the lawyer reportedly hid it in her undergarments, and proceeded to delete the photographs and videos after which she handed over the cell phone. The matter was however, disposed on technicalities and the court did not determine the issue.

The obvious ramifications are that technology continues to make incursions into privacy in many ways than one. Inevitably, a question arises whether the current constitutional provisions adequately address potential breaches of privacy necessitated by technological developments? It is submitted that the seeming shortcomings of section of 57 of the Constitution in terms of safeguarding privacy in the digital era are not intractable and, depending on the attitude of the courts, may be cured regard being had to the rules of statutory interpretation.

A close analysis of section 57 of the Constitution shows that the spectra of privacy constitutionally protected by the section are not exhaustive. For the avoidance of doubt, section 57 provides, in part, that 'every person has the right to privacy, *which includes* the right...' The ordinary grammatical meaning of the phrase '*which includes*' denotes that the forms of privacy enumerated in section 57 are not exclusive.[122] The courts are therefore likely to interpret the provisions of section 57 broadly to encompass all conceivable situations where an individual has a reasonable expectation of privacy. Consequently, invasion of one's privacy through electronic surveillance will almost certainly be deemed unconstitutional if a broad, generous and purposive interpretation of section 57 of the Constitution is adopted. This approach

[122] Section 47 of the Constitution of Zimbabwe provides that Chapter 4 (Declaration of Rights) does not preclude existence of other rights and freedoms that may be recognized or conferred by law to the extent that they are consistent with the Constitution.

finds support in the Constitution itself to the extent that it requires courts, when interpreting the provisions of Chapter 4 of the Constitution, to 'give full effect to the rights and freedoms' enshrined therein.[123] It is submitted that new areas of privacy, whether necessitated by technological developments or otherwise, must of necessity find protection under the broad right to privacy enshrined in section 57 of the Constitution.

2.5 Constitutional remedies for breach of privacy

It is one thing to talk about constitutional rights without corresponding mechanisms to enforce such rights. A person must be able to approach the courts to vindicate their constitutional right where such right has been or is likely to be violated. Section 85 of the Constitution deals with enforcement of fundamental human rights and freedoms. The section confers upon any person the right to approach a court alleging that a fundamental right or freedom enshrined in the Constitution has been, is being or is likely to be infringed.[124] In *Mudzuru & Anor v Minister of Justice, Legal and Parliamentary Affairs*[125] the Constitutional Court had the following to say:

> 'Section 85(1) of the Constitution is the cornerstone of the procedural and substantive remedies for effective judicial protection of fundamental rights and freedoms and the enforcement of the constitutional obligation imposed on the State and every institution and agency of the government at every level to protect the fundamental rights in the event of proven infringement. The right to a remedy provided for under s 85(1) of the Constitution is one of the most fundamental and essential rights for the effective protection of all other fundamental rights and freedoms enshrined in Chapter 4.'

[123] Section 46 (1) (a) of the Constitution of Zimbabwe

[124] Section 85(1) of the Constitution.

[125] *Mudzuru & Anor v Minister of Justice, Legal and Parliamentary Affairs* [2015] ZWCC 12 at p. 13

The court may grant appropriate relief, including a declaration of rights and an award of compensation.[126] Accordingly, a person who alleges a breach of their right to privacy may seek recourse in terms of section 85 of the Constitution. The right of a person to approach the courts to assert their constitutional rights or seek compensation is not defeated by the fact that the person has contravened a law.[127] Similarly, a person seeking relief should not be boggled down by formalities or procedural technicalities.[128] As a matter of law, courts are enjoined to develop flexible rules of procedure that ensure citizens are able to enforce constitutional rights and seek appropriate relief with minimum restrictions.

2.6 Conclusion

The first part of this chapter canvassed the meaning, nature and scope of the right to privacy. It was noted that the right to privacy is multi-faceted and cannot be accorded a singular definition. The notion of privacy comprises a 'bundle' of values protected by the law that relate to personal autonomy, liberty, dignity and the individual's instinctive desire for exclusion from the public and publicity in certain spheres of life.

An in-depth analysis of the constitutional framework regulating the right to privacy in Zimbabwe was carried out. The obtaining legal position is that the right to privacy is an integral part of the Declaration of Rights in the Constitution. A critique of the relevant constitutional provisions revealed that not all facets of privacy are explicitly protected by the Constitution thereby creating a lacunae necessitated by developments in the field of ICT. However, the versatility of section 57 of the Constitution makes it

[126] Section 85(1) of the Constitution

[127] *Ibid.*

[128] *Ibid*.

possible for the courts to accord a wider interpretation to cover novel elements attendant to the right to privacy. The chapter also looked at constitutional remedies available in the event of infringement of the right to privacy. The ensuing chapter will continue exploring the legal landscape in Zimbabwe by focusing on other legislation with a direct impact on privacy as well as the common law remedies for breach of privacy.

CHAPTER 3

Statutory and Common Law Protection of Privacy in Zimbabwe

3.0 Introduction

Legal discourse in the previous chapter centred on constitutional protections on the right to privacy in Zimbabwe. This chapter seeks to explore other domestic sources of law with a bearing on the protection of privacy. In particular, focus will be on the Access to Information and Protection of Privacy Act, the Interception of Communications Act, the Criminal Law (Codification and Reform) Act, among others. The chapter will also assess common law remedies for breach of privacy. The essence of this chapter is to ascertain the extent to which the current legal framework in Zimbabwe safeguards the right to privacy as well as to identify any gaps in the law.

3.1 Access to Information and Protection of Privacy Act

Apart from the Constitution, other pieces of legislation purport to protect the right to privacy in Zimbabwe. The Access to Information and Protection of Privacy Act[129] (AIPPA) is the primary legislation in Zimbabwe governing access to information and protection of privacy. It is important to highlight from the onset that this legislation has been incisively criticised as a repressive law designed to control free flow of information rather than make it more accessible.[130] The Act was passed in 2002 before the new Constitution of Zimbabwe 2013. Accordingly, the Act is misaligned with the Constitution of Zimbabwe in a number of material respects.[131]

---

[129] [Chapter 10:27]

[130] See generally MISA Zimbabwe, Foreword to The Access to Information Model Law; C. Ncube (n 104 above) in which the author states that AIPPA 'was viewed in civil society circles largely as a weapon to be used against journalists.'

[131] Section 64(4) of the Constitution of Zimbabwe provides that legislation must be enacted to give effect to the right of access to information.

3.1.1 Objectives of Access to Information and Protection of Privacy Act

The Act regulates an array of diverse and seemingly intractable issues ranging from access to information held by public bodies; personal information privacy and regulation of the media profession, issues which could be conveniently and independently catered for in separate pieces of legislation.[132] For purposes of this research, the focus is on those objectives of the Act relating to the protection of personal privacy and the privacy of personal information (data protection). The Act applies to all matters relating to access to information, protection of privacy and mass media.[133]

The Act, *sensu stricto*, does not protect privacy per se, but provides for protection of personal information against unauthorised collection, use or disclosure by public bodies. Section 25 states that 'the head of a public body shall not disclose personal information to an applicant if the disclosure will result in the unreasonable invasion of a third party's personal privacy.' As such, the provisions of the Act in this regard may be aptly described as data protection legislation as opposed to privacy legislation in general. The view that there is no data protection legislation in Zimbabwe is therefore somewhat incorrect. The position of the law is that the Act protects personal information from unauthorised collection, use or disclosure by public institutions, which in essence is the objective of data protection legislation.

[132] MISA Zimbabwe states that 'the law lumps together media regulation with citizens' fundamental right to access to information, which two issues should be treated and legislated separately in line with regional and international best practice.' See MISA Zimbabwe Foreword to the Access to Information Model Law.

[133] Section 3 of the Act

3.1.2 Data protection principles

In Zimbabwe, jurisprudence in the field of data protection is virtually undeveloped although the country is one of the first nations on the African continent to promulgate legislation incorporating some principles of data protection.[134] However, literature shows that 'a number of national and international privacy frameworks have largely converged to form a set of core, baseline data protection principles.'[135] These rudimentary principles have been designed to safeguard personal data from wanton abuse by data controllers. These data protection principles 'are at the root of data protection law'.[136] The principles are 'fair information practices' developed and adopted by international human rights bodies that informed the development of national laws on data protection.

Part V of the AIPPA covers data protection principles relating to the collection, protection and retention of personal information by public bodies. Section 30(2) of AIPPA incorporates the *fair and lawful processing principle* and requires a public body to inform a person from whom it intends to collect personal information not only the purpose for which the personal information is being collected, but also the 'legal authority' for collecting it. The principle encapsulates the notion that 'those who process information concerning individuals are subject to a regulatory framework within which they can process personal data lawfully'.[137] Similarly, the

[134] AIPPA was promulgated in 2002. Other countries introduced data protection legislation much later. For instance, South Africa enacted data protection legislation in 2013.

[135] Personal Data Protection Guidelines for Africa: A joint initiative of the Internet Society and the Commission of the African Union, 2018 p. 9.

[136] D. I. Bainbridge, *Introduction to Information Technology Law*, 6th Ed. Pearson Education Limited, 2008. 503

[137] *Ibid*. 497

principle requires that data must be processed fairly if due regard is to be had to the rights of the individual whose personal data is being processed. Section 36 of AIPPA also incorporates the '*purpose specification principle*' as one of the cardinal principles of data protection. The section stipulates that

> 'a public body may only use personal information
> (a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose; or
> (b) if the person to whom the information relates has consented, in the prescribed manner, to such use.'

This principle states that a data controller may collect, store, and use an individual's personal data or information only for a specified and lawful purpose. In addition, personal information may not be utilised for purposes other than for, or incompatible with, the original purpose for which the information was collected or processed. Thus the use of personal data for purposes other than those specified should occur only with the consent of the data subject or with legal authority.[138] The Act also enshrines the right of the data subject to be informed of the *purpose* for which the personal information is being collected and the *legal authority* for collecting the personal information.[139] This data protection principle thus enables a data subject to have some semblance of control over their personal information.

Other data protection principles enshrined in the Act include the *adequacy and relevance data principle*; *accuracy of data principle*;[140] *data retention principle*;[141]

---

[138] L. A. Bygrave "Data Protection to the Right to Privacy in Human Rights Treaties" *Journal of Law and Information Technology*, Vol. 6 247-284

[139] Section 30(2) of AIPPA

[140] Section 31 of AIPPA

[141] Section 34 of AIPPA. See *Pazvakavambwa v Portcullis (Pvt) Ltd* HH-175-11 which bears testimony to the ugly side of retention of personal information for longer than necessary.

data rectification principle and the *data security principle*.[142] The adequacy and relevance data principle is concerned with limitations imposed by the law relating to the relevance and quantum of personal information a data controller may process in relation to a particular purpose. In Zimbabwe, the biometric voters registration sparked debate on whether the inclusion of voters' photos on the voters roll was not excessive as to violate their privacy.[143]

The *data rectification principle* is important in order to safeguard against false, incorrect or incomplete personal information held by public bodies.[144] As one author puts it:

> 'Various types of information – be it truthful, false, outdated or taken out of context – may cause harm to individuals, and may threaten important values, such as dignity or personal autonomy, which are protected by the right to privacy under international human rights law.'[145]

The data rectification principle resonates with the constitutional right 'to the correction of information, or the deletion of untrue, erroneous or misleading information, which is held by the State or any institution or agency of government'.[146] The data rectification principle is premised on the right of access to information, for without access to information one cannot know that information held by others is not incorrect, inaccurate or misleading. As such the underlying right of access to information is the foundation upon which data subjects may be able to have their data

[142] Section 33 of AIPPA

[143] See article 'People Speak on Voters' Roll – Pictures Violate Privacy' The Herald, 27 June 2018 at page 3.

[144] Section 32(1) of AIPPA provides that "Where a person has reason to believe that personal information relating to him that is in the custody or control of a public body contains an error or omission, he may request the head of that public body to correct such information."

[145] Article 19 (n 37 above). 4

[146] Section 62(3) of the Constitution of Zimbabwe

held by others corrected. Albeit the Act provides for important data protection principles, it is disappointing to note that these principles have largely remained dormant. The Act attracted attention for the wrong reasons and is on the verge of being relegated to the dustbins of repealed legislation.

3.1.3 Freedom of Information Bill and Cybersecurity and Data Protection Bill

The Access to Information and Protection of Privacy Act has been trenchantly criticized for various reasons. The Stakeholder Report on the Right to Privacy in Zimbabwe highlights that 'the Act's title is a misnomer, as it does not serve to protect privacy, but instead allows the government to control aspects of the media, through measures such as the accreditation of journalists.'[147] Even with the data protection principles, the Act only applies to personal information held by public institutions. However, the Act will be repealed if the Freedom of Information Bill[148] becomes law. Although a detailed discussion of the bill is beyond the scope of this thesis it is important to highlight some of the salient provisions contained therein.

The objectives of the bill are to 'provide for the constitutional rights of expression, and freedom of the media; to provide further for the right of access to information held by entities in the interest of public accountability or for the exercise or protection of a right.' For purposes of the right to privacy, clauses 21 and 22 provide for the protection of personal information of natural and juristic persons, respectively. In terms of the bill, information officers are compelled to refuse a request for access to information if the access results in disclosure of confidential information.

[147] Stakeholder Report (n 38 above). 4

[148] Freedom of Information Bill [H.B. 6, 2019]

A Cybersecurity and Data Protection Bill[149] is also in the pipeline awaiting publication in the Government Gazette. If it comes into law, the bill will, inter alia, criminalize dissemination of data concerning an identifiable person knowing it to be false and intending to cause psychological or economic harm. The bill will also address offences relating to cyber bullying and harassment, among others things.

3.2 Criminal Law (Codification and Reform) Act

The Criminal Law (Codification and Reform) Act seeks to protect both the concept of privacy and the notion of dignity by proscribing any serious impairment of the dignity of a person or invasion of the privacy of another. Section 95(1) of the Code states:

> 'Any person who, by words or conduct –
>
> (a) seriously *impairs the dignity* of another person; or
>
> (b) seriously *invades the privacy* of another person;
>
> shall be guilty of criminal insult if he or she intended his or her words or conduct to have an effect referred to in paragraph (a) or (b) or if he or she realized that there was a real risk or possibility that his or her words or conduct might have such an effect.'

The legal position is that privacy is also protected under criminal laws of Zimbabwe. Thus any act that seriously impairs the dignity or privacy of another is a criminal offence attracting serious sanctions under the Code.[150] In order for a person to be convicted of criminal insult in terms of section 95(1) of the Code, the words or conduct must seriously impair the dignity of another person or seriously invade the privacy of another person. The 'words' or 'conduct' therefore constitute the physical ingredients (*actus rea*) of the offence.

In addition, a person is guilty of criminal insult if the intention in uttering the words

[149] [H.B. 18, 2019]

[150] The offence attracts a fine not exceeding level six or imprisonment for a period not exceeding one year or both. See section 95 (1) of the Criminal Law (Codification and Reform) Act.

or perpetrating the conduct is to seriously impair the dignity or invade the privacy of another. In other words, the mental ingredients (*mens rea*) of the offence must be established.[151] Alternatively, a person may be convicted of the offence if he lacked the requisite criminal intent but realized that there was a real risk or possibility that his or her words or conduct might result in serious impairment of the dignity or invasion of the complainant's privacy. In *Phiri v The State*[152] appellant was convicted of criminal insult for contravening section 95(1) of the Code in that he had allegedly uttered words that unlawfully and seriously impaired the dignity of the complainant. On appeal the conviction was quashed on the basis that appellant's guilt had not been proven beyond reasonable doubt.

New forms of threats to privacy have emerged as a result of technological developments such as revenge pornography. To this end, the provisions of section 95 of the Criminal Law Code are pertinent in the world of technology where it is easy for a person to publish material online which may impair the dignity or privacy of another. Cases of persons who publish intimate videos or photographs of another on social media platforms are on the increase[153] and the Criminal Law Code may be potentially used to prosecute offenders to dissuade invasion of privacy.

Chapter VIII of the Criminal Law Code deals with computer-related crimes. Some of the offences include unauthorized access or use of computers;[154] unauthorized use or

[151] See *S v I & Another* 1976 (1) SA 781: 788E-F in which the court concluded that accused had the necessary *mens rea* to be convicted of criminal *injuria* when she entered upon the private property of complainant and peeped at her whilst she was lying in bed in the company of a man.

[152] *Phiri v The State* HB 139/16

[153] There are currently no known statistics in Zimbabwe but the print media regularly publish stories involving such cases.

[154] See section 163 of the Criminal Law Code

possession of credit or debit cards;[155] and unauthorized use of password or pin number.[156] The offences are, inter alia, intended to protect the privacy of information in computer systems and personal information in digital form such as financial records. However, there is currently no comprehensive computer and cyber crime legislation in Zimbabwe and as such, personal information in digital form may be susceptible to hacking. This has implications on privacy where unauthorized access to digital information may result in disclosure of confidential and personal information.

3.3 Interception of Communications Act

One of the key facets of the right to privacy protected by the Constitution is the right of every person 'not to have the privacy of their communications infringed.'[157] Needless to say, interception of communications constitutes a grave danger to privacy. Interception of communications connotes unjustified meddling with the right to privacy of communications. Developments in the ICT industry have made it extremely easy to intercept communications and to carry out electronic surveillance on citizens.[158] Despite constitutional safeguards against unwarranted interception of communications, the law recognizes the need to intercept communications in order to serve other legit interests such as law enforcement and national security. As observed

[155] See section 167 of the Criminal Law Code

[156] See section 168 of the Criminal Law Code

[157] See section 57 (d) of the Constitution

[158] R. K. Suri, P. Diwan & S. Kapoor, *Information Technology Laws (Laws relating to cyber & e-commerce)* Pentagon Press, 2000. 193-194 highlight that: 'With the ability to digitize any form of information, boundaries between the various forms of surveillance are disappearing with the application of information technology linking surveillance techniques into a near seamless web of surveillance...'

by Goldsmith[159] 'the question of electronic surveillance has long posed a classic confrontation between privacy interests and the need for effective law enforcement.' To this end, interception laws tend to limit the right to privacy. The law should strive to strike a balance between the competing interests to ensure that citizens' privacy rights are not jeopardized while at the same time ensuring that national interests are not compromised.

3.3.1 Objectives of Interception of Communications Act

The Interception of Communications Act (IoCA)[160] is the primary legislation regulating interception of communications in Zimbabwe. The Act provides for the 'lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or other related service or system in Zimbabwe.' Section 2 of the Act defines 'interception' as follows:

> "intercept", in relation to any communication which is sent -
> (a) by means of a telecommunication system or radiocommunication system, means to listen to, record, or copy, whether in whole or in part;
> (b) by post, means to read or copy the contents, whether in whole or part;"

The wording of section 2 of the IoCA suggests that a communication may only be intercepted during the course of its transmission,[161] that is, in the process of being broadcast or sent out from one person or place to another. Hale and Edwards,[162] define 'interception' as follows:

> 'A person intercepts a communication *in the course of its transmission* if, as a result of his interference in the system or monitoring of the transmission, some or all of the contents are

[159] M. Goldsmith, 'The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance', 74 *Journal of Criminal Law & Criminology* 1. 3

[160] [Chapter 11:20] Act No. 6 of 2007

[161] Section 3(1) of IoCA

[162] A. Hale & J. Edwards 'Getting it Taped' (2006) 12 *Computer and Communications Law Review* 71

made available, while being transmitted, to a person other than the sender or the intended recipient of the communication.' (Emphasis supplied)

The end result is that information or data is incapable of interception unless it is being transmitted or communicated. This implies that a person who accesses data or information resident in a computer cannot be said to be intercepting communications.

3.3.2 Prohibition against interception of communications

The legal position is that interception of communications is generally prohibited in Zimbabwe because it impinges on the right to privacy. The IoCA outlaws interception by stipulating that no person shall intercept any communication in the course of its transmission by means of a telecommunication system or radiocommunication system. [163] There are however exceptions to the general prohibition against interception. Thus interception is legally permissible where the person intercepting the communication is a party to the communication,[164] or they have the consent of the person to whom, or the person by whom, the communication is sent;[165] or he or she is authorized by warrant.[166] Section 3(2) of the IoCA provides that subsection (1) shall not apply to the bona fide interception of a communication for the purpose of or in connection with the provision, installation, maintenance or repair of a postal, telecommunication or radiocommunication service.

Thus the Act protects the privacy of communications by generally prohibiting interception of communications. The Act categorically makes it an offence for any

[163] Section 3(1) of IoCA

[164] Section 3(1)(a) (i) of IoCA

[165] Section 3(1)(a) (ii) of IoCA

[166] Section 3(1)(a) (iii) of IoCA

person to intentionally intercept or attempt to intercept, authorize or procure any other person to intercept any communication in the course of its occurrence or transmission. [167] Accordingly, the gist of section 3 is that interception of communications is unlawful save in circumstances provided in the Act.

There is little case law on unlawful interception of communications in Zimbabwe. However, a case in point is *Paradza v Chirwa N.O. & Ors*[168] in which applicant, a judge, had his telephone conversation with another judge tape-recorded. The case revolved around the admissibility of the tape-recorded evidence, with applicant contending that the evidence would infringe his constitutional right to a fair hearing because the evidence was obtained in breach of applicant's right to the privacy of communications enshrined in the constitution. The court highlighted that 'it is not our law that evidence obtained as a result of an unlawful interception of a telephone conversation should be excluded from use in court proceedings.' However, section 8 of the IoCA provides that evidence obtained through unlawful interception shall not be admissible in any criminal proceedings except with the leave of the court.[169]

3.3.3 Critique of the Interception of Communications Act

Section 86 of the Constitution of Zimbabwe permits limitations of rights and freedoms only in terms of a law of general application. There is no doubt that the

[167] Section 3(3) of IoCA. The offence attracts a penalty of a fine not exceeding level fourteen or imprisonment for a period not exceeding five years or both.

[168] *Paradza v Chirwa N.O. & Ors* SC 25/05

[169] See also *S v Naidoo* 1998 (1) BCLR 46 (D) where it was held that the monitoring done subsequent to the direction issued by a judge on the basis of false information could not constitute a limitation on the right to privacy in terms of the Interception and Monitoring Prohibition Act 127 of 1992, but was an unwarranted violation of the accused's right to privacy. See also *Tap Wine Trading CC and Anor v Cape Classic Wines (Western Cape) CC and Anor* 1999(4) SA 194 (K).

Interception of Communications Act is a law of general application. In addition, section 86 of the Constitution provides that the limitation must be fair, reasonable, necessary and justifiable in a democratic society. One of the relevant factors to be taken into account is the purpose of the limitation, that is, whether it is necessary, for instance, in the interests of defence, public safety, public order, public health or the general public interest.[170]

One of the grounds upon which interception of communications may be justified is when a warrant is issued authorizing such interception. The Minister may, in terms of section 6(1) of the IoCA issue a warrant where he/she has reason to believe that a serious offence has been or is likely to be committed. Additionally, the warrant may be issued where there is an actual threat to 'national security' or compelling 'national economic interest' or a potential threat to 'public safety' or 'national security'. The Act does not define these wide terms and this renders the provisions prone to abuse. In order protect privacy of communications, applicants for interception warrants must show that other investigative procedures have failed to yield the required information or evidence.[171] This provision is in sync with section 86(2)(f) of the Constitution which provides one of the relevant factors to taken into account for purposes of a limitation of constitutional rights is 'whether there are any less restrictive means of achieving the purpose of the limitation.'

Although the IoCA somewhat satisfies some of the relevant factors justifying limitation of constitutional rights, a major drawback to the interception legislation is that it confers sweeping powers on the Minister to issue and cancel warrants of

[170] Section 86(2)(b) of the Constitution of Zimbabwe

[171] Section 5(3)(e) of the IoCA

interception. Ideally, the power to issue warrants should ordinarily reside in judges or magistrates to provide for judicial oversight.[172] This ensures that an impartial and detached authority is interposed between law enforcement agents and citizens whose privacy rights are subject of infringement. Section 6 of the Act enjoins the Minister to issue a warrant to authorized persons if there are 'reasonable grounds' to believe that a serious offence by an organized criminal group has been or will be committed. The use of the words, 'has reason to believe' in the statute leaves too much to the discretion of the Minister in deciding whether to issue a warrant or not. There are no set parameters to curtail the powers of the Minister in this regard.

Section 7 of the IoCA deals with the scope of the warrant for interception of communications. The warrant issued under the Act is valid for such a period not exceeding three months but may, on good cause being shown by the authorized person, be renewed for a further period of six months by the Minister in case of serious offences by an organized criminal group or by the Minister in consultation with the Attorney-General where offences in the Schedules to the Criminal Procedure and Evidence Act are involved. It is contended that a period of six months of monitoring and intercepting communications of citizens is unduly long and constitutes unwarranted intrusion on privacy particularly where it eventually turns out that the target did not commit any offence.

[172] Warrants of search and seizure in Zimbabwe are issued by a Magistrate or Justice of Peace in terms of section 54(2)(b) as read with section 50(1)(a) of the Criminal Procedure and Evidence Act [Chapter 9:07].

Monitoring, surveillance and interception of communications under the Act may be virtually perpetual as section 7(4) gives the Administrative Court powers to renew the warrants successively for periods not exceeding three months at a time. The absence of or limited judicial oversight on the issuance of interception warrants is the *Achilles heel* of the legislation on interception of communications in Zimbabwe. These shortcomings may be manipulated by agents of the state to carry out untrammelled surveillance on citizens in flagrant breach of the privacy of their communications. It is submitted that the powers of the Minister to issue and extend warrants of interception of communications are 'too broad and overreaching to be reasonably justified in a democratic society.'[173]

3.4 Postal & Telecommunications (Subscriber Registration) Regulations

Legislation regulating postal and telecommunications services in Zimbabwe also have a positive and negative bearing on the right to privacy. On the positive side, the Postal and Telecommunications Act[174] prohibits the disclosure of confidential information and use of information acquired by inspectors or employees of POTRAZ in the course their duties.[175] The nature of information protected from disclosure or use for personal gain includes information relating to financial affairs of a person or commercial secrets.[176]

A number of regulations issued under the Postal and Telecommunications Act also seek to protect certain information from abuse or disclosure. For instance, section

[173] *Law Society of Zimbabwe v Minister of Transport and Communications & Anor* SC 59/2003

[174] [Chapter 12:05]

[175] See section 104 of the Act

[176] Section 104 (a) & (b) of the Act

15 of the Postal and Telecommunication (Internet Services) Regulations, 2001,[177] makes it a condition of issuance of a licence for licensees to sign a declaration of secrecy undertaking not to disclose the contents of any message received by means of an internet service, its origin, destination or existence.

The Postal and Telecommunications (Subscriber Registration) Regulations of 2014[178] prohibits telecommunications and internet service providers from activating a SIM card[179] or providing a service unless customer details have been registered.[180] It also requires telecommunication service providers to implement systems to enable them to obtain, record and store subscribers' personal details such as full names, permanent residential addresses, nationality, gender, subscriber identity numbers, national identification numbers or passport numbers.[181] The regulations also authorize POTRAZ to establish and maintain a central subscriber information database for storage of subscriber information.[182] Albeit the regulations require subscriber information contained in the central database to 'be held on strictly confidential

[177] Statutory Instrument 262 of 2001

[178] Statutory Instrument 95 of 2014

[179] SIM is an acronym for 'Subscriber Identity Module'. 'The SIM card has the capacity to holds mostly personal information of the subscriber. Such information includes text messages, phone number, address book and other relevant data.' See O. Kufandirimbwa, N. Zanamwe, G. Hapanyengwi, & G. Kabanda Mobile Money in Zimbabwe: Integrating Mobile Infrastructure and Processes to Organisation Infrastructure and Processes *Online Journal of Social Sciences Research*, Vol. 2, Issue 4, (2013) 92-110 Available Online at http://www.onlineresearchjournals.org/JSS

[180] Section 3(1) of the Regulations

[181] See Section 4(1) of SI 95 of 2014

[182] See section 95 of the Regulations

basis'[183] such personal information may be abused in the absence of proper legal safeguards.[184]

The Postal and Telecommunications (Subscriber Registration) Regulations have grave implications on the privacy of personal information of subscribers. As aptly observed by one author:

> 'SIM card registration, in particular, violates privacy in that it limits the ability of citizens to communicate anonymously. It also facilitates the tracking and monitoring of all users by law enforcement and intelligence agencies. Research shows that SIM card registration is not a useful measure to combat criminal activity, but actually fuels the growth of identity-related crime and black markets to those wishing to remain anonymous.'[185]

In the Canadian case of *R v Spencer*,[186] the court held that the respondent had a reasonable expectation of privacy with respect to his subscriber information. The court noted that 'subscriber information, by tending to link particular kinds of information to identifiable individuals, may implicate privacy interests relating to an individual's identity as the source, possessor or user of that information.'

Although the regulations prescribe the circumstances upon which subscriber information may be released, it remains debatable whether sufficient legal safeguards are in place against arbitrary infringement of citizens' personal privacy and privacy of communications. According to MISA Zimbabwe, 'while [the regulations] could be in

[183] Section 8(5) of SI 95 of 2014

[184] Statutory Instrument 95 of 2014 was preceded by Statutory Instrument 142 of 2013 Postal and Telecommunications (Subscriber Registration) Regulations which was hastily repealed after a public outcry. SI 142 of 2013 was repealed after 8 months in operation. However, the provisions of SI 95 of 2014 are substantially similar to the repealed provisions of SI 142 of 2013.

[185] Stakeholder Report Universal Periodic Review, 'The Right to Privacy in South Africa', 27th Session, October 2016. 12

[186] *R v Spencer* [2014] SCC 43

keeping with other international jurisdictional trends to fight, detect and curb ICT-generated crimes, the regulations and requirements therein, should not be as broad and vague as obtains in the Zimbabwean scenario. They should be narrowly defined to avert infringement of fundamental human rights.'[187] Suffice it to say that the regulations are unconstitutional and have far-reaching implications as subscribers' personal information may be released to law enforcement agencies without a warrant or any form of judicial oversight.

3.5 Right to Privacy under Common Law

The Zimbabwean legal system largely hails from the Roman-Dutch law system. Under the law of delict the concepts of dignity and privacy are generally protected by the *actio injuriarum*. The protection of the right to privacy under the *actio injuriarum* was amply explained in the South African case of *NM & Ors v Smith*[188] as follows:

> 'The right to privacy finds protection in the law of delict and, specifically, in the *actio injuriarum*. This cause of action, recognised since the classical Roman period, protects a range of personality rights under the Latin terms *corpus*, *fama* and *dignitas* – which can loosely be translated respectively, as physical and mental integrity, good name and dignity understood in a broad sense. Privacy has been protected under the rubric of *dignitas*. The elements of the *actio injuriarum* are the intentional and wrongful infringement of a person's *dignitas*, *fama* or *corpus*.'

In *Rhodesian Printing and Publishing Co Ltd v Duggan*[189] the Rhodesia Appellate Division observed that 'prima facie every person has an inborn right to the tranquil enjoyment of his peace of mind' and that 'every incursion of that right is an *injuria*.' The delict of *injuria* is actionable where a person affronts another person's dignity or

[187] See MISA Zimbabwe Statement on the Postal and Telecommunications (Subscriber Registration) Regulations, 1 April 2016.

[188] *NM & Ors v Smith* [2007] ZACC 6; 2007 (5) SA 250 (CC) (footnotes omitted)

[189] *Rhodesian Printing and Publishing Co Ltd v Duggan* 1975 (1) SA 590 (RA) at p 590.

invades their privacy. In *Chituku v Minister of Home Affairs & Ors*[190] the court held that 'the right to dignity is recognized in the Roman-Dutch law as an independent right that can be protected by the *actio injuriarum*.' The court cited with approval the case of *Minister of Police v Mbilini*[191] where it was stated that:

> 'It is trite law that one of the rights which is protected by the actio injuriarum is the right to an unimpaired dignity. Dignity was defined by Melius de Villiers in 1899 in his well-known work *The Roman and Roman-Dutch Law of Injuries* at 24 as-'that valued and serene condition in his social or individual life which is violated when he is either publicly or privately, subjected by another to offensive and degrading treatment, or when he is exposed to ill-will, ridicule, disesteem or contempt.'

A person should have a reasonable expectation of privacy in order to enjoy protection of the right under the common law. The right is subject to the dictates of the society and to other rights. A person seeking recourse for an invasion of privacy under the *actio iniuriarum* must prove (i) impairment of their privacy; (ii) wrongfulness; and (iii) intention (*animus injuriandi*).[192]

In Zimbabwe, various facets of the right to privacy have been protected under the common law. For instance, in *Reid-Daly v Hickman*[193] the court noted that the 'planting of a listening device in an apartment does of itself amount to an impairment of the occupier's *dignitas*.' In this case plaintiff alleged invasion of his *dignitas* and privacy *animo injuriandi* on the grounds that certain military officers had tapped his telephone and kept him under surveillance. The case is also authority for the legal

[190] *Chituku v Minister of Home Affairs & Ors* 2004 (1) ZLR 36 (H)

[191] *Minister of Police v Mbilini* 1983 (3) 705 (AD) 715G

[192] *NM & Ors v Smith & Ors* [2007] ZACC 6; 2007 (5) SA 250 (CC)

[193] *Reid-Daly v Hickman* 1980 ZLR 201, 1981 (2) SA 315 (ZA) 323

proposition that surreptitious removal and copying of another person's personal documents constitutes a wrongful invasion of privacy.[194]

The right to privacy is also infringed under common law when a person's private facts are disclosed. Each person has a right to decide what aspects of his or her life he or she wishes to keep private from unauthorized disclosure.[195] Disclosure of private facts may also entail unauthorized possession or publication of personal information. In *Mr. & Mrs. "X" v Rhodesia Printing & Publishing Co. Ltd*[196] the publication of a dispute pertaining to custody of children by a newspaper was held to be an offensive invasion of the right to privacy 'going beyond the bounds of decency.' Davies J was satisfied that 'such conduct would in our law be regarded *prima facie* as an *injuria*, giving rise to an action for damages or, in appropriate cases, to a right to claim an interdict.'[197]

Not all invasions of privacy have been held unjustified under common law. In *S v Israel & Anor*[198] a woman hired a private detective to secure evidence of adultery of her husband for purposes of a divorce action. The detective peeped through the window and saw the husband in bed with another woman. The court held that the invasion of privacy was justified as this was done for a bona fide motive of obtaining evidence of adultery.

---

[194] *Ibid.* at p. 323

[195] See G. Feltoe, *A Guide to the Law of Delict in Zimbabwe*, 3rd Ed. Legal Resources Foundation, 2006

[196] *Mr. & Mrs. "X" v Rhodesia Printing & Publishing Co. Ltd* 1974 (4) 508 (R) at 513E-F

[197] *Ibid.* 513E-F

[198] *S v Israel & Anor* 1975 (2) RLR 191 (A)

The common law also provides remedies for breach of privacy. For instance, an interdict may be an appropriate remedy in circumstances where there is threatened wrongful publication of private facts. Needless to say, the aggrieved person will be required to satisfy the well-settled requirements for an interdict. The *locus classicus* on the subject is *Setlogelo v Setlogelo*[199] in which the court set out the requirements for an interdict.

In *Mr. & Mrs. "X" v Rhodesia Printing & Publishing Co. Ltd*[200] the court held that the applicants had, on behalf of their children, a clear right to privacy and that the only effective means of enforcing that right was by way of an interdict. However, in *Mandaza v Daily News & Anor*[201] the court refused to grant an interdict to prevent publication of photographs of a person's properties on the basis that the right to privacy only extends to unlawful intrusion into privacy. Damages are also a primary remedy in an action for breach of privacy. A person who, without reasonable justification, invades the privacy of another may be liable to a claim for delictual damages.[202] In *Zimunya v Zimbabwe Newspapers (1980) Ltd*[203] the court was seized with a claim for damages following the publication of a photograph in a newspaper misleadingly suggesting plaintiff relieving himself outside some offices. The court awarded damages for *injuria*.

[199] *Setlogelo v Setlogelo* 1914 AD 221. See also *Tribac (Pvt) Ltd v Tobacco Marketing Board* 1996 (2) ZLR 52 (S) 56 B-D for the requirements of a mandatory interdict.

[200] *Mr. & Mrs. "X" v Rhodesia Printing & Publishing Co. Ltd* 1974 (4) SA 508

[201] *Mandaza v Daily News & Anor* 2002 (2) ZLR 296 (H)

[202] See generally Feltoe, (n 195 above). 206

[203] *Zimunya v Zimbabwe Newspapers (1980) Ltd* 1994 (1) ZLR 35 (H)

3.6 Conclusion

This chapter discussed various legislative enactments with a bearing on the right to privacy in Zimbabwe. One such legislation is the defunct Access to Information and Protection of Privacy Act. The Act does not protect the right to privacy in its entirety but merely deals with privacy of personal information. The provisions of the Interception of Communications Act were also explored to ascertain the extent to which the law protects the privacy of communications. The major drawbacks of the Interception of Communications Act were also highlighted. The chapter concluded by looking at the common law action and remedies for breach of privacy. The next chapter covers international human rights instruments on the right to privacy.

CHAPTER 4

International and Regional Instruments on the Right to Privacy

4.0 Introduction

The right to privacy has been described as 'something that forms the foundation of, or at least part of the justification for, various rights espoused throughout human rights treaties and legislation.'[204] Thus privacy not only finds legal protection in local jurisdictions but also recognition in international human rights jurisprudence. The right is also guaranteed explicitly and implicitly in various international and regional treaties and national constitutions the world over. The preceding chapters delved into the legal framework regulating the right to privacy in Zimbabwe. The main objective of this chapter is to scrutinize a number of notable international and regional human rights instruments undergirding the right to privacy. An international perspective on the right to privacy is also imperative given the extra-territorial surveillance of communications capabilities in the digital era.[205]

The essence of the discourse in this episode is to ascertain the extent to which Zimbabwean privacy laws conform to international benchmarks. The primary focus will generally be on hard law international instruments due their binding nature as opposed to soft law instruments. However, soft law instruments in the international legal arena will be referred only to the extent that they are pertinent.

---

[204] A. Conte, 'Privacy, Honour and Reputation' in Conte, A. & Burchill, R. (eds), *Defining Civil and Political Rights, The Jurisprudence of the United Nations Human Rights Committee*, 2nd Ed. Ashgate Publishing Ltd, 2009. 201

[205] For instance, Edward Snowden exposed nefarious activities of the National Security Agency (NSA) involving extra-territorial surveillance activities over countries around the world.

4.1 Universal Declaration of Human Rights

The Universal Declaration of Human Rights of 1948 (UDHR) is one of the earliest international human rights instruments to recognize the right to privacy. Diggelmann and Cleis[206] posit that 'the right to privacy became an international human right before it was a nationally well-established fundamental right.' The UDHR has inspired many international and regional human rights treaties and constitutional frameworks. The UDHR is pertinent by virtue of Zimbabwe's membership to the United Nations General Assembly. The right to privacy is espoused in Article 12 of the UDHR, which provides that:

> 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

The wording of Article 12 is expansive and guarantees, not only protection against indiscriminate interference with a person's privacy in general, but also the privacy of the family, home as well as privacy of correspondence. In the same vein, Article 12 does not merely provide for the right to privacy but also confers on all human beings the right to the protection of the law against infringement of their privacy. The use of the word 'protection' in the Article implies more duties for the State than the obligation to respect the freedom from interference.[207] The corollary is that Article 12 places a positive obligation on States to develop a conducive legal framework to enable citizens to enjoy their right to privacy and to seek the protection of the law in the event that the right is under siege.

---

[206] Diggelmann & Cleis (n 58 above)

[207] Diggelmann & Cleis (n 58 above). 448

Against this backdrop, it is important to ascertain the extent to which the Zimbabwean legal system adheres to the objectives of Article 12 of the UDHR. As highlighted in Chapter 2 of this thesis, the Constitution enshrines the right to privacy in section 57. The length and breadth of the section 57 right cover various facets of privacy including protection of the home, premises, property and possessions against unauthorized entry, search or seizure. It also protects the privacy of communications against infringement. In this regard, section 57 provides wider protection than Article 12 which prohibits arbitrary interference with a person's correspondence. It is submitted that the term 'communications' is broader in its import than 'correspondence'. Section 57 also seeks to protect the privacy of a person's health condition, a protection of which is not provided in Article 12 of the UDHR.

The inclusion of the right to privacy and enforcement mechanisms in the Constitution of Zimbabwe is, at least on paper, commendable and in line with the standards of the UDHR. However, whether Zimbabwean citizens enjoy the full scope of the right to privacy in practice is a story for another day. Suffice it to say that the privacy laws of Zimbabwe appear to be in sync with the Universal Declaration of Human Rights.

4.2 International Covenant on Civil and Political Rights

Zimbabwe ratified the International Covenant on Civil and Political Rights 1966 (ICCPR) on 13 May 1991 and therefore bound by its provisions. The right to privacy as enshrined under the ICCPR is modeled along the provisions Article 12 of the Universal Declaration of Human Rights. Article 17 of the ICCPR 'protects the important right to privacy, family, home and correspondence.'[208] Conte[209] highlights

[208] J. Rehman, *International Human Rights Law – A Practical Approach*, Pearson Education, 2003. 77

that 'the ICCPR guarantees privacy as a right in and of itself, the scope of which is detailed under article 17 of the Covenant'. For the avoidance of doubt, Article 17 of the ICCPR states:

> 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.

As with Article 12 of the UDHR, Article 17 of the ICCPR guarantees personal privacy as well as that of family and home.[210] The term 'home' has been extrapolated to extend, not only to the place where a person resides, but also to the place where a person carries out his or her usual occupation.[211]

Article 17 of the ICCPR has been construed as also providing protection of the privacy of correspondence and communication in whatever form.[212] The Human Rights Committee succinctly explained this in General Comment 16 when it said:

> 'Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.' [213]

The Article has also been interpreted to include protection of personal information held by public authorities and private individuals or bodies. Thus individuals have the

---

[209] Conte (n 204 above). 201

[210] In *Ngambi v France*, [Communication 1179/2003, UN Doc CCPR/C/81/D/1179/2003 (2004), para 6.5] the Human Rights Committee noted that inquiries conducted by French authorities concerning status and family relations, following a request for a visa for family reunification, amounted to a necessary interference upon private and family life.

[211] See Conte (n 204 above). 217

[212] For instance, in *Estrella v Uruguay* Communication 74/1980, UN Doc CCPR/C/18/D/74/1980 (1983), para 9.2 it was acknowledged that protection against interference with a person also extended to measures of control and censorship over prisoners' correspondence.

[213] See para 8 of the General Comment 16

ability to ascertain personal data stored about them as well as the right to request rectification or elimination of information that the individual believes is incorrect.[214] Although Articles 12 and 17 of the UDHR and the ICCPR, respectively, are almost identically worded, 'the sole difference between the two norms is that Article 17 of the ICCPR not only prohibits 'arbitrary' interferences with one's privacy and with more specific aspects of the private sphere, but also 'unlawful' ones.[215]

The essence of Article 17 is that interference with a person's privacy can only be justified if it is neither 'arbitrary' nor 'unlawful'. In this regard, 'arbitrary' interference with the right to privacy connotes an interference with privacy by random choice or on the basis of mere opinion or interference that is unrestrained or despotic.[216] On the other hand, 'unlawful interference' denotes a situation where the law provides for circumstances constituting lawful interference with privacy, and the interference falls short of conformance with such law. In *Garcia v Colombia*,[217] the Human Rights Committee stressed that article 17 of the Covenant requires any interference with privacy to be lawful, as well as not arbitrary.

The implications of Article 17 are obvious: if a State wishes to authorize interference with the right to privacy, then it can only do so on the basis of the law.[218] Similarly, any such prescription by law must itself comply with the provisions, aims and objectives of the ICCPR.[219] Indeed, Article 4 of the ICCPR permits States to

[214] Conte (n 204 above). 207

[215] Diggelmann & Cleis (n 58 above). 449

[216] Conte (n 204 above). 204

[217] *Garcia v Colombia* Comm. 687/1996, U.N. Doc. A/56/40, Vol. II, at 48 (HRC 2001)

[218] Conte (n 204 above). 204

[219] *Ibid*, p. 204

temporarily derogate from their obligations in time of public emergency threatening the life of the nation. However, interference with the right to privacy not prescribed by law remains proscribed and unjustified under the provisions of Article 17.

A case in point is *Van Hulst v The Netherlands*[220] that involved the surveillance of telephone conversations in which an author's calls with his lawyer were intercepted and recorded. The Committee acknowledged the importance of safeguarding the confidentiality of communications, particularly those relating to the attorney-client relationship, but also highlighted the need for States to take effective measures for the prevention and investigation of criminal offences. The Committee held that there was no infringement of article 17 of the ICCPR as the interference was proportionate and justified to achieve the legitimate purpose of combating crime.

The parlance of Article 17 leaves no doubt that 'State parties carry an obligation to adopt legislative and other measures to give effect to the prohibition against such interferences (with the right privacy) as well as for the protection of this right.'[221] Article 17 carries both a prohibitive duty, not to inference, and a positive duty, to protect.[222] The Human Rights Committee[223] explained that 'the right to privacy must be guaranteed against all arbitrary or unlawful interferences and attacks, whether they

[220] *Van Hulst v The Netherlands,* Communication 903/1999, UN Doc CCPR/C/82/D/903/1999 (2004), para 7.10

[221] See Conte (n 204 above). 202

[222] See General Comment 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputations (Art 17), UN Doc CCPR General Comment 16 (1988), paras 1 and 9

[223] *Ibid*.

emanate from State authorities or from natural or legal persons.'[224] In Zimbabwe, the right to privacy is guaranteed in the Constitution. However, there are limited legislative safeguards outside the constitutional framework to ensure the full enjoyment of the right to privacy.

4.3 United Nations Resolutions on the Right to Privacy

Questions on the ability of Article 17 of the ICCPR to adapt to technological developments have been raised. The convention was adopted in 1966 when telephones were less ubiquitous and the Internet did not exist but the provision has been applied to these technologies nevertheless.[225] For example, the United Nations Human Rights Committee's General Comment 16 of 1988 stipulates that 'surveillance, whether electronic or otherwise, interceptions of telephone, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.'[226]

A number of UN resolutions expound on the right to privacy in the digital environment. Both the UN General Assembly and the Human Rights Council acknowledge the need for human beings to be able to enjoy rights in the 'cyber' or 'virtual' world in the same way as they do in the physical world. In this regard, the General Assembly Resolution 69/166 of 2014[227] and the Human Rights Council U.N.

[224] Conte (n 204 above). 201

[225] A. Peters (note 105 above) p. 147-148

[226] Human Rights Committee, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. 1), 8, CCPR General Comment No. 16; Article 17 (The Right to Respect of Privacy, Family, Home and Correspondence, and the Protection of Honour and Reputation)

[227] G. A. Res. 69/166,3, The Right to Privacy in the Digital Age (Dec. 18. 2014)

Doc A/HRC/27/37 of 2015[228] on the right to privacy in the digital age clearly state that 'the same rights that people have offline must also be protected online, including the right to privacy.'[229]

The UN General Assembly is on record for expressing concern about 'the negative impact that surveillance and/or interception of communications have on the exercise and enjoyment of human rights.' [230] General Assembly Resolution 69/166 is of cardinal importance as it enjoins all states to:

> (a) respect and protect the right to privacy, including in the context of digital communication, and
> (b) take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring the relevant national legislation complies with their obligations under international human rights law.

Similarly, General Assembly Resolution, 68/167 of 2013 also reiterated the importance of the right to privacy and made a clarion call for states to adopt measures targeted at putting an end to violations of this right. This resolution is particularly important at the international plane as it obligates states to review their procedures, practices and legislation concerning extra-territorial surveillance of private communications. For instance, surveillance via the internet tend to violate the human right to privacy and the confidentiality of correspondence.[231]

---

[228] Human Rights Council U. N. Doc. A/HRC/28/L.27, 3, The Right to Privacy in the Digital Age (Mar. 24. 2015)

[229] The wording in both instruments is identical.

[230] Id. at preamble at 2; G. A. Res. 69/166, preamble at 2

[231] Peters (n 106 above). 146

4.4 African Conventions on the Right to Privacy

The African Charter on Human and Peoples' Rights[232] is the embodiment of the human rights within the African context. The preamble to the African Charter on Human and Peoples' Rights states that the objective of the instrument is to 'promote and protect human and peoples' rights and freedoms'[233] whilst taking into consideration the legal and political cultures of African states as well as preserving African tradition and identity.[234] The preamble also acknowledges that 'freedom, equality, justice and dignity are essential objectives for the achievement of the legitimate aspirations of the African peoples.'

Surprisingly, whether by shear inadvertence, omission or by design, the African Charter on Human and Peoples' Rights does not explicitly provide for the right to privacy. For this reason, the Charter has been incisively criticized for not being 'as progressive as it is made out to be'.[235] The lack of explicit recognition of the right to privacy is often cited as one of the major shortcomings of the Charter.[236] However, nuggets of the right to privacy may be gleaned from other provisions in the Charter. For instance, Article 4 of the Charter stipulates that 'every human being shall be

---

[232] The African Charter on Human and People's Rights was adopted in 1981 and came into force in 1986.

[233] *Ibid*. see preamble thereof

[234] The African Charter on Human and Peoples' Rights: How effective is this legal instrument in shaping a continental human rights culture in Africa? (2014) https://www.lepetitjuriste.fr/the-african-charter-on-human-and-peoples-rights-how-effective-is-this-legal-instrument-in-shaping-a-continental-human-rights-culture-in-africa/

[235] V. Nmehielle, *The African Human Rights System: Its Laws, Practice, and Institutions* Martinus Nijhoff Publishers, 2001. 325

[236] The African Charter on Human and Peoples' Rights: How effective is this legal instrument in shaping a continental human rights culture in Africa? (2014) (n 71 above)

entitled to respect for his life and the integrity of his person.' Similarly, Article 5 provides, *inter alia*, every individual's 'right to the respect of the dignity inherent in a human being.' Apart from these provisions no semblance of the right to privacy is found in the Charter.

Unlike the African Charter on Human and Peoples' Rights, the African Charter on Rights and Welfare of the Child explicitly provides for the right to privacy of the child. Article 2 defines a child as 'every human being below the age of 18 years.' Article 4(1) stipulates that 'in all actions concerning the child by any person or authority the best interests of the child shall be the primary consideration.' Article 10 specifically deals with the protection of privacy. It provides that

> 'No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.'

The first part of the provision is identical to Article 12 of the Universal Declaration of Human Rights save that it makes specific reference to the child. This implies a child enjoys the full scope of protection of the right to privacy as guaranteed in the UDHR in the same way as any adult person. The use of the words 'arbitrary or unlawful interference' suggests that the right may be limited under appropriate circumstances. Similarly, parents or legal guardians may interfere with the right in the 'exercise of reasonable supervision of the conduct of their children'.

The Charter also confers an obligation on State parties to create a legal framework for the protection of the child against interferences with or attacks on their privacy. Put

differently, the child is entitled to the right to the protection of the law with regards to their privacy interests. In the digital era, children are prone to various potential attacks on their privacy. Coincidentally, Article 28 protects children against sexual exploitation and prohibits the use of children in pornographic activities, performances and materials. Thus Article 28 is important as it implicates the right of privacy of the child.

Other regional human rights instruments also provide for the right to privacy in the digital sphere. For instance, the African Declaration on Internet Rights and Freedoms states that lawful surveillance of online communications must be governed by clear and transparent laws that provide for the following minimum basic principles:

- communications surveillance must be both targeted and based on reasonable suspicion of commission or involvement in the commission of serious crime;
- communications surveillance must be judicially authorised and individuals placed under surveillance must be notified that their communications have been monitored as soon as practicable after the conclusion of the surveillance operation;
- the application of surveillance laws must be subject to strong parliamentary oversight to prevent abuse and ensure the accountability of intelligence services and law enforcement agencies.

The above provisions of the African Declaration on Internet Rights and Freedoms are pertinent regard being had to Zimbabwean laws such as the Interception of Communications Act.[237] This latter Act is devoid of judicial or parliamentary oversight when it comes to issuance of interception of communication warrants save

[237] [Chapter 11:20]

in very limited circumstances. It is important to highlight that the Zimbabwean legal framework provides better protection of the right to privacy compared with the African Charter on Human and Peoples' Rights which is deafeningly silent on the right to privacy.

4.5 Conclusion

This chapter endeavoured to trace the right to privacy in various international and regional human rights instruments. A common thread running through the various international covenants is that the right to privacy, and the privacy of the home, family and correspondence are specifically guaranteed. These various human rights instruments prohibit arbitrary and unlawful interference with privacy and enjoin State parties to provide legal protection against infringement of the right to privacy. Although most of the international human right treaties were adopted at a point in history when information communication technologies, such as the Internet, were virtually non-exist, attempts have been made to extend the protection of privacy in the digital world. In general, the privacy laws of Zimbabwe compare favourably with benchmarks set in international human rights instruments although it has its own shortcomings highlighted in the preceding chapter. The ensuing chapter adopts a comparative approach by focusing on the right to privacy in other jurisdictions.

CHAPTER 5

Comparative Perspectives on Right to Privacy

5.0 Introduction

Previous chapters focused on domestic and international laws on the right to privacy. The remit of this chapter is to introduce a comparative perspective in order to establish how Zimbabwean laws on privacy compare with laws in other jurisdictions. A comprehensive comparative analysis of relevant laws of other jurisdictions is beyond the scope of this thesis. As such, only a synopsis of privacy laws of South Africa and the United Kingdom will be presented. The chapter will show that in each of these two jurisdictions, the right to privacy is recognized and protected in one form or another.

5.1 Right to Privacy under South African Law

Under South African law the right to privacy is protected by the Constitution as well as through legislative enactments and the common law. The right to privacy has also received considerable judicial attention with the courts playing a fundamental role in developing jurisprudence in this area of the law.

5.1.1 Constitutional protection of privacy in South Africa

The right to privacy has not always been an independent constitutional right in South Africa. Devenish[238] posits that 'as an autonomous concept and as an individual right, privacy is a relative newcomer to the body of justiciable and fundamental rights.' Be that as it may, the South African Constitution now provides for a person's right to privacy encompassing the right not to have their person or home searched; their

[238] G. E. Devenish, *A Commentary on the South African Constitution*, Butterworth's, 1998. 55

property searched; their possessions seized; or the privacy of their communications infringed.[239] The recognition of the right to privacy as a fundamental human right in the South African Constitution is an indication of its importance.[240] For the avoidance of doubt, section 14 provides that:

> 'Everyone has the right to privacy, which includes the right not to have –
> (a) their person or home searched;
> (b) their property searched;
> (c) their possessions seized; or
> (d) the privacy of their communications included.'

From a comparative perspective, section 57 of the Zimbabwean Constitution is substantially similar to section 14 of the South African Constitution. The main difference is that, unlike its counterpart provision, section 57 of the Constitution of Zimbabwe provides for every person's right not to have 'their home, premises or property entered without their permission.' In other words, the Zimbabwean Constitution also protects privacy by prohibiting unauthorized entry into one's home, premises or property. No corresponding protection is found in the South African Constitution although this is generally implied in section 14 regard being had to the right not to have one's home searched.

Further, section 57 of the Constitution of Zimbabwe provides for every person's right not have 'their health condition disclosed'. There is no analogous provision in section 14 of the South African Constitution. Apart from these differences, the right to privacy in section 57 of the Zimbabwean Constitution is almost identical to section 14 of the South African Constitution.

---

[239] See section 14 of the Constitution of South Africa

[240] See South African Law Reform Commission, 'Privacy and Data Protection', Discussion Paper 109, Project 124 October 2005, p. iv

As with the Zimbabwean Constitution, the South African Constitution does not explicitly provide for the protection of information privacy. A reasonable assumption is that information privacy finds protection under the general constitutional right to privacy. The preamble to the Protection of Personal Information Act[241] gives credence to this assumption by acknowledging the right to privacy enshrined in section 14 of the Constitution. The case of *Mistry v Interim Medical and Dental Council of South Africa*[242] further lends support to this proposition. In this case, the court noted that although breach of information privacy was not expressly mentioned in section 13 of the Interim Constitution (now section 14 of the current constitution) it would be covered by the broad protection of the right to privacy guaranteed by the section. In Zimbabwe, the constitution does not expressly provide for the protection of personal information save in the context of privacy of communications and personal information relating to health conditions. However, the courts are likely to follow the South African approach by according a wide interpretation to section 57 to accommodate privacy of personal information.

Under South African law, just like in Zimbabwe, the right to privacy is available to both natural and juristic persons. Section 8(2) of the South African Constitution stipulates that 'a provision of the Bill of Rights binds a natural or juristic person if, and to the extent that, it is applicable, taking into account the nature of the right and the nature of any duty imposed by the right.' Similarly, the Declaration of Rights in the Constitution of Zimbabwe does not only bind natural and juristic persons[243] but also provides for the enjoyment of the rights and freedoms by both natural and juristic

[241] Act 4 of 2013

[242] *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC)

[243] Section 45 (2) of the Constitution of Zimbabwe

persons to the extent that those rights and freedoms can appropriately be extended to them.[244]

Both the South African Constitution and its Zimbabwean counterpart do not provide for an absolute right to privacy. The right to privacy may be limited in terms of law of general application and has to be balanced with other rights entrenched in the Constitution.[245] In terms of enforcement of constitutional rights, both constitutions confer upon any person the right to approach a court claiming that a fundamental right or freedom has been, is being or is likely to be infringed. In this regard, section 85 and section 38 of the Zimbabwean and South African constitutions, respectively, are similarly worded. Both sections empower the courts to grant appropriate relief in the event of an infringement of a constitutional right, including a declaration of rights. However, section 85 of the Zimbabwean Constitution specifically allows courts to make an award for compensation for infringement of a constitutional right.

In Zimbabwe, section 57 of the Constitution has not received much judicial attention. Conversely, South African courts have on divers occasions dealt with cases implicating the constitutional right to privacy. For instance, taking blood tests of a non-consenting adult for purposes of paternity tests was held to constitute an invasion of personal privacy.[246] Similarly, legislation prohibiting the use or possession of

[244] Section 45 (3) of the Constitution of Zimbabwe

[245] See South African Law Reform Commission, (n 240 above). iv

[246] See *D v K* 1997 (2) BCLR 209 (N)

cannabis by an adult in private for personal consumption was held to be constitutionally invalid on the basis that it infringed the right to privacy.[247]

5.1.2 Legislative protection of privacy in South Africa

The privacy of communications is not only protected in section 14 of the South African Constitution but also by virtue of other legislative enactments. The Regulation of the Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002 (RICA) is one such enactment. The Act prohibits the interception of communication by expressly providing that

> '...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.'[248]

The Act makes it an offence for any person to engage in unlawful interception of communication.[249] The essence of the Act is the regulation of interception and monitoring of telecommunication surveillance of both direct and indirect communications by law-enforcement officers and agencies.[250] Thus the Act does not

---

[247] See *Minister of Justice and Constitutional Development and Others v Garreth Prince and Others* 2018 (6) SA 393 (CC) in which the Constitutional Court of South Africa declared statutory provisions in the Drugs and Drug Trafficking Act 140 of 1992 and the Medicines and Related Substances Control Act 101 of 1965 to be constitutionally invalid on the basis that the provisions infringed the right to privacy entrenched in section 14 of the Constitution. The implication of the judgment was that it decriminalized the use or possession of cannabis by an adult in private for personal consumption in private in the name of the right to privacy.

[248] See section 2 of the RICA.

[249] See section 49 of the RICA. The penalties for committing such an offence are drastic as the Act provides for a fine not exceeding R2 million or imprisonment not exceeding 10 years.

[250] N. Bawa, *The Regulation of the Interception of Communications and Provision of Communication Related Information Act*, in Thornton et al (eds) *Telecommunications Law in South Africa*, Lisa Thornton Inc, 2006. 308

prohibit interception of communications in *toto* but provide for lawful interception. The Act stipulates that any 'authorised person who executes an interception direction or assists with the execution thereof, may intercept any communication'.[251]

A key feature of the Act is that it provides for judicial supervision of interception operations. A person may apply to a designated judge[252] for interception directions in terms of section 16(1) of the Act. An interception direction may only be issued if the designated judge is satisfied, *inter alia*, that there are '*reasonable grounds to believe*' that a serious offence has been or will be committed. This provision has been criticized for being speculative and providing 'a low threshold for the granting of interception directions, and is patently open to abuse.'[253] Be that as it may, the South African interception of communications legislation is favourably disposed than its Zimbabwean counterpart[254] in that it, at least, provides for judicial oversight on interception warrants.

In order to give effect to the constitutional right to privacy, the South African legislature also enacted the Protection of Personal Information Act ('POPI Act'). Although the Act was promulgated in 2013 it is still not operational as it awaits

[251] Section 3(a) of the RICA.

[252] Section 1 of RICA defines 'designated judge' as any judge of a High Court discharged from active service or any retired judge designated by the Minister to perform the functions of a designated judge for purposes of the Act.

[253] See Stakeholder Report Universal Periodic Review, (n 185 above). 5

[254] The Interception of Communications Act of Zimbabwe does not have a provision for applying to a judge for an interception warrant. See Chapter 3 *supra*.

Presidential proclamation to come into effect.[255] The objects of the Act are, among other things, 'to promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Regulator...'.[256]

The preamble to the Act acknowledges the right to privacy enshrined in section 14 of the Constitution of South Africa. It further acknowledges that 'the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information.'[257] The import of the POPI Act is therefore to foster the right to privacy by providing 'data subjects' a certain level of control over their personal information.[258] The Act requires personal information to be processed in a responsible and lawful manner and provides remedies in the event of unlawful and irresponsible processing of personal data.[259]

The POPI Act encompasses various principles regulating the collection and processing of personal information.[260] The said data protection principles in the South African POPI Act are somewhat akin to the data protection principles enshrined in the

[255] The major reason for the delay is to enable the office of the Information Regulator to be established and become fully functional.

[256] See the preamble to the Act. The office of the Information Regulator is provided in section 39 of the Act.

[257] See the preamble to the Act

[258] The preamble to the Act provides the purpose as "to promote the protection of personal information processed by public and private bodies".

[259] An aggrieved data subject may institute a civil action for payment damages for patrimonial and non-patrimonial loss in terms of section 99 of the Act. Section 107 provides criminal penalties for breach of certain provisions of the Act.

[260] See sections 8 through 25 of the POPI Act

Access to Information and Protection of Personal Privacy Act.[261] Similarly, some of the principles under South African and Zimbabwean data protection laws are also found in the UK Data Protection Act 2018.[262]

5.1.3 Common law protection of privacy in South Africa

Under the common law of South Africa, every person is conferred with personality rights including the right to bodily integrity, reputation, dignity and privacy. This bundle of personality rights is embodied in the concept of '*dignitas*'. The term '*dignitas*' is given a wide meaning in South African law and it has long been interpreted to include the notion of privacy.[263] However, an independent right to privacy was recognized in the *locus classicus O'Keefe v Argus and Publishing Co Ltd*[264] in which the gravamen of the dispute was the publication of a photograph of the plaintiff without her consent. Similarly, in *Bernstein & Ors v Bester NO & Ors*[265] the court acknowledged that the common law recognizes the right to privacy as an independent personality right.

A person whose right to privacy has been infringed may bring an action under the *actio iniuriarum*, that is, an 'action for damages open to a plaintiff who can show that the defendant has committed an intentional wrongful act which constitutes an

[261] [Chapter 10:27]. See Chapter 3 *supra* for a detailed discussion of the above data protection principles under Zimbabwean law.

[262] Data protection legislation in the United Kingdom is discussed in detail below.

[263] F. du Bous *et al* (eds) *Wille's Principles of South African Law*, 9th Ed. Juta & Co (Pty) Ltd, 2007. 1198

[264] *O'Keefe v Argus and Publishing Co Ltd* 1954 (3) SA 244 (C)

[265] *Bernstein & Ors v Bester* NO & Ors 1996 (2) SA 751 (CC)

aggression upon his person, dignity or reputation.'[266] In order for the action to succeed, one has to prove an unlawful and intentional interference with a legally protected personality interest, in this instance, the right to privacy. More specifically, the common law action for invasion of privacy premised on the *actio iniuriarum* requires the plaintiff to prove three essential elements, *viz*; (i) impairment of their privacy; (ii) wrongfulness; and (iii) intention (animus iniuriandi).[267] However, 'although early cases equated the invasion of privacy with an infringement of dignity in the sense of insult and required that there should be an element of *contumelia*, later cases made it clear that the invasion of privacy did not require *contumelia*.'[268]

Zimbabwean courts have adopted the above common law position of South Africa on the existence of a right to privacy. For instance, in *Mr. & Mrs. "X" v Rhodesia Printing & Publishing Co Ltd*[269] the court cited with approval the case of *O'Keeffe v Argus Printing and Publishing Co. Ltd*.[270] Davies J stated that it was 'clear that there is a qualified right to privacy.' Similarly, in *Chituku v Minister of Home Affairs & Ors*[271] the court held that 'the right to dignity is recognized in the Roman-Dutch law as an independent right that can be protected by the *actio injuriarum*.' Similarly, in *Reid-Daly v Hickman*[272] the court noted that the 'planting of a listening device in an apartment does of itself amount to an impairment of the occupier's *dignitas*.' In this

[266] See *O'Keefe v Argus and Publishing Co Ltd* 1954 (3) SA 244 (C)

[267] See *NM & Ors v Smith & Ors* [2007] ZACC 6; 2007 (5) SA 250 (CC). In *Jansen van Vuuren and Anor NNO v Kruger* 1993 (4) SA 842 (AD) the court opined that as a general rule, a plaintiff who relies on the *actio iniuriarum* must allege *animus iniuriandi*.

[268] du Bous (n 263 above). 1199

[269] *Mr. & Mrs. "X" v Rhodesia Printing & Publishing Co Ltd* 1974 (4) SA 508 (R), confirmed in *Rhodesia Printing & Publishing Co Ltd v Duggan* 1975 (1) SA 590 (RA) at 592.

[270] *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 (3) SA 244 (C)

[271] *Chituku v Minister of Home Affairs & Ors* 2004 (1) ZLR 36 (H)

[272] *Reid-Daly v Hickman* 1980 ZLR 201, 1981 (2) SA 315 (ZA) at 323

case plaintiff alleged invasion of his *dignitas* and privacy *animo injuriandi* on the grounds that certain military officers had tapped his telephone and kept him under surveillance.

Although Zimbabwean and South African common law on the right to privacy is, by and large, similar, South African courts have been actively developing the common law by infusing it with the 'spirit' of the Constitution. South African courts have had to grapple with the extent to which the Bill of Rights has application in common law disputes. In *Bernstein & Ors v Bester NO & Ors*,[273] it was noted that courts must be circumspect when attempting to protect common law principles when interpreting fundamental rights and their limitations. A distinction was drawn between the two-pronged constitutional inquiry into whether a right has been infringed and whether the infringement is justified, and the single inquiry under common law regarding whether an unlawful infringement of a right has taken place. It remains to be seen whether Zimbabwean courts will adopt a similar approach when interpreting constitutional and common law rights.

5.2 Right to Privacy under English Law

The UK legal system is unique in that it does not have a written constitution in the sense understood in other jurisdictions, as the parliament cannot bind its successors. Each parliament must be free to make or unmake the law of the land.[274] As aptly highlighted by Carroll,[275] 'prior to 1998, the British 'constitution' contained no

[273] *Bernstein & Ors v Bester NO & Ors* 1996 (2) SA 751 (CC)

[274] See *R (on the application of Miller and Another) v Secretary of State for Exiting the European Union* (2017) in which the court confirmed that UK does not have a constitution in the sense of a single coherent code of fundamental law which prevails over all other sources of law.

[275] A. Carroll, *Constitutional and Administrative Law*, 7th Ed. Pearson Education Ltd, 2013

positive statement of basic human rights similar to those found in the constitutional provisions of many other liberal democracies.'[276] As such, the focus will be on common law protection of privacy as well as an analysis of the Human Rights Act of 1998.

5.2.1 Common Law Privacy under English Law

In the UK, the right to privacy has not existed explicitly but partially protected under the law of confidence. In *Wainright & Anor v Home Office*[277] the court confirmed that the UK courts have so far been reluctant to formulate a general principle of 'invasion of privacy'. A number of reasons have been advanced for this general disinclination on the part of English courts. For instance, Foster[278] posits that:

> 'As the notion of privacy and private life is often nebulous, domestic law might be reluctant to pass or develop a specific law of privacy, preferring to rely on established legal principles, such as the laws of trespass and confidentiality, which recognise and protect more tangible rights and interests. Secondly, the law will need to determine the extent of the right to privacy and, more specifically, when it is legitimate to violate that right.'[279]

The same author (Foster) argues that the 'uncertain character of privacy and private life, contributed to a general reluctance to accommodate this right in domestic law and still poses acute dilemmas for the legal system.'[280] English courts have more often than not made reference to an individual's fundamental right to privacy, but refusing to recognize an individual's legal right to privacy.[281] The decision in *Malone*

[276] *Ibid*., p. 483

[277] *Wainright & Anor v Home Office* [2001] EWCA Civ 2081 at para 19

[278] Foster (n 2 above)

[279] *Ibid*. p. 559

[280] Foster (n 2 above). 559

[281] See, for instance, *R v Ministry of Defence, ex parte Smith*, [1996] 1 All ER 257

v Metropolitan Police Commissioner[282] epitomized the non-existence of a general right to privacy under English domestic law. In this case, the court held that the plaintiff had no remedy when the police had tapped his telephone for the purpose of detecting possible criminal activities. The plaintiff could not rely on Article 8 of the European Convention on Human Rights (ECHR) as it had not been incorporated into English law, and the domestic laws of trespass and confidentiality did not provide him with a remedy. Similarly, in *Kaye v Robertson*[283] it was held that English law did not recognize the right of privacy and thus an individual could not rely on that concept to obtain legal redress. Ironically, the court acknowledged that there had been a 'monstrous' invasion of the plaintiff's privacy, but held that that alone did not entitle him relief in English law.

English courts have therefore tended to shy away from developing jurisprudence encompassing a clear right to privacy. Thus in *R v Central Independent Television*[284] the court highlighted that although there was room for the creation of a right of privacy under English law, 'it would be more appropriate for the remedy to be provided by the legislature rather than the judiciary.'[285]

From a comparative perspective, English law is different from the South African and Zimbabwean common law positions on the right to privacy. Unlike in Zimbabwe and South Africa, where the common law right to privacy was initially recognized as part of the concept of *dignitas*, and recently as a standalone right, the English common law

[282] *Malone v Metropolitan Police Commissioner (No 2)* [1979] Ch 344

[283] *Kaye v Robertson* [1991] FSR 62

[284] *R v Central Independent Television PLC* [1994] 3 All ER 641 at 652

[285] See also Foster (n 2 above). 579

only protects privacy under the laws of trespass and confidentiality. Accordingly, the protection of privacy is generally restricted under English common law unlike in the other two jurisdictions.

5.2.2 Legislative Protection of Privacy under English Law

A number of legislative enactments provide protection of privacy under the English legal system. Some of the notable enactments include the Human Rights Act, the Data Protection Act and the Regulation of Investigative Powers Act.

(a) Human Rights Act of 1998

The enactment of the Human Rights Act 1998 was a major milestone in the legislative history of the United Kingdom. For once, UK citizens were 'provided with a charter of positive human rights which the state is obliged to respect and observe.'[286] Hitherto, a number of human rights such as the right to life, religion and privacy, did not enjoy direct legal protection in the UK.[287] The Act enables rights and freedoms enshrined in the European Convention on Human Rights to become directly enforceable in the UK courts to the extent compatible with primary legislation and the ultimate sovereignty of Parliament.[288] The Act imposes a duty on all 'public bodies' to act in accordance with the Convention rights. By implication, there is no corresponding duty on 'private bodies' or individuals to act in accordance with the rights enshrined in the Convention.

[286] Carroll (n 275 above). 486

[287] *Ibid*.

[288] *Ibid*.

Prior to the domestication of the European Convention on Human Rights in the UK legal system through the promulgation of the Human Rights Act, a stand alone right to privacy was alien to the English legal system. However, the enactment of the Human Rights Act somewhat kindled hope on the possibility of developing a fully-fledged right to privacy in English law based on Article 8 of the European Convention on Human Rights. The right to respect for private and family life is now part of the English law by virtue of Article 8 of the Convention. In *Douglas v Hello! Magazine*,[289] the Court of Appeal accepted that the common law had reached the point where the right to privacy could now be recognized.

The hope for a standalone right to privacy evanesced in *Wainwright v Secretary of State for the Home Department.*[290] In this case, the House of Lords refused to recognize a specific right to privacy. The essence of the decision in *Wainwright* was that the incorporation of Article 8 of the ECHR into domestic law did not in itself translate into a specific action in privacy. The Court of Appeal held that the Human Rights Act could not be relied on to introduce a retrospective right to privacy that did not exist at common law. Thus the court maintained its obduracy that no separate cause of action existed in English law for invasion of privacy. Instead, the courts sought to develop the law of confidentiality in a manner that resembled the right to private life under Article 8 of the Convention. The court further held that the absence of a specific law of privacy in domestic law was not in contravention with the UK's obligations under the European Convention as the Convention did not require an

[289] *Douglas v Hello! Magazine*, [2001] 2 WLR 992. See also *Venables and Thompson v MGN* [2001] 2 WLR 1038 in which the law of confidentiality was expanded to protect the claimants from disclosure of information relating to their identity and whereabouts.

[290] *Wainwright v Secretary of State for the Home Department* [2004] 2 AC 406

individual to make a separate claim for breach of privacy but merely required that domestic law provide an adequate remedy in the event of violation of Article 8.

The English law position appears to be that, although the Human Rights Act provides a statutory remedy with respect to violations committed by public authorities, a tort of privacy has not yet been fully developed per se. The courts refused to create a new law of privacy but expanded the existing law of confidentiality and data protection in light of Article 8 of the European Convention.[291] Accordingly, the courts had to tinker with the tort of confidence to accommodate various aspects of privacy, particularly protection of information privacy. The result has been nothing more than the proverbial square peg in a round hole. In *Campbell v MGM Ltd*[292] Lord Nicholls stated:

> 'Now the law imposes a duty of confidence whenever a person receives information he ought to know is fairly and reasonably to be regarded as confidential. Even this formulation is awkward. The continuing use of the phrase 'duty of confidence' and the description of the information as 'confidential' is not altogether comfortable. Information about an individual's private life would not, in ordinary usage, be called 'confidential'. The more accurate natural description today is that such information is private.'

Although the courts appear reluctant to develop a specific law of privacy and rely on the expansion of existing law,[293] the general trend appears to be that English courts are slowly gravitating towards acceptance of an express right to privacy despite

[291] Foster (n 2 above). 582. See for instance *R v Wakefield MBC ex parte Robertson* [2002] 2 WLR 889 in which law of confidentiality was used to prohibit the electoral authorities from passing on the claimant's personal details for various marketing purposes.

[292] *Campbell v MGM Ltd* [2004] UKHL 22; [2004] 2 AC 457; [2004] 2 WLR 1232

[293] Foster (n 2 above). 584

earlier attempts to hold tenaciously to the tort of confidence. This position was confirmed in *Browne v Associated Newspapers*[294] in which the Court of Appeal said:

> 'The first question under Art 8 is whether the claimant has a reasonable expectation of privacy in the particular circumstances of the case. That is the relevant question in determining whether there was previous confidential relationship between the parties or not...The cause of action...has now thrown off the need for an initial confidential relationship.'

Under English law, the focus is no longer on the existence of a confidential relationship when it comes to the privacy of information but on the nature of the information itself.[295] The duty will arise 'whenever the party subject to the duty is in a situation where he knows, or ought to know that the other person can reasonably expect his privacy to be protected.'[296] English courts should be able to adapt the existing laws of privacy with little difficult as courts are public authorities within the Act, with a duty to develop and interpret the law, both public and private, to ensure that rights are not violated, and to provide a remedy if none existed prior to the Human Rights Act.

From a comparative perspective, the inescapable inference is that, unlike Zimbabwe and South Africa, the UK does not have a constitutional right to privacy. This stems from the absence of a 'written' constitution in the UK. Unlike in South Africa and Zimbabwe, English law is generally cast in terms of breaches of duty rather than positive declarations of rights in a constitution.[297] The Human Rights Act 1998 is the embodiment of human rights in the UK. Even though the Human Rights Act

---

[294] *Browne v Associated Newspapers* [2007] EWCA Civ 295

[295] *Venables and Thomson v News Group Newspapers Ltd* [2001] Fam 430

[296] Carroll (n 275 above). 519

[297] See *Attorney-General v Guardian Newspapers Ltd* (No. 2) [1988] 3 All ER

domesticates the European Convention on Human Rights, English courts have grappled with the need to develop an explicit right to privacy. Be that as it may, the English legal system is slowly coming to terms with the need to recognize the right to privacy.

(b) Data Protection Act

The English legal system has been strong on protection of information privacy through data protection legislation despite the general reluctance to develop an express right to privacy. The UK Data Protection Act 1998, which was repealed and replaced by the Data Protection Act 2018, was an offshoot of the European Directive 95/46/EC whose thrust was to create universal European standards for the collection, storage and processing of personal information.[298] The Data Protection Act 2018 provides, inter alia, for the regulation of the processing of information relating to individuals and functions of the Information Commissioner.

From a comparative perspective, it is important to highlight that some (if not all) of the data protection principles in the UK Data Protection Act are also found in the Zimbabwean Access to Information and Protection of Privacy Act[299] discussed in detail in Chapter 3 of this thesis. From the foregoing discourse, one major take away is that the English legal system, though weak in terms of recognizing and providing for a standalone right to privacy, is strong with respect to the data protection aspect of privacy.

[298] See Stahl (n 50 above). 55-68

[299] [Chapter 10:27]

(c) Regulation of Investigative Powers Act

The Regulation of Investigative Powers Act 2000[300] is also relevant insofar as it protects the privacy of communications in the UK. The Act makes 'provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed.'[301]

The Act makes it an offence for a person to 'intentionally and without lawful authority' intercept, anywhere in the United Kingdom,[302] any communication in the course of its transmission by a public postal service or public or private telecommunication system. However, section 5 of the Act permits interception of communication with a warrant issued by the Secretary of State in the interests of national security,[303] for purposes of preventing or detecting serious crime[304] or for purposes of safeguarding the economic well being of the United Kingdom.[305] The Regulation of Investigatory Powers Act therefore protects the privacy of communications by prohibiting unauthorized interceptions. In the same vein, Zimbabwe and South Africa have similar legislation intended to safeguard the privacy of communications. Unlike the South African Regulation of Interception of

[300] This Act repealed the UK Interception of Communications Act 1985

[301] See the preamble to the Regulation of Investigative Powers Act 2000

[302] In *R v P* [2001] 2 All ER 58 the House of Lords ruled that telephone intercepts effected in another state could be admitted as evidence in a criminal trial in the United Kingdom. The House of Lords categorically stated that section 9 of the Interception of Communications Act 1985, which precluded the use of such evidence, applied only to intercept evidence obtained in the country. See section 17 of the Regulation of Investigatory Powers Act).

[303] Section 5(3)(a) of the Act

[304] Section 5(3)(b) of the Act

[305] Section 5(3)(c) of the Act

Communications Act, the UK legislation is bereft of judicial oversight on interception warrants as the Secretary of State issues warrants of interception. In Zimbabwe, the Minister issues warrants authorizing lawful interception of communications.

5.3 Conclusion

This chapter was an attempt to providing a glimpse into the privacy laws of other jurisdictions. Privacy laws of South Africa and the United Kingdom have been pithily explored. A common theme in these jurisdictions, apart from the UK, is that the right to privacy is directly or indirectly guaranteed and protected in national constitutions. The UK legal system is peculiar in the sense of having no written constitution. The Human Rights Act however incorporates into domestic laws, human rights and fundamental freedoms enshrined in the European Convention on Human Rights. Despite this dissimilarity with other jurisdictions, and the reluctance to develop a specific right to privacy, various facets of privacy are protected under English law. It is also clear that all of the said jurisdictions have taken great strides in protecting the privacy of information through data protection legislation as well as privacy of communications through interception legislation. This bears testimony to the importance of the right to privacy in the sense that other jurisdictions or legal systems seek to protect privacy as a fundamental right. The next chapter marks the tail end of this thesis as it deals with the findings, conclusions and recommendations emanating from the research.

CHAPTER 6

Findings, Conclusions, and Recommendations

6.0 Introduction

The preceding chapters capped the law on privacy as it obtains in Zimbabwe, in terms of international human rights instruments and in other jurisdictions. After all is said and done, it remains to present the findings, conclusions and recommendations flowing from the research. Recommendations will be tabled regarding ways in which the legal framework may be enhanced to guarantee full protection of the right to privacy in Zimbabwe. The Chapter will conclude by highlighting areas for further research in order to facilitate development of jurisprudence in the field of privacy law.

6.1 Findings

This research set out to evaluate the current legal framework regulating the right to privacy in Zimbabwe in general as part of its objectives. The evaluation carried out reveals that the right to privacy is recognized and protected through constitutional provisions, under the common law and through legislative enactments. The Constitution of Zimbabwe guarantees the right to privacy in section 57 thereof. The Constitution not only provides a general right to privacy but also proceeds to enumerate various facets of privacy specifically protected. These include the right of every person not have their home, premises or property entered without their permission; their person, home, premises or property searched; their possessions seized; the privacy of their communications infringed; or their health condition disclosed.

The research has also shown that a number of legislative enactments provides for the protection of the right to privacy in Zimbabwe. Although there is no specific Act dealing with the full spectrum of the right to privacy, the Access to Information and Protection of Privacy Act partially protects the privacy of personal information. The Interception of Communications Act also regulates the right to privacy of communications by prohibiting unlawful interception of communications. The research also reveals that criminal sanctions are imposed in terms of the Criminal Law (Codification and Reform) Act where there is serious impairment of dignity or invasion of privacy. However, the law on privacy is Zimbabwe remains largely fragmented and spasmodic.

The research has also established that the right to privacy is recognized and protected under the common law concept of *dignitas* although a specific right to privacy now exist. The common law also affords protection of the right to privacy under the *actio injuriarum* and provides remedies in the event of breach of privacy rights. For instance, an interdict may be the appropriate remedy in circumstances where there is threatened wrongful publication of private facts. Similarly, damages are also a primary common law remedy in an action for breach of privacy. A person who, without reasonable justification, invades the privacy of another may be liable to a claim for delictual damages.

Despite the existence of various laws protecting the right to privacy, the research makes the finding that there is a lacuna in the law relating to specific facets of the right to privacy affected by developments in the field of information and communication technologies. The research has shown that the right to privacy is a

multivalent concept comprising various aspects. Some of the facets of privacy continue to evolve with technological developments, especially information privacy. A notable gap in the Zimbabwean legal framework is the absence of comprehensive data protection legislation. Although the Constitution of Zimbabwe enshrines a general right to privacy, it does not provide for the right to protection of the privacy of personal information save for information relating to a person's health conditions and, to some extent, personal information forming part of a communication.

Although some data protection principles exist in the statute books, the principles are incorporated in the Access to Information and Protection of Privacy Act that is largely defunct and on the verge of being repealed in the event of the Freedom of Information Bill coming into law. In any event, the data protection principles in the Access to Information and Protection of Privacy Act have largely remained obscure and dormant in Zimbabwe as confirmed by the absence of case law in this area. The absence of an information regulator in Zimbabwe is also a major shortcoming in this digital era where inordinate amounts of personal data and information are collected and processed instantaneously through information and communication technologies. Similarly, the absence of comprehensive cyber crime legislation implies that personal information may also be hacked and abused without adequate recourse to aggrieved citizens.

Developments in information and communication technologies have necessitated the ease with which communications may be intercepted and surveillance may be carried out on citizens. Although the Constitution of Zimbabwe outlaws infringement of the privacy of communications and the Interception of Communications Act prohibits

arbitrary interception of communications, there are conceivable gaps particular in the latter legislation. A glaring weakness of the Interception of Communications Act is the absence of judicial oversight on warrants for interception of communication as these are exclusively issued by the Minister. The Act confers sweeping powers upon the Minister to issue, extend and perpetually renew warrants of interception. Such untrammeled powers may be subject to abuse thereby placing the privacy of communications in jeopardy.

In the same vein, yawning gaps are also evident in subsidiary legislation such as the Postal and Telecommunications (Subscriber Registration) Regulations of 2014 (Statutory Instrument 95 of 2014) that prohibit telecommunications and internet service providers from activating SIM cards or providing services unless customer details have been registered. The regulations also authorize the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) to establish and maintain a central subscriber information database for storage of subscriber information. In the absence of proper legal safeguards, such personal information may be abused thereby placing privacy rights at stake. The legal requirement for registration of SIM cards limits the ability of citizens to communicate anonymously and facilitates tracking and surveillance of citizens.

Privacy laws of Zimbabwe have been juxtaposed with international human rights instruments and legal positions in other jurisdictions on the right to privacy. It has been established that most international human rights instruments incorporate a general right to privacy prohibiting arbitrary or unlawful interference with privacy, privacy of the home and privacy of correspondence. International human rights

instruments also enjoin state parties to provide legal protection against infringement of the right to privacy. The research has shown that, in general, the privacy laws of Zimbabwe compare favourably with benchmarks set in international human rights instruments although there are inherent shortcomings.

A comparison of the right to privacy in Zimbabwean with laws of other jurisdictions results in a general finding that other jurisdictions make provision for a direct or indirect right to privacy in their national constitutions. Like Zimbabwe, countries such as South Africa have constitutional provisions pertaining to the right to privacy. Only the UK has no constitutional right to privacy due to the nature of its legal system that does not provide for a written constitution. The existence of a right to privacy in legal systems of other nations bears credence to the importance of privacy as a fundamental right.

A general finding that may be drawn from the research is that other legal systems including South Africa and the United Kingdom provide for common law as well as legislative protection of privacy. From a legislative standpoint, privacy legislation is generally common in areas such as regulation of interception of communications, data protection as well as laws relating to search and seizure. An evaluation of legal frameworks in other jurisdictions reveals that Zimbabwe is not lagging far behind in terms legislation protecting the right to privacy save for areas such as data protection and interception of communications which are in need of legislative overhaul.

6.2 Conclusions

From a theoretical and philosophical standpoint, one can inevitably conclude that the notion of privacy cannot be grasped with utter certainty given its complexity and

multi-faceted attributes. There is no uniformity in definition, nature and scope of the concept of privacy. This uncertainty about privacy explains the reluctance by legal systems such as the United Kingdom to develop a standalone right to privacy. The philosophical underpinnings around privacy have influenced how different jurisdictions have recognized, treated and protected the different facets of the right to privacy.

This research has shown the extent to which the right to privacy is protected in Zimbabwe. The right to privacy finds protection in the Constitution of Zimbabwe, under legislative enactments and in terms of the common law. To this end, the inescapable conclusion is that the currently legal framework in Zimbabwe safeguards the right to privacy to a greater extent although there are a number of gaps in dire need of revision in this area of the law.

6.3 Recommendations

Pursuant to the various findings made above, the following recommendations are made:

- Zimbabwean courts, in particular the Constitutional Court, need to accord section 57 of the Constitution a wide and purposive interpretation in order to give effect to the full spectrum of the constitutional right to privacy. This will ensure that emerging facets of privacy emanating from technological developments will come within the ambit of the protections guaranteed by the general right to privacy. The courts have the power to develop jurisprudence in the area of privacy rights in sync with international human rights instruments.

- The minister responsible for the administration of Interception of Communications Act must consider proposing amendments to this Act in order to provide for judicial oversight regarding the issuance of interception of communications warrants. Applications for interception warrants must be in writing and on oath or affirmation to a judge who will determine whether the circumstances justify interception of communications. This will ensure that, where interception of communications is necessary on justifiable grounds, a warrant for interception is issued by a judge as opposed to a Minister who is for all intents and purposes a political appointee.
- There is urgent need for the Minister of Information Communication Technology and Courier Services to expedite the promulgation of specific data protection legislation to safeguard the privacy of personal data and information in the digital era. The proposed data protection legislation may incorporate some or all of the data protection principles enshrined in Part V of the defunct Access to Information and Protection of Privacy Act [Chapter 10:27] as well provide for the office of the information regulator. The proposed data protection legislation must also be in sync with international laws and standards given that the collection and processing of personal data transcends national boundaries.
- The Minister of Information Communication Technology and Courier Services must ensure that relevant legislation provides for strong mechanism for the protection of personal data and information collected and processed by service providers through compulsory subscriber registration. The law must also provide stiffer penalties against telecommunications service providers who unlawfully disclose personal information.

- It is imperative for the Minister of Information Communication Technology and Courier Services to accelerate the process of promulgating computer and cyber crime legislation in order to deter criminals and other unauthorized persons from accessing computer-related information. This will go a long way in protecting the privacy of data and information in computer systems.

6.4 Areas for Further Research

A number of areas with respect to privacy require further research. For instance, the area of data protection is still in its nascent stages of development and requires nurturing through legislative enactments and jurisprudential discourse. This calls for further research in order to ensure that any data protection legislation developed is adequate to promote the right to privacy. In the same vein, further research may also be commissioned around trans border privacy issues necessitated by technological developments. Interception of communications and electronic surveillance, internet privacy are some of the areas ripe for comprehensive research.

6.5 Conclusion

This chapter provided concluding remarks and presented general findings flowing from the research. The chapter has also made a number of recommendations with respect to how the legal framework may be enhanced to ensure the protection of the full spectrum of privacy rights and interests in Zimbabwe. Given the expansive nature of issues relating to the concept of privacy coupled with emerging privacy interests necessitated by technological developments, areas for further research have also been highlighted.

REFERENCE LIST

Article 19, 'The "Right to be Forgotten": Remembering Freedom of Expression', 2015, Free Word Centre, available at http://www.article 19.org

Atkon, A. 'Privacy and Data Protection in the Light of Smart TV Technology' Master Thesis, Tilburg Institute for Law, Technology & Society available at http://arno.uvt.nl/show.cgi?fid=140063

Bainbridge, D. I. (2008) Introduction to Information Technology Law, 6th Ed. Pearson Education Limited, England

Bawa, N. The Regulation of the Interception of Communications and Provision of Communication Related Information Act, in in Thornton, L; Carrim, Y; Mtshaulana, P & Reburn, P (eds) Telecommunications Law in South Africa, 2006 Lisa Thornton Inc, Johannesburg, South Africa

Birks, P. "The Academic and the Practitioner", (1998) 18 *Legal Studies*, 377

Blumberg, A. J. and Eckersley, P (2009) On Location Privacy and How to Avoid Losing it Forever, Electronic Frontier Foundation, http://www.eff.org

Bradley, A. W. & Ewing, K. D. (2011) Constitutional & Administrative Law, 15th Ed. Pearson Education Limited, England

Brandeis, L. and Warren, S. 'The Right to Privacy' *Harvard Law Review*, Vol. 4 No. 5 (Dec 1890)

Bygrave, L. A. "Data Protection to the Right to Privacy in Human Rights Treaties" Journal of Law and Information Technology, Vol. 6 247-284

Carr, I. (2014) International Trade Law, 5th Ed. Routledge Taylor Francis Group, London & New York

Carroll, A. (2013) 'Constitutional and Administrative Law', 7th Ed. Pearson Education Ltd

Centre for Internet & Society (2014), "Search and Seizure and the Right to Privacy in the Digital Age: A Comparison of US and India downloaded from <https://cis-india.org/internet-governance/blog/search-and-seizure-and-right-to-privacy-in-digital-age >

Conte, A. & Burchill, R. (eds) (2009) Defining Civil and Political Rights, The Jurisprudence of the United Nations Human Rights Committee, 2nd Ed. Ashgate Publishing Ltd

Davis, S in Smith, R. K. M. and van den Anker, C. (eds) (2005) The Essentials of Human Rights, Hodder Arnold, London

Devenish, G. E. (1998) A Commentary on the South African Constitution, Butterworths

Diggelmann, O. and Cleis, M. N. "How the Right to Privacy Became a Human Right" Human Rights Law Review, Vol. 14, Issue 3, (2014), pp 441-458 https://doi.org/10.1093/hrlr/ngu014

Du Bous, F. (ed) *et al* (2007) Wille's Principles of South African Law, 9th Ed. Juta & Co (Pty) Ltd

Du Plessis, L. M. & De Ville, J. R. 'Personal Rights: Life, Freedom and Security of the Person, Privacy, and Freedom of Movement' in Van Wyk *et al* D (Ed) (2004) Rights and Constitutionalism: The New South African Legal Order, Clarendon Press, Oxford Juta & Company Ltd

Feltoe, G. (2006) A Guide to the Law of Delict in Zimbabwe, 3rd Ed. Legal Resources Foundation

Finn, R. L.; Wright, D. and Friedewald, M. "Seven Types of Privacy" (2013) in de Hert, P. J. A., Gutwirth, S., Leenes, S., & Poullet, Y (Eds.) *European Data Protection: Coming of Age*, Springer, Dordrecht

Foster, S. (2008) Human Rights & Civil Liberties, 2nd Ed. Pearson Education Limited, England

Goldsmith, M. 'The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance', 74 J. Crim. L. & Criminology 1 (1983)

Gonzalez, B. 'Drones and Privacy in the Golden State, 22 Santa Clara High Tech. L.J. 288 (2017) http://digitalcommons.law.scu.edu/chtlj/vol33/iss2/3

Gormely, K., "One Hundred Years of Privacy", Wisconsin Law Review, Vol. 1992, ed. 5, 1992, 1335

Hale, A and Edwards, J, 'Getting it Taped' (2006) 12 Computer and Communications Law Review 71

Kufandirimbwa, O. Zanamwe, N., Hapanyengwi, G. and Kabanda, G. (2013) *Mobile Money in Zimbabwe: Integrating Mobile Infrastructure and Processes to Organisation Infrastructure and Processes* Online Journal of Social Sciences Research, Vol. 2, Issue 4, pp 92-110 Available Online at http://www.onlineresearchjournals.org/JSS

Mevedzenge, J. A. 'Accessing the National Voters' Rolls through the Right of Access to Information in Zimbabwe', *Zimbabwe Rule of Law Journal* Vol. 1 Issue 1, February 2017 International Commission of Jurists and Center for Applied Legal Research

Miller, A. R., (1971) The Assault on Privacy: Computers, Data Banks and Dossiers, University of Michigan Press, Michigan

Mironenko, O. 'Body Scanners versus Privacy and Data Protection' *Computer Law and Security Review* 27 (2011) 232-244 available at www.sciencedirect.com

MISA, "Digital Rights Lessons from Zimbabwe Internet Shutdown" https://misa.org/news/digital-rights-lessons-from-zimbabwes-internet-shutdown/

MISA Zimbabwe, 'Digest: Facial Recognition Technology and its possible impacts on Privacy Rights', http://zimbabwe.misa.org/2018/05/29/digest-facial-recognition-technology-privacy-rights/

MISA Zimbabwe, Foreword to The Access to Information Model Law

MISA Zimbabwe Statement on the Postal and Telecommunications (Subscriber Registration) Regulations, 1 April 2016. Available on http://zimbabwe.misa.org/2016/04/01/misa-zimbabwe-statement-on-the-postal-and-telecommunications-subscriber-registration-regulations/

Ncube, C. B. 'Data Protection in Zimbabwe', in Makulilo, A. B. Ed. (2016) 'African Data Privacy Laws', Springer International Publishing

Ncube, C. 'A Comparative Analysis of Zimbabwean and South African Data Protection Systems', 2004 (2) *The Journal of Information, Law and Technology*

Personal Data Protection Guidelines for Africa: A joint initiative of the Internet Society and the Commission of the African Union

"Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission", Privacy Protection Study Commission, July 12, 1977, http://aspe.hhs.gov/datacncl/1977privacy/toc.htm quoted in George Reynolds "Ethics in Information Technology", Cengage Learning

Peters, A. "Privacy, Rechtsstaatlichkeit, and the Legal Limits on Extra-territorial Surveillance" in Miller, R. A. (Ed) Privacy and Power: A Translantic Dialogue in the Shadow of the NSA-Affair

Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) Abridged Postal and Telecommunications Sector Performance Report: Second Quarter 2019 Report

Privacy Protection Study Commission, "Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission", 1977, http://aspe.hhs.gov/datacncl/1977privacy/toc.htm

Rehm, G. M. 'Privacy in the Digital Age: Vanishing into Cyberspace? In Friedmann, D and Barak-Erez, D. (Eds) (2001) Human Rights in Private Law, Hart Publishing, Oxford-Portland, Oregon

Rehman, J. (2003) International Human Rights Law – A Practical Approach, Pearson Education Ltd, England

Rengel, A. "Privacy as an International Human Right and the Right to Obscurity in Cyberspace" Groningen Journal of International Law, Vol 2(2): Privacy in

International Law, <https://grojil.files.wordpress.com/2015/04/grojil_vol2-issue2_rengel.pdf

Reynolds, G. (2015) "Ethics in Information Technology", 5th Ed.Cengage Learning

Rubenfeld, J. "The Right of Privacy" (1989) Yale Law School, Faculty Scholarship Series, Paper 1569 at 751 http://digitalcommons.law.yale.edu/fss_papers/1569

Solove, D. J. Privacy and Power: Computer Databases and Metaphors for Information Privacy, (2001) 53, Stanford Law Review, 1393 at 1394

South African Law Reform Commission, 'Privacy and Data Protection', Discussion Paper 109, Project 124 October 2005

Stahl, B. C. (2008) 'What Privacy? The Impact of the UK Human Rights Act 1998 on Privacy Protection in the Workplace' in Subramanian, R. (ed) Computer Security, Privacy and Politics, Current Issues, Challenges and Solutions, IRM Press

Stakeholder Report Universal Periodic Review, 'The Right to Privacy in South Africa', 27th Session, October 2016

Stakeholder Report Universal Periodic, 26th Session, "The right to privacy in Zimbabwe" (March, 2016) submitted by the Zimbabwe Human Rights NGO Forum, the Digital Society of Zimbabwe, the International Human Rights Clinic at Harvard Law School, and Privacy International

Stefanick, L. (2011) "Controlling Knowledge: Freedom of Information and Privacy Protection in a Networked World", AU Press, Athabasca University

Suri, R.K.; Diwan, P. and Kapoor, S. (2000) Information Technology Laws (Laws relating to cyber & e-commerce) Pentagon Press, New Delhi

The African Charter on Human and Peoples' Rights: How effective is this legal instrument in shaping a continental human rights culture in Africa? (2014) downloaded from https://www.lepetitjuriste.fr/the-african-charter-on-human-

and-peoples-rights-how-effective-is-this-legal-instrument-in-shaping-a-continental-human-rights-culture-in-africa/

The Herald, 27 June 2018 'People Speak on Voters' Roll – Pictures Violate Privacy'

Vibhute, K and Aynalem, F. (2009) Legal Research Methods Teaching Material, chilot.worldpress.com

Warren, S. D. and Brandeis, L.D. "The Right to Privacy" *Harvard Law Review,* Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220 at 195. Available at http://www.jstor.org/stable/1321160 [Accessed: 14 November 2019]

Westin, A. F., (1970) Privacy and Freedom, Atheneum, New York

Wicker, S. B. (2013) 'Cellular Convergence and the Death of Privacy' Oxford University Press

Winick, R. *Searches and Seizures of Computers and Computer Data*, 8 Harv. J. L. Tech 75,104 (1994)

Young, J. B. "Introduction" In Young, J. B. ed., Privacy 2, 1978