Examining the relationship between national security and the individual citizen's right to privacy in South Africa between 1994 and 2021

By

Angel Cartwright

A mini-dissertation submitted in partial fulfilment of the requirements for the degree

Master of Arts in Security Studies (MSS)

Department of Political Sciences,

Faculty of Humanities, University of Pretoria

Supervisor: Prof V. Graham

September 2022

DECLARATION OF ORIGINALITY

Full names of student: Angel Cartwright

Student number: u17226997

Declaration

1. I understand what plagiarism is and am aware of the University's policy in this regard.
2. I declare that this report (e.g., essay, report, project, assignment, dissertation, thesis, etc.) is my own original work. Where other people's work has been used (either from a printed source, Internet or any other source), this has been properly acknowledged and referenced in accordance with departmental requirements.
3. I have not used work previously produced by another student or any other person to hand in as my own.
4. I have not allowed and will not allow anyone to copy my work with the intention of passing it off as his or her own work.

SIGNATURE OF STUDENT: 

DATE: 31 August 2022

ACKNOWLEDGEMENTS

Firstly, and most highly, I thank the Omnipresent and Almighty God.

Secondly, I am grateful to my supervisor Prof. V. Graham at the Department of Political Sciences, for the expert direction and motivation in completing this thesis. Without Prof. Graham's input, this thesis would not have been possible.

Thirdly, my deepest gratitude goes to my editor Anne Marais.

Lastly, my earnest appreciation goes to my family and friends, my father, Quinton, my cherished grandmother Pamela, my siblings, Faith and Gabrielle and my dearest best friend, Kimberly Munatsi. I am incredibly thankful for their unwavering support and reassurance.

ABSTRACT

The aim of this qualitative study is to attempt to characterise the complex relationship that exists between the individual's right to privacy and the state's national security in democratic South Africa. Arguably, the root of the complex relationship between these two concepts is caused by the inherent tensions that exist between the government's responsibility to ensure national security and the citizens' right to their own privacy. Ultimately, technological advancements, particularly those that have enabled increased mass surveillance by governments, have caused the relationship between the state and citizens to change. This is because of, *inter alia*, government access to mass information as well as the monitoring of the private activities of citizens, leading to threats to civil liberties, notably, the right to privacy. South Africa is used as a case study to contextualise the causes and implications of the complex relationship between privacy and national security using the social contract theory. The study finds that technology has led to mass surveillance being used to ensure national security. However, this has led to tension between the individual's right to privacy and national security. The study concludes by characterising the relationship between national security and the individual's right to privacy and provides recommendations that will hopefully add to the growing literature on matters of privacy and national security.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS/ ACRONYMS

ASWJ	Ahla Sunna Wal Jummaa
BIIS	Bophuthatswana Intelligence and Internal Service
CCTV	Closed-circuit television
CID	Crimes Intelligence Division
DIS	Department of State Security
ECHR	European Convention on Human Rights
ECT Act	Electronic Communications and Transactions Act 25 of 2002
ECtHR	European Court of Human Rights
E3A	Everything, Everywhere, All the time
FICA	Financial Intelligence Centre Act 38 of 2001
ICT	Information Communications Technology
ICPR	International Covenant on Civil and Political Rights
IMPA	Interception and Monitoring Prohibition Act 127 of 1992
IMSI	International Mobile Subscriber Identity-Catcher
ITAD	Information Technology Asset Disposition
JCSI	Joint Standing Committee on Intelligence
MPs	Members of Parliament
NCC	National Communications Centre
NIA	National Intelligence Agency
NICOC	National Intelligence Co-ordinating Committee
NIS	National Intelligence Services
NSA	National Security Agency
OIC	Office for Interception Centres
PASS	Pan African Security Service
POPIA	Protection of Personal Information Act 4 of 2013
POSIB	Protection of State Information Bill
PAIA	Promotion of Access to Information Act 2 of 2002
RICA	Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002

SANDF	South African National Defence Force
SACN	South Africa Cities Network
SANAI	South Africa National Academy of Intelligence
SAPS	South African Police Service
SARS	South African Revenue Services
SASSA	South African Social Security Agency
SASS	South African Secret Service
SSA	State Security Agency
TIS	Transkei Intelligence Service
UDF	United Defence Force
UK	United Kingdom
UN	United Nations
UNDP	United Nations Development Program
UNHRC	United Nations Human Rights Committee
VINS	Venda National Intelligence Service

CHAPTER 1: BACKGROUND AND RESEARCH OVERVIEW

1.1 INTRODUCTION TO THE RESEARCH PROBLEM

During the past two decades, the evolution of technology has played an instrumental role in providing governments with the necessary mechanisms to undertake surveillance (Underwood & Saiedian 2021:20). These technological developments ensure that much of an individual's "life" now occurs electronically (Shamsi & Abdo 2001) with their communication and other transactions (among other things) now almost entirely online (Stansberry et al. 2019). Therefore, technology plays a significant role in creating tension between individuals' right to privacy and national security. When considering the tension between these concepts in South Africa, it is notable that during apartheid, national security (this concept is defined below) fixated on military strength and policing (Cawthra 2013:6). By contrast, democratic South Africa's security concerns incorporate much more than military and policing matters. It also includes politics, the economy, and social and environmental matters. Essentially post-1994 South Africa has embraced a humanist framework to security (Cawthra 2013:6). Thus, it presents a unique opportunity to study the national security versus privacy debate.

On 11 September 2001 (9/11[1]), nineteen militants associated with "al Qaeda", an Islamic extremist group, hijacked four aeroplanes in order to carry out suicide attacks against the United States. The group flew into the World Trade Center's north and south towers in New York City. The two other targets included the Pentagon and Pennsylvania, which resulted in over 3000 people dying due to the 9/11 terrorist attacks. The aftermath of 9/11 emphasised that states found themselves in a new environment (Jones 2009:18); this new environment has brought forth risks where the "new" enemies of the state have the capacity to "exploit the open nature of modern society" to commit acts of terror. Moreover, the rise in technology represents a significant threat to cybersecurity as cyberspace has opened avenues for those who wish to achieve criminal objectives; these include cyber blackmail, identity theft, and fraud (Iranddoost 2018). However, these threats do not end

[1] '9/11' refers to the four coordinated terrorist attacks carried out by the Islamist extremist group known as al Qaeda on the United States of America on 11 September 2001.

there; they can cause massive harm to the security of states (Clarke & Knake 2010). This reality has put the focus on protecting national security (George 2014: 220). National security can be understood as alleviating the threats to cherished values, especially those "threats that remain unchecked and threaten specific referent objects" survival in the immediate future (Williams 2013:6). The "national security quintet" considers five elements of national security, namely national interest, national identity, national will, national values, and national power (Bester 2019:11). A threat to these elements is a threat to national security. Mass surveillance uses technologies or systems that analyse, collect, and generate the data of large numbers of unidentified people instead of limiting the surveillance to individuals under suspicion of wrongdoing (Privacy International 2021). Currently, the available global forms of mass surveillance allow governments to capture virtually all aspects of people's lives (Shamsi & Abdo 2001). Various states have adopted mass surveillance to safeguard their national security; nevertheless, the scale of surveillance has led many to question whether current-day threats are sufficient to validate the abuse of the citizen's privacy in the interest of protecting national security. These threats include terrorism[2] (United Nations Office on Drugs and Crime, 2020), service delivery protests[3] (Campbell 2014), cyber-attacks[4] (Pratt 2022), insurrections[5] (Allan 2022) and more. Lopach and Luckowski (2006: 246) noted that "the world finds itself confronted by an enemy that is not defined by borders or boundaries". Furthermore, as the world is experiencing its Fourth Industrial Revolution, technology will evolve continuously, allowing mass surveillance to only grow larger (Underwood & Saiedian 2021:21). Hlase (2018:7) states that mass surveillance has caused a paradoxical phenomenon. This is because policymakers have to balance the obligation to preserve the nation's safety (Larson 2020) with the need to ensure that the obligation does not enforce an undue burden on citizens (Finkelstein et al. 2017:293).

---

2 Defining terrorism is complex and controversial. A basic definition is the calculated use of violence to cause fear within a population to achieve a political objective.

3 The concept of 'service delivery' is commonly used in South Africa. It refers to the delivery of basic resources such as land, housing, water, electricity, and sanitation infrastructure. Protests happen to improve service delivery.

4 Cyber-attacks are unwelcome attempts to steal, expose, alter, disable or destroy information through unauthorised access to computer systems.

5 A usually violent attempt to take control of a government.

The most noteworthy threats to national security in South Africa are domestic threats: "Our greater threats are domestic linked largely to persistently high levels of inequality. There are few compelling reasons to limit fundamental rights such as privacy unduly, especially on national security grounds" (Swingler 2018). The country does not face significant terrorism threats compared to the "Five Eyes" countries, also referred to as the FVEY[6](Swingler 2018). However, the use of mass surveillance by South Africa has resulted in an increased violation of the individual's privacy in the name of upholding national security. Accordingly, "it's been open season on our data, and massive data breaches have threatened public security [and] safety" (Swingler 2018). Peter Carter concludes, "it must be quite clear that there is a fundamental difference between the interests of national security – in other words, something catastrophic, like the destruction of an entire computer network – compared to an embarrassment to a sitting administration … That is not national security. That is politics" (Swingler 2018). Therefore, hiding behind the national security argument is no longer valid as the individual's privacy continues to be eroded. Thus, this research will evaluate the relationship between national security and the individual's right to privacy in South Africa.

1.2 RESEARCH PROBLEM AND QUESTION

The research problem that this study will attempt to address concerns the relationship between national security and privacy using South Africa as the case study. The problem is that too much security imposed by the state creates insecurity of the individual due to said security measures violating the individual's right to privacy. However, too much privacy causes potential insecurity in the state particularly when individual actions result in actual threats to the state, which is a problem because the state is obligated to ensure national security. Inevitably, questions arise such as: When, if ever, do national security priorities trump the rights of the individual and, if so, in what circumstances is it acceptable? Why is the trade-off between national security and privacy so problematic? Lastly, what necessary safeguards and accountability mechanisms can be adopted to balance national security and privacy in South Africa?

[6] The FVEY refers to the intelligence alliance between the United States, the United Kingdom, Australia, New Zealand, and Canada

The main research question that the study asks is: How can the relationship between national security and the individual's privacy in South Africa between 1994 and 2021 be characterised? Thus, the aims of this study will be to:

- Determine how mass surveillance has evolved into a tool or an instrument of national security in South Africa and the consequence of this on the individual's right to privacy.
- Examine the role that technology plays in creating tension between national security and individual privacy in South Africa.

1.3 LITERATURE REVIEW

The goal of this thematic literature review is to organise and discuss existing literature based on the concepts of national security, mass surveillance and privacy to provide some context for understanding the research.

1.3.1 Defining National Security as an Evolving Concept

According to Ullman (1983:129), Goldman (2001:43) and Fjäder (2014:117) traditional national security had a narrow focus. It focused on preserving the sovereign and territorial integrity of the "state as well as its primary political and cultural values, specifically protecting it against external military threats". This placed less emphasis on internal threats. Therefore, national security is pivotal to the state's ability to address the above-mentioned threats. Nonetheless, the definition of national security has not always been exact. Wolfers (1952:481) contended that the concept of national security should be "met with scepticism" as it "may not mean the same thing to different people; while appearing to offer guidance and a basis for a broad consensus they may be permitting everyone to label whatever policy he favours with an attractive but possibly deceptive name". Neo-realists such as Hans Morgenthau and Kenneth Waltz understood security as the state's main interest. This is because the international environment is anarchic and poses a significant threat to the state. As a result, Morgenthau (1952: 973) stated: "the survival of a political unit, such as a nation, in its identity is the irreducible minimum, the necessary element of its interest vis-a-vis other units". Likewise, Waltz (1979:126) argued: "In

anarchy, security is the highest end. Only if survival is assured can states seek such other goals as tranquillity, profit, and power". Therefore, the focus of security was the state.

Moreover, theorists such as Joseph Nye and Donald Nuechterlein considered national interest a key component when conceptualising national security. Nye (1999:23) defined national interest as "the set of shared priorities regarding relations with the rest of the world". These incorporated values related to human rights such as democracy, freedom, justice or issues which the public regarded vital to society and their identity as a whole. Nuechterlein (1976:246) defined national interest as the "perceived needs and desires of one sovereign state in relation to other operation states compromising the external environment". Thus, Nye and Neuchterlein have similar interpretations of national interest by defining it as the way states navigate how they interact with the world. Although Nye's approach focused on values and Nuechterlein's on perception, both indicate that national interests guide states' interactions with other states to ensure their security and development. Ultimately, both theorists were significantly influenced by the Cold War; however, the conclusion of the Cold War presented new arguments regarding national security as the world faced a fundamental shift in international security. This led to a revised conception of security among academics, which concentrated on "broadening" security issues beyond the military focus of the state. It also included issues such as "mass migration, environmental degradation, economic issues, famine and organised crime" and the "deepening" of security by considering other actors beyond the state (Krause & Williams 1996: 230). Therefore, the broadened interpretation of national security was more inclusive and considered threats to environmental, socio-economic and political aspects, which involved "more than the mere concentration of state power" (Buzan 1991:29). Ultimately, the new approaches to security involved human security and environmental security. Thus, as security became evolved, so did national security; it was no longer focused primarily on the military defending the state and external threats. Instead, it evolved into considering global issues which impact the state and the individual. As a result, security focuses on the individual, which is referred to as human security. The concept of human security is linked to the 1994 United Nations Development Program Report (UNDP) (Arinze 1995:85). It is also associated with economist Mahbuh ul Haq, who stated that security is not only about states or nations but also about people

and individuals. He argued that the world entered a “new era of human security” in which the concept would change from state-focused to the security of individuals (Bajpai 2000:10-13). The UNDP was published in the same year as Haq's monograph. The UNDP defines human security as ‘freedom from fear’ and ‘freedom from want’, which consist of several components; these are “economic security, food security, health security, environmental security, personal security, community security and political security” (Williams 2013:225).

1.3.2 Mass Surveillance

The cost of surveillance has been significantly reduced through technological advancements (Duncan 2018:5), and states can easily use electronic signals, which place entire populations under surveillance (Gürses, Kundnani, & Van Hoboken 2016:580). The rapid evolution of technology has led to a rise in mass surveillance as states can access bulk communication-related content and information (Arun 2014:111). The introduction of new Information and Communications Technologies (ICTs) since the 2000s has aided states and private companies in collecting and analysing massive databases (Zalnieriute 2015:111) through telephone calls or email (Conway et al. 2017:313). This is referred to as metadata, which specifies individual interests, reading or travelling habits, and associates and closest friends (Schuster et al. 2017:77). It can also identify the sender, receiver, time (Conway et al. 2017:313), date, duration, and communication channel (Schuster et al. 2017:77). This data can be used to determine religion, sexual preferences, political leanings and more (Bernal 2016:253). Thus, mass surveillance touches almost every aspect of people’s daily life (Goold & Neyland 2009:xy). Ultimately, different arguments exist regarding mass surveillance because the concept is understood differently by different groups of people, such as civil society, businesses and states. The word “surveiller” in French etymology is defined as being watched over or overseeing; this implies that a hierarchy exists as the word is related to “observer, caretaker and supervisor concepts” (Amiradakis 2016:282). Understanding surveillance in this manner allows it to be interpreted as a “coercion technique or a form of control” exercised over a person through supervision (Lena & Cable 2017:766). Panopticism is a social framework established by Michel Foucault, who claimed that those being observed through

surveillance adopt a submissive role in an existing power structure (Foucault 1977:205). Foucault pronounces that when individuals are conscious of being under observation, their behaviour deviates to benefit the observer (Waters 2018:1296); thus, the panoptic schema represents the change of instruments in communal control (Caluya 2010:622). Duncan (2018:45) states that mass surveillance has led to the state "becoming like a one-way mirror"; this underscores that the "state can view more and more what citizens do and say, but citizens see less and less what states do with the data they have gained".

1.3.3 National Security Arguments in favour of Mass Surveillance

Gathering and analysing information places national security agencies in a problematic position. Cohen (2000) proclaims that the relationship between "surveillance and national security interests is complex" because, as Mavedzenge (2020:362) claims, governments must respect citizens' privacy on the one hand and protect national security on the other hand (Perez 2020). Ultimately, Moore (2018:251) states that when agencies fail in gathering the information necessary to accomplish their objective, they are blamed for not using the latest technologies and techniques. Thus, in a security failure, national security is scrutinised to a more considerable degree than privacy issues, as security failures render the individual and state as a whole to be worse off. Similarly, Perez (2020) argues that national security should be placed above the individual's concern for privacy as the common good outweighs personal preferences, and surveillance is a method which is required to advance the common good. Because mass surveillance guarantees improved security and intelligence measures, which help to prevent the loss of life, it should be prioritised over privacy (Schuster et al. 2017:80). Citizens who have come to accept surveillance argue that privacy is impossible to achieve because of the increasingly digitised era; Jonathan Cable and Linna Dencik describe this phenomenon as "surveillance realism" (Duncan 2018:32). Former President Barack Obama (2013) claimed that one could not have 100 per cent security and seek 100 per cent privacy and expect no inconvenience. He said this when replying to the National Security Agency's (NSA's) spying activities revealed by Edward Snowden. At the same time, Solove (2011:2), Cayford and Pieters (2018:94), and Milanovic (2015:143) argue that national security should have the necessary oversight and regulation. The purpose is to validate

that the interference is an essential measure and is proportionate to the risk being mitigated (Kleinig et al. 2011:181).

1.3.4 Privacy Concerns opposing Mass Surveillance

Mass surveillance by states to ensure their national security has resulted in privacy being traded off for security (Lieshout et al. 2013:124). Ünver (2018:8) states that the modern world has never before experienced such abuse of the individual's right to privacy. Arun (2014) refers to this as the feeling of the Big Brother being omnipresent, which some fear the state will use against citizens which some states such as China already do (Qian et al. 2022). Bigo (2013:34) argues that the national security argument for using mass surveillance does not mean that "anything goes". Also, it does not justify the decrease in regulation, accountability, oversight, and the violation of citizens' civil liberties. According to Duncan (2018:31), the protection of privacy by advanced governments has declined. Privacy is considered an essential human right that supports 'human dignity and upholds values such as freedom of speech and association' (Bernal 2016:245). Article 12 of the United Nations Declarations of Human Rights states:

> 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 (United Nations 2015:12).

However, privacy becomes moot as mass surveillance becomes a tool to provide national security. Stahl (2016:35) argues that nothing stops the authorities from using personal data for greater social monitoring and control. This distorts the difference Aristotle made between the "private sphere of the home and the public sphere", which encompasses political activity (Moore 2018:134). Nonetheless, governments claim that people have nothing to fear if they have nothing to hide (Scheiner 2015:92). However, Watt (2017) claims that this argument is problematic because it adopts the narrative that the government's motive behind using surveillance is pure. This is dangerous as citizens will not know when they will need their right to privacy. Notably, once an individual's privacy is violated, it cannot be reversed because once something is known, it cannot be

unknown. Therefore, Davis (2003:178) and Bambauer (2013:683) argue there needs to be a "balance between the security needs of society and government" to prevent stripping away individual privacy (Etzioni 2014:36). Benjamin Franklin once said: "Any society that would give up a little liberty to gain a little security will deserve neither and lose both" (Levi & Wall 2004:206). Ultimately, the arguments presented by those in favour and against mass surveillance do not show how to effectively create a balance between national security and privacy; hence, little attention is given to solving or mitigating issues regarding mass surveillance.

1.3.5 Mass Surveillance and National Security versus Privacy in South Africa

Democratic South Africa implemented various legislation which addressed national security and the individual's right to privacy; these are: The Constitution (1996); the Intelligence Service Act 38 of 1994; the Regulation of Interception of Communications and Provisions of Related Information Act 70 of 2002 (RICA); and the Protection of Personal Information Act 4 of 2013 (POPIA). These surveillance and national security declarations will be analysed as South Africa presents a unique opportunity to understand the relationship between national security and privacy. This is primarily because of the transformation of its security compared to that of its colonial and apartheid predecessors. Thus, the relationship between privacy and security can be determined by using and analysing South Africa as a case study.

1.4 THEORETICAL FRAMEWORK

The theory used in this study is the social contract theory. In political philosophy, it is known as a theoretical compact or agreement between the ruled and their rulers (Aondohemba & Shaapera 2015:38). Each has its own rights and duties. This theory is attributed to Thomas Hobbes and John Locke, both English philosophers, and Jean-Jacques Rousseau, a French philosopher (Neidleman 2012:1). Social contract theories differ on the purpose of the social contract; some preserve the sovereign's power, others safeguard the individual from being oppressed by the sovereign (Aondohemba & Shaapera 2015:37). Hobbes contends that when individuals agree to enter into a social contract, they give their "liberty to the sovereign on the conditions that they [the sovereign]

will safeguard their lives' (Laskar 2013:2). Alternatively, Locke believes that the social contract is based on protecting individuals' natural rights, including property rights (Laskar 2013:4); thus, sovereign powers that violate this can rightly be overthrown (Aondohemba & Shaapera 2015:37). Rousseau reasons that when the government takes away the power of the people, the social contract is violated and the citizens are "no longer compelled to obey them and have a duty to rebel" (Laskar 2013:5). Therefore, applying it to the national security and privacy debate would mean that the government must ensure national security. However, the execution of this duty to ensure national security can create tension when the individual privacy is violated, leading to strained relations between the government and citizens. This tension threatens the social contract between the government and citizens.

1.5 RESEARCH METHODOLOGY

This desktop study uses an explanatory and qualitative approach. It is a literature-based study which uses a combination of primary and secondary sources; these include government white papers, journals, books, research publications and the Internet. The qualitative approach is fitting for this study as it seeks to critically evaluate the inter-relationship between mass surveillance, privacy and national security concepts. The traditional review method of research will be used to structure the study. A case study based on South Africa will be used to discuss how mass surveillance is used to protect national security and violates individual privacy. Also there will be a discussion on what attempts have been made to ease tension between the two concepts. A case study allows for a holistic, thorough (Kumar 2011:379) and in-depth exploration of why mass surveillance emphasises the conflict between the two concepts (Bryman 2012:76). The limitations of the study are that the focus will be on mass domestic surveillance, thereby excluding the impact of foreign surveillance from the argument.

This study has no human participants. Therefore, this mini-dissertation has no special or unusual ethical considerations beyond the declaration that the dissertation will be the researcher's own work and that all information sources used will be acknowledged within the text and the reference list. The researcher is aware that plagiarism is an offence

against the Republic of South Africa's laws and the regulations of the University of Pretoria.

1.6 STRUCTURE OF RESEARCH

Chapter 1 of the research has focused on the background and methodology of the research. Chapter 2 will examine the theoretical framework used. Chapter 3 is an analysis of the relationship between mass surveillance and national security, particularly the global arguments favouring benefits and arguments against using mass surveillance due to privacy concerns. Chapter 4 will be a South African case study evaluating several policies that have been implemented between 1994 and 2021 to address the tension that mass surveillance causes between national security and individual privacy. Lastly, Chapter 5 will consist of recommendations and concluding remarks.

CHAPTER 2: EXPLORING THE SOCIAL CONTRACT THEORY

2.1 INTRODUCTION

This study investigates the complex relationship that mass surveillance causes between national security and privacy. This chapter provides the theoretical framework for understanding the state's relationship with its citizens. It is rooted in the understanding of the social contract which exists between citizens and states. The chapter explores various interpretations of the social contract, particularly the role that the state plays and what citizens are prepared to sacrifice in order to live under the state's rule. Furthermore, it evaluates possible threats to the relationship between the state and citizens. These theoretical understandings will examine how the violation of the individual's privacy to uphold national security threatens the relationship between the state and citizens.

2.2 SOCIAL CONTRACT THEORY

A lot has been written regarding the state of technological modernisation and how these developments can deliver solutions to the emerging threats facing humanity in the twenty-first century. The rise in new technologies raises questions about our relationship with technology and the impact this relationship will have on society. It is thus essential to consider how certain technologies will either threaten or preserve human dignity, as the integrity of our social fabric is at stake (Al-Rodhan 2018). The social contract is the understanding that a "contract exists between persons in a pre-social or pre-political condition upon which they agree to form a society or submit to political authority". It explores the limitations of political obligations by evaluating what a rational actor is prepared to lose and gain. Political philosophy refers to it as an agreement or theoretical compact which exists among rulers and the ruled, with each having their own duties and rights (Aondohemba & Shaapera 2015:38). A commonality within the social contract theory is the acceptance that the "political order and the state exist to ensure the people's general interest", where life, liberty, and property are protected. Therefore, in the age of rapidly evolving technologies such as mass surveillance, it is vital to assess "the role of liberties, the functions of the sovereign, and the limits of control" (Al-Rodhan 2018). The social contract theory is ascribed to the English philosophers Thomas Hobbes, John

Locke and the French philosopher Jean-Jacques Rousseau (Neidleman 2012:1). In the twentieth century, “moral and political theory” regained “philosophical momentum” as a result of John Rawls’s Kantian perception of the social contract theory. Several social contract theories exist; however, they differ with regard to the purpose of the social contract, with some prioritising the preservation of the sovereign’s power; alternatively, others maintain that the individual should be safeguarded to avoid them being oppressed by the sovereign (Aondohemba & Shaapera 2015:37). In light of the above, this chapter will focus on different interpretations of theories related to the social contract theory. The purpose of this is to explore the core ideas put forward by these theorists to form a framework. The framework will be used to investigate the extent to which mass surveillance creates tension between national security and the individual’s privacy.

2.3 MODERN INTERPRETATIONS OF THE SOCIAL CONTRACT

2.3.1 Thomas Hobbes’s understanding of the social contract

Hobbes’s theory of the social contract appeared in *Leviathan* for the first time. It was published in Britain during the Civil War in 1651. Hobbes used the social contract method to conclude that society should submit to the authority of absolute sovereign power (Mouritz 2010:125). He argued that subjects should only go against the sovereign power when their lives are in danger (Mouritz 2010:125). Hobbes's justification, according to Royce (2010:48), is that since men are self-interested and rational, they succumb to the authority of a sovereign to live in a civil society that supports their own interests. Hobbes describes this by “imagining men in their natural state”, which he calls the “state of nature”. The state of nature permitted man’s life to be one of selfishness and fear. Because mankind lived in chaotic conditions they were plagued with constant fear. Hobbes (1651) describes the state of nature as “solitary, poor, nasty and short” and that the state of nature is “purely hypothetical” (Mouritz 2010:126).

Moreover, the state of nature has several conditions; these include that within the state of nature, “men are exclusively and naturally self-interested, they are not equal to each other, resources are limited, and there is a lack of power to ensure [that] men cooperate” (Mouritz 2010:125). Accordingly, Hobbes finds that the state of nature is “the worst

position one can find themselves" in; therefore, in order to escape this, civil society should be created (Mouritz 2010:125). This is where the social contract is formed by firstly agreeing to establish society by collectively renouncing men's rights against one another in the "state of nature". Also, they must come to an agreement to live "collectively under common laws by creating an enforcing mechanism for the social contract and the laws that constitute it" (Laskar 2010:4). Hobbes agrees that although living under the authority of a sovereign can be harsh, one is better off compared to living in the state of nature (Ritchie 1891:670). Hence, Hobbes argues that it does not matter how much one objects to the sovereign rules; resisting the sovereign is never justified because it is the only thing in the middle of us and the state of nature (Ritchie 1891:670). Hobbes urges subjects to surrender all their rights in order to render liberties to the sovereign to preserve life, prosperity, and the peace of all subjects (Laskar 2013:2). Therefore, "natural law" became a "directive or moral guide" for the sovereign in order to protect and preserve the natural rights of subjects (Laskar 2013:2). Consequently, Hobbes believes that people should willingly surrender their freedom to authority in exchange for security and protection. At the core of Hobbes's social contract theory is the premise that individuals choose to "relinquish some of their rights" in exchange for their "protection from the dismal life in a state of nature" (Al-Rodhan 2018).

2.3.2 John Locke's understanding of the social contract

Alternatively, to Hobbes's understanding of the social contract, Locke deems the purpose of the social contract to be the protection of the individual's natural rights, such as property rights. Thus, the sovereign power can be overthrown if this is violated (Mouritz 2010:124). Locke views the state of nature differently than Hobbes. Locke argues that the state of nature is the "natural condition of mankind". It is a "state of perfect and complete liberty to live as one sees fit, free from interference from others" (Royce 2010:51). However, this does not mean one can do what one pleases as the state of nature is not without morality. Locke believes that people are equal to another in a state and bounded by the law of nature (Locke 1689:269). Property is central to Locke's argument for civil government and the contract that establishes it. He states that private property is created when an individual combines their "labour with the raw materials of nature". Nevertheless, due to

the challenges within the law of nature, there are limitations to “how much property an individual can own”, as man should not take “more than his own fair share” (Laskar 2013:4). Mouritz (2010:126) finds that property is central to Locke’s argument for the social contract and civil government as men within the state of nature feel the need to protect their property (Mouritz 2010:126). The social contract meant that man did not have to “surrender their rights to one individual”, but they could only surrender their rights in order to “maintain or preserve order and enforce the law of nature” (Laskar 2013:4). Thus, individuals could reserve their right to life, liberty and estate as these rights were considered the “natural and absolute rights of men” (Laskar 2013:4).

Locke claims that the law of nature is the foundation of all “morality ordained by God”, who orders that we “do not harm others regarding their life, health, liberty, or possessions” (Locke 1689). Therefore, Locke argued that the purpose of the government was to protect and uphold the natural rights of men. If government fulfils this purpose, only then can the laws it brings forth be seen as valid and obligatory; but, if it fails to do so, then “laws will not be valid, and the government can be thrown out of power” (Ritchie 1891:663). Because Locke believed that unlimited sovereignty opposed natural law, he advocated for the principle of the state of liberty and not of license. Locke promoted a state which focuses on the “general good of the people and thus promotes a constitutionally limited government”. He believed that to not return to the state of nature, the civil government must be rejected to construct an even better civil government (Laskar 2013:4). Ultimately, Hobbes’s and Locke’s understanding of the social contract in terms of the nature of morality and human nature is completely different. Locke’s social contract primarily focused on the rights of citizens to rebel against the sovereign; these sentiments played an influential role in democratic revolutions. In essence, according to Locke, the social contract meant government could only govern through the people’s consent; without it, the government could be overthrown. Locke maintains that the main role of government is to protect rights such as “life, liberty and property” (Locke 1689).

2.3.3 Jean-Jacques Rousseau’s understanding of the social contract

In his works *The Social Contract* and *Emile,* Rousseau deliberated the social contract theory. According to Rousseau, “the social contract is not a historical fact but a

hypothetical construction of reason" (Laskar 2013:5). He claims that before the social contract, life within the state of nature was "happy, men were equal, and humans were free". Rousseau states that the creation of property represents humanity's "fall from grace" out of the state of nature (Laskar 2013:6). As a result of this, men surrendered their rights "not to an individual but to the community as a whole which he refers to as [the] general will" (Aondohemba & Shaapera 2015:38). Henceforth, through the social contract, a new form of social organisation was formed where the state was established to "guarantee and assure rights such as liberties, freedom, and equality". At the core of Rousseau's theory of general will is the premise that the "law and the state were a direct result of the general will of the people" (Aondohemba & Shaapera 2015:38). The purpose of the general will is to reflect the will of the majority of citizens to whom blind obedience should be given. The majority's view was accepted based on the belief that the "majority's view is more correct than the minority's". Thus, each individual is not subjected to another individual but to the "general will and to obey this is to obey himself" (Royce 2010:53). Therefore, if government and laws do not conform to the general will, they will be discarded. Rousseau favoured "people's sovereignty" (Ritchie 1891:672) and based his theory of social contract on the principle of "man was born free, and he is everywhere in chains" (Rousseau 1893). Ultimately, whereas Hobbes's theory of social contract supported absolute sovereignty, Locke and Rousseau maintained that individuals preferred the state or government (Ritchie 1891:667).

2.4 CONTEMPORARY INTERPRETATIONS OF THE SOCIAL CONTRACT

2.4.1 John Rawls's Understanding of the Social Contract

In 1971, John Rawls published *A Theory of Justice,* which relied on Immanuel Kant's understanding of individuals and their capabilities. Rawls uses a social contract model, which he referred to as "justice as fairness" (Rawls 1971:4). In Rawls's interpretation of the social contract, associates start from the "original position", in which they imagine the reasoning behind a "veil of ignorance". This means that they unaware of their "relative social status in the society they are hypothetically constituting" (Neidleman 2012:3). He uses the concept of the veil of ignorance as a tool to theorise the "principles of justice within a context of equality". Neidleman (2012:2) claims that Rawls's original position is

an “abstracted form of the state of nature”. Boucher and Kelly (1994:8) state that from this position, the nature of justice can be described as what is needed by individual persons and social institutions to live together cooperatively. Thus, behind the veil of ignorance within the original position, one does not know one’s circumstances, namely gender, talents, disabilities, age, the conception of what the state or society in which one lives is, and what constitutes a good life (Boucher & Kelly 1994:9). Furthermore, it is assumed that individuals are disinterested in another individual’s wellbeing and are rational. As a result of these conditions, Rawls contends that the principles of a just society can be chosen and are selected from initial inherently fair conditions. Hampton (1980:326) claims that this is possible as no one has knowledge that could be used to develop principles that favour their own circumstances. According to Rawls, the principles that persons find themselves in are “the original position, behind the veil of ignorance”; they would choose to regulate society, which is referred to as the two principles of justice. The first principle is focused on broadly distributing civil liberties in line with equality which precedes the second principle, concerned with the distribution of economic and social goods. Hence, Upadhyav (1993:388) finds that one should not decide to relinquish some civil liberties in return for greater economic advantage; instead, one must focus on satisfying the first principle’s demands before moving to the second principle.

2.5 CONCLUSION

This chapter has laid the groundwork for understanding the social contract between citizens and the state. It has been done by considering the literature on the social contract theory Although several interpretations exist of this social contract, this study will use Rousseau's understanding of the social contract. The social contract depends on the relationship between the state and citizens. This includes how much power is granted to the state and what the citizens are prepared to give up regarding their liberties. The people's will creates the state, and in return, the state guarantees citizens liberties such as privacy. However, when the state begins to use their power against citizens by eroding their rights, the social contract is broken, and the state should be discarded. Thus, when the social contract theory is applied to the debate, it highlights that even though the state has the power to ensure national security they have to uphold individual rights. This is

because the absence of this will only threaten the social contract between the state and its citizens. The execution of this duty is dependent upon the rights of the individual. For this reason, it results in tension between the relationship of citizens and the state when the individual's privacy is violated. Ultimately, the social contract theory highlights the complex relationship between privacy and national security as it directly impacts the state and its relationship with its citizens. The following section will further evaluate mass surveillance, national security and privacy to determine the complex relationship between these concepts.

CHAPTER 3: EXAMINING THE RELATIONSHIP BETWEEN MASS SURVEILLANCE, NATIONAL SECURITY AND PRIVACY WITHIN THE WORLD

3.1 INTRODUCTION

This study explores the role played by mass surveillance in creating tension between the individual's right to privacy and national security. The preceding chapter provided a theoretical framework to emphasise that a social contract exists between the state and its citizens. It also highlighted that once the contract is violated, the relationship between them is weakened. Applying it to the national security and privacy debate, it shows that citizens enter into society with the state by giving the state power to rule; however, once the power is used against citizens, the social contract is violated. This chapter explores how technological advancements have caused mass surveillance to be used as an instrument to provide national security. This is followed by various arguments that claim that an individual's lack of privacy is, in some instances, a necessary trade-off to ensure national security. Arguments highlighting that such a trade-off is problematic and results in negative consequences are also presented. Lastly, the discussion will introduce the argument pertaining to national security and privacy in South Africa.

3.2 MASS SURVEILLANCE AND NATIONAL SECURITY

Mass surveillance has largely been made possible due to the rapid evolution of technology. States in the twenty-first century are capable of accessing bulk communication-associated information and content (Arun 2014:111). Additionally, they can mine the communication data to explore specific information and keywords which can identify targets. This essentially revolutionises the way people receive and exchange information and it allows government agencies to monitor citizens (Dworkin 2015:1). It allows the government to spy on an entire nation at any moment in time (Hosein & Altshuller 2017: 68). It is for this reason that mass surveillance has developed in such a way that it has become an effective tool government uses for security purposes. Therefore, national security has legitimised the use of mass surveillance to provide governments security. Watt (2017:14) notes that organised state surveillance of "specific or exact parts of the population" is not a new aspect and "it extends beyond just a specific

intelligence agency or a single country". Snowden (2019:141), along with several others, has revealed and warned that the degree of surveillance transcends and exceeds anything the public can imagine "its power touches everyone, but its hand is heaviest in communities already disadvantaged by their poverty, race, religion, ethnicity, and immigration status" (Gellman & Adler-Bell 2017). Therefore, mass surveillance has been able to redefine the future and the sustainability of states' surveillance practices. Goiten and Patel (2020) argue that the freedoms people have "to speak, travel, and worship; freedom from intrusive government surveillance; and freedom from invidious discrimination" are the guardians of our democracy. These freedoms have rarely been threatened before in our history. Duncan (2018:5) claims that the cost of surveillance has been significantly reduced due to the advancement of technology; Gürses, Kundnani, and Van Hoboken (2016:580) state that this has allowed government to use electronic signals to place entire populations under surveillance. The 2000s' introduction of new Information and Communications Technologies (ICTs) has aided governments and private companies in analysing and collecting massive databases (Zalnieriute 2015:111) by way of emails or telephone calls (Conway et al. 2017:313). People's interests, reading and travelling habits, friends or associates can be accessed in detail. This is referred to as metadata (Schuster et al. 2017:77). The sender, receiver, period (Conway et al. 2017:313), date, duration, and communication channel can also be identified (Schuster et al. 2017:77). Bernal (2016:253), notes that this data can be used to determine "religion, sexual preferences, political leanings and more". Thus, the complexity of the relationship between security and privacy has become increasingly prevalent (Cavelty & Leese 2018:63), due to what Goold and Neyland (2009:xy) describes as mass surveillance having the capacity to touch "almost every aspect of people's daily lives".

Moreover, using contract tracing for cell-phone location information, during the COVID-19 pandemic, highlights the extent to which mass surveillance can be used to monitor individuals. The movements of patients infected with Covid-19" can be tracked and has led to "authorities and the public having to weigh the value of privacy against the possibility that data collection could save millions of lives" (Amit 2020:1168). The current pandemic has made this essential, as control over data is control over bodies (Mahapatra

2021:9). Although contact tracing allows infected individuals to identify all other individuals they have been in contact with (Ram & Gray 2020:3), privacy concerns immediately arise. This is because the mass surveillance programmes can sweep up and reveal location data indiscriminately. Even though contact tracing is defended due to a health crisis, this can still lead to the data being abused.

Moreover, history has shown that surveillance powers claimed under the pretence of an emergency remain intact after the emergency has ended. They tend to "morph into tools of social control targeted against disfavoured individuals and groups" (Ram & Gray 2020:4). Before the significant development of mass surveillance, governments who wanted to spy on their citizens had to place the citizens under physical surveillance. Because this could easily be uncovered, it had political risks for the government. Also, using expensive equipment like telephone bugging had several limitations as people knew exactly what to look out for. Security has also played a central role in the expansion of mass surveillance and has significantly impacted investments and the marketing of surveillance equipment. States invest in these surveillance companies; however, they have expanded globally and provided surveillance equipment beyond their home market to various markets. Hence, Duncan (2018:58) concludes that the privatisation and securitisation of surveillance have become mutually reinforcing developments due to globalisation. Privacy International (2018) and Amnesty International (2020) report that many governments continue the expansion of their mass surveillance capacities. This is not a surprise as the increase in surveillance is the direct result from it becoming a big business. State surveillance programmes and consumers have become so united that distinguishing between the two is nearly impossible. States have become dependent on private companies to store vast sets of data in the cloud. However, these datasets are commercialised by the private sector as the datasets are sold for profit to other businesses, mainly advertisers. Therefore, states and the private sector can operate within a charmed circle, whereby intelligence is used to advance a state's commercial interests. Imperial powers usually use this to prevent losing their dominance in international affairs. Due to this, states incorporate safeguarding of their commercial interests when defining national security (Duncan 2018:186). Nonetheless, arguments

which are in favour of surveillance usually articulate and advocate for national security. Nevertheless, it in no way justifies the lack of essential safeguards which ensure that human rights are protected and that the power, which is fundamental to democracy, is balanced. Arun (2014) argues that unrestricted mass surveillance not only damages democracy but weakens it to the core.

Various arguments exist in favour of and against mass surveillance. It is based on how different groups, such as government, businesses, and civil society perceive mass surveillance. Moreover, when individuals become conscious of the observation, their behaviour changes to "favour the observer" (Waters 2018:1296); Caluya (2010:622) claims that for this reason, the panoptic schema should be seen as a "instance of change in instruments of communal control". Duncan (2019:45) claims that mass surveillance has led to the state becoming a one-way mirror where the state is capable of seeing "more of what citizens say and do; however, citizens see less of what the state does with collected data". Ultimately, when being surveilled, they become more cautious, resulting in a chilling response that has a psychological effect and leads to unintended social consequences (Hagen & Lysne 2016:86).

3.3 NATIONAL SECURITY ARGUMENTS FAVOURING MASS SURVEILLANCE

The gathering and analysing of information have placed national security agencies in the difficult position of providing security and privacy for individuals. Accordingly, Cohen (2000) emphasises that the relationship between national security and surveillance is complex for the reason that government is responsible for respecting the privacy of its citizens (Mavedzenge 2020:362) and ensuring national security (Perez 2020). As a result of the nature of modern-day threats, there comes the point where the search for greater security will become oppressive and burdensome to the public. This will be the case when the public considers what they are expected to give up so that the government can provide national security. However, at the same time, the public views the provision of security as the government's first responsibility; thus, the government faces a dilemma (Ormand 2013:16). Moore (2018:251) highlights this by arguing that when state agencies fail to

gather essential information required to accomplish their mission, these agencies are then faulted for failing to use modern methods and technologies. Therefore, when a security failure occurs, “national security is penalised more heavily than privacy issues because security failures render the individual and the state worse off”. Likewise, Perez (2020) finds that the individual’s concern for personal privacy is secondary to national security, which should be prioritised because the common good outweighs personal preferences.

According to Perez (2020), the common good necessitates surveillance methods. Schuster et al. (2017:80) confirm that mass surveillance guarantees better security and intelligence actions, which helps to prevent the loss of life. Jonathan Cable and Linna Dencik state that citizens have accepted surveillance because privacy is impossible to achieve within this digitised era (Lena & Cable 2017:766). They refer to this phenomenon as “surveillance realism” (Duncan 2018:32). Similarly, former President Barack Obama (2013) argued that “one could not have 100 per cent security and expect 100 per cent privacy with no inconvenience”. He said this when responding to Edward Snowden’s revelations about the National Security Agency’s (NSA’s) spy activities. Alternatively, Milanovic (2015:143), Cayford and Pieters (2018:94) and Solove (2011:2) state that to prove that interference is a needed response to the risk being addressed, the necessary oversight and regulations need to be implemented. This is to avoid that national security is being used for false pretences. Nonetheless, politicians continue to be accused of making a trade-off between security and privacy to legitimise national security measures that invade the individual’s privacy. Ünver (2018:8) concludes that there have never been so many violations of the individual’s right to privacy, as is currently the case in modern world history. Nonetheless, those who view surveillance as pervasive and inevitable question privacy sceptics. This is because they believe “one should not be troubled with safeguarding privacy if one has got nothing to hide and has done nothing wrong” (Solove 2011:2).

Nevertheless, this statement does not consider the fact that citizens will never know when they require their privacy to be protected. Watt (2017) argues that all citizens need privacy, even more so political activists who are agents of change. Because political

activists are prone to contest, the way power is organised within society causes them to attract the interest of the state trying to use surveillance to track or monitor their activities. Feldstein (2019:11) states that although many are against the extent of mass surveillance, more people have come to accept it, as citizens have become "resigned to the idea of a surveillance state". The use of national security to corroborate mass surveillance and interfere with privacy shows that constitutionally approved rights are limited in certain circumstances; the limitation is only "justifiable and reasonable in terms of an open and democratic society rooted within human dignity, freedom, and equality". Because national security can limit privacy, it forces states to "justify this reasoning as the relationship between privacy and national security is complex" (Cohen 2000). Hence for national security to erode privacy, the classification and scope of the concept should be effectively outlined. It should also complement the presumptions and rules on the burden and standard of proof to facilitate and establish a balance between the state's interest and the individual right to privacy. This view is promoted by the European Court of Human Rights (ECtHR). It emphasises that state members exploit the use of national security interests for their own agendas which inevitably distorts the meaning and nature of national security. Accordingly, it is vital that the meaning of such concepts is expanded and explained to improve the system, which will help to achieve the goals to prevent crime or terrorism.

Mass surveillance debates and arguments can be represented as two sides of a coin, whereby individuals who find themselves at the wrong end of mass surveillance need to understand that the state monitors them as a means safety. However, mass surveillance can also be perceived negatively. This is because of the individual's "privacy, communications, secrets and, to a large extent, freedom and individuality that are being stripped away by the government in the name of national security" (Bambauer 2013:683). In order to accurately recognise the significance of personal data and privacy matters, it is essential to evaluate how the adversary would reason. Henceforth, it is crucial to deliberate whether mass surveillance ensures national security or if it only encroaches upon the individual's right to privacy; thus, it assesses whether it is "fair […] to undermine the privacy of millions who are otherwise innocent users in order to seek out a few

criminals or terrorists" (Laidey 2015:237). Therefore, it is important to consider how this power can be abused or corrupted by various actors, such as terrorists. This is why surveillance by states should be controlled or supervised. Laidey (2015:237) concludes that rogue elements can use surveillance practices to "twist the system for their own agendas or nefarious purposes". Besides, privacy and national security are multifaceted issues to be evaluated by citizens. This is because citizens are not part of the process and they are unaware of the information agencies gather or the extent agencies go to in order to attain the information. Citizens are left to trust that the information the state has collected will not be abused; however, this is not enough; therefore, states should implement the necessary oversight mechanism which prevents them from overstepping their boundaries.

National security agencies are put in a difficult position when gathering and analysing information. This is because they have to achieve their goal of providing security but are criticised when they are unable to use the latest technologies on the market to address security threats. This includes using mass surveillance; however, when security agencies are perceived to gather too much information, citizens consider this as invading their right to privacy. Therefore, security agencies face the duty of safeguarding national security to the best of their abilities, yet they are limited by the requirement of achieving this without violating individuals' privacy. Moore (2011) argues that security grants individuals a safe environment in order to be able to take control of their lives as security protects the most fundamental right of the individual, which is the right to life. For this reason, although privacy is essential, it can never rise to the level of security of life and limb (Moore 2011:147). Perez (2020) maintains that the state's mass surveillance has reached a level which is extreme and "it threatens not only democracy but the rights of citizens that are granted under democracy". Therefore, mass surveillance has become the embodiment of the abuse, overreach, and complete violation of the individual by the state. Some state that people's individual rights should be guaranteed by all means and should serve as the core priority over any demand or expectation regarding government actions. Nevertheless, it is also vital to ponder that when a security disaster threatens a state's livelihood, its national security is judged at a higher rate than privacy security issues.

Moore (2018:251) claims that there are no contending moral claims to resolving security flaws as the individual and the state will be rendered worse off.

The tension between national security and the right to individual privacy gained significant traction in modern politics after the 9/11 terror attacks in New York. This has led to the "war on terror" and prompted the "security transformation of domestic life" (Baker 2003:548). This change led to returning to "wartime" viewpoints in modern society, which caused civil liberties to be viewed as "luxury items". This is similar to how "silk stockings were categorised during World War II; they were diverting valuable resources from the war effort" (Baker 2003:548). George (2014:220) claims that the aftermath of 9/11 highlighted the risks associated with the new environment they found themselves in; these risks included 'new' enemies of the state, which are capable of exploiting the open nature of modern society to accomplish evil ends. Therefore, the world suddenly faced an unfamiliar reality whereby boundaries or borders do not define the enemy. As a result, policymakers and academics had to determine how governments would efficiently balance providing "civil liberties while providing appropriate levels of national security measures during conflict" (Lopach & Luckowski 2006: 246). The new threats, namely "global terrorism, nuclear proliferation, and transnational organised crime", necessitate new security approaches which focus vigorously on handling risks, and preventing conflict and threats (Pavone, Gomez & Jaquet-Chifelle 2016:227).

Due to the globalised nature of the world, surveillance is vital in some cases, as the world has changed; now, the most significant threats to a state's security do not derive from other states but come from terrorism. Random individuals can now undertake massive attacks on citizens, threatening the state's national security; hence, surveillance will continue to play a significant role in our lives. Threats, such as terrorism, denote a unique challenge within modern society and have resulted in states implementing mass surveillance practices to ensure national security. After 9/11, many countries reformed their privacy laws; at the forefront were the United States of America (USA) and the United Kingdom (UK). Likewise, many states justify using mass surveillance to ensure national security by limiting individual privacy because the well-being of states faces higher risks

in the twenty-first century. According to Larson (2020), threats such as terrorism have allowed many to welcome their privacy to be restricted in the name of national security. For this reason, states argue, “if people do not have anything to hide, they should not have anything to fear”. This justification is attributed to George Orwell; similarly, Joseph Goebbels, the Nazi Minister of Propaganda, is known for using this justification. However, this argument is problematic as it adopts the narrative that states use surveillance based on pure intentions. It ignores that states can use this power to spy on those who challenge them, such as political opponents and “investigative journalists whose aim is to hold governments to account for their actions” (Duncan 2018:4).

Nonetheless, states universally continue to validate the use of surveillance on citizens as a “necessary evil” to successfully address threats to national security, specifically the significant threat that terrorism poses (Duncan 2018:4). Other states reason that besides terrorism or crime, surveillance exists to “calm communal associations and, more specifically, in order to collect information on [those] who risk exposing or challenging the way society is currently being organised” (Duncan 2018:4). Notably, the main objective of surveillance in the broader environment is to classify individuals under observation as problem subjects who are considered susceptible to public and private influence; thus, the aim of surveillance is determining individual risk profiles. Once it is determined that they are risks, they are then managed as risks. This allows states to act against the risks; when they shift to extreme risks, states can effectively act against them, which is referred to as intelligence work. However, the wide-ranging understanding of what can be seen as a national security threat, along with the advancement in technological use of mass surveillance, has serious consequences. It has resulted in state spies being able to gain excessive amounts of personal information which violates the individual’s right to privacy (Duncan 2018:5).

Acknowledging the right to privacy is not a new phenomenon; it is deeply rooted in history. Anthropological and psychological studies have proposed that all civilisations, regardless of being advanced or underdeveloped, implement mechanisms and bodies allowing them to “repel infringement from other entities or people” (South African Law Reform

Commission 2005:37). Therefore, what is essential to the security versus privacy debate is effectively balancing the state's safety and security needs with the needs of society. Public safety here refers to collective benefit, whereas the infringements of privacy by the state to ensure public safety tends only to affect "persons or minute or politically negligible groups of individuals, usually taking place over a short [period of] time" (Hladik 2014:35). Hladik (2014:35) concludes that this allows officials in charge of communal protection to have more access which disregards and diminishes the confidentiality apprehensions that their activities could cause. The government has to consider the degree of the threat by evaluating whether it is a shallow risk to an individual or a higher risk to society (Ormand 2013:23). Therefore, where the risks are small, the constraints on liberty will be few; however, where the risks are more significant and imminent, citizens should expect "liberty to be appropriately, substantially and justifiably diminished" (Kleinig et al. 2011:174). Raab (2017) claims that individuals seek privacy, but citizens seek protection from harm; thus, in the end, the privacy that individuals want needs to be weighed against the security that is needed. Galantonu (2016) argues that "[a] person is freer if one understands the necessity of security than if one struggles for more civil liberties". It is essential to consider that because technology is so fast-paced, mass surveillance is used in order to connect and integrate all data to keep up with technological advances (Galantonu 2016:61).

3.4 PRIVACY CONCERNS OPPOSING MASS SURVEILLANCE

States' use of mass surveillance to ensure national security has led to privacy being traded off for security (Lieshout et al. 2013:124). Ünver (2018:8) argues that there have never been so many violations of the right to privacy due to "the use of mass surveillance for security purposes". Arun (2014) defines this as a feeling of Big Brother being omnipresent, causing individuals to fear that the state will use the organs of state against them. *Permanent Record* by Snowden (2019) claim that the public of not only one country but of the whole world was never granted the opportunity to "raise their view or vote on mass surveillance methods". Therefore, the existing system can only be defined as

universal surveillance. It has been formed and established without considering consent by purposely hiding crucial programme characteristics from the public.

Furthermore, Snowden (2019:150) refers to the lack of consideration for individual privacy as democracies regress into authoritarian populism. Mahapatra (2021) also refers to this as authoritarian creep occurring within democracies due to states' use of mass surveillance. Moreover, advanced governments are deteriorating with regard to safeguarding the individual's right to privacy. Yet, Article 12 of the United Nations Declarations of Human Rights considers it a fundamental right and that "no individual should be exposed to indiscriminate intrusion regarding their personal affairs or letters and assaults on their status and integrity" (United Nations 2015:12). But under the current use of mass surveillance for national security purposes, privacy has become moot. This means nothing prevents the authorities from using the collected data to implement larger social monitoring and control (Stahl 2016:35). Moore (2018:134), argues that this distorts the line that Aristotle established between "the private sphere of the home and the public sphere" which is concerned with political activity. In the same way, Bauman et al. (2014:136) claim that the distinction between the state and civil society (public and private) is a significant component of the twentieth century.

Nevertheless, governments continue to argue that people have nothing to fear if they do not have anything to hide (Scheiner 2015:92). Watt (2017) problematises this statement as it adopts the notion that governments' motives for undertaking surveillance are pure and citizens will never be able to distinguish when the right to privacy is needed. It is for this reason that Bambauer (2013:683) and Davis (2003:178) advocate for balancing the security needs of society and government in order to avoid eroding the right of individuals to privacy (Etzioni 2014:36). The national security argument that supports the use of mass surveillance does not equate that with "anything goes". It also does not validate the lack of "regulation, accountability, oversight, and the violation of citizens' civil liberties" (Bigo 2013:34). Duncan (2018:31) and Bernal (2016:245) claim that advanced government has significantly declined in protecting the right of privacy. The latter is regarded as a critical human right that "upholds human dignity and maintains values such as freedom of association and speech".

The European Conventions on Human Rights (ECHR) contains the most compelling articulation of the right to confidentiality. Additionally, the legal norms pertaining to international human rights entail clear reasoning behind any type of intrusion with the individual's right to privacy. The *Liberty versus United Kingdom (UK) case* highlighted the mass surveillance issues of the European Court of Human Rights (EctHR). The outcome of the case revealed that the UK's method of obtaining information contravened the protection of privacy granted under the ECHR. Although the case was significant, Arun (2014:111) highlights that it was unsuccessful in providing proper or suitable guidelines to protect the right to privacy and surveillance. Ultimately, when governments secretly use mass surveillance mechanisms, it showcases the risk of arbitrariness. Cayford and Pieters (2018:94) argue that when states use mass surveillance to ensure national security, citizens should be provided with a "clear and adequate indication of the circumstances surrounding what kind of interceptions will take place". The UK case was largely influenced by civil society organisations such as Big Brother Watch, the Open Rights Group, English Pen, and Constanze Kurz. These organisations took the UK government to court because of the mass surveillance of data. Navi Pillay, the previous UN Special High Commissioner for Human Rights, maintained that "the right to privacy is of utmost importance" (Arun 2014:112); she too argued that safeguards must be implemented to protect the individual's right to privacy with regard to mass surveillance.

Similarly, Scheiner (2006) emphasised that internal procedures adopted to safeguard individuals' privacy "without monitoring an external independent entity" are insufficient in protecting the individuals. The right to privacy should be acknowledged as a societal interest in order to provide assistance to frame the surveillance debate. The focus should be placed on oversight and accountability mechanisms. The government's expansion of surveillance capabilities raises a growing concern as the purposes for which it is used are being questioned. The intentions behind states using mass surveillance are being assessed. It is specifically assessed with regard to whether it is to secure the safety of citizens and uphold democracy or for malicious reasons. Malicious reasons would include instances such as repressing social control to pacify citizens or specifically those that the state regarded as a threat to their interests.

Duncan (2018:45) states that in order to address unaccountable surveillance effectively, collective action should be implemented. This is because the enigmatic nature of mass surveillance activities is alarming to individuals. Despite this, states continue to invest significantly in mass surveillance activities which raises privacy concerns. The government of Singapore has implemented E3A, which means “Everyone, Everything, Everywhere, All the Time” (Moore 2018:131). “Everyone, Everything, Everywhere, All the Time” was created to provide mass surveillance, determine whether big-data analysis prevents terrorism, and, to a larger extent, examine how technology is used to engineer a harmonious society (Stahl 2016). Initiatives like this immediately spark privacy concerns because there is no constitutional right to protect citizens’ privacy; therefore, citizens’ autonomy and agency become weakened. However, the enhancement of the executive’s power can be used positively in certain cases, such as distributing welfare more extensively and guaranteeing universal healthcare through access to credit. Although executive power can be used positively, it is essential to consider that it can also be abused. This abuse occurs when specific groups are targeted by rejecting access or preventing them from voicing opposing opinions and thereby separating the groups.

During the 2014 protests in Ukraine, protestors in Kiev received text messages from state agencies. They claimed that they were “aware of citizens participating in mass riots and that they knew their identities and watched them” (Moore 2018:245). Henceforth, mass surveillance can significantly jeopardise politics as it has become ‘plagued by algorithms and automation’; this is because surveillance democracy makes it impossible for individuals to “preserve anonymity or protect themselves from their privacy being invaded” (Moore 2018:245). Mass surveillance is a direct result of the over-prioritisation of security; for this reason, the focus of the debate on privacy in security should be directed towards implementing proper checks and balances (Ergun 2018:22). Finding the appropriate combination of judicial and legislative action to provide national security and uphold individual rights and freedoms is complex. The maximum security is required in a peaceful society at the minimum expense of infringing on human rights (Ergun 2018:24). Ormand (2013) also states it in a democracy, it is vital to ensure public security through the confidence that government can manage risks while also respecting society’s human rights and values. New laws should be implemented to regulate when and how

governments conduct mass surveillance in the modern era (Hosein & Altshuller 2017:69). If privacy should be traded for security, there should be probable cause, meaning states should adhere to strict rules to justify the interference (Bauman et al. 2014:132). Also, accountability and transparency should be established (Moore 2011:153). Proper safeguards against mass surveillance (Ring 2016:7), transparency and congressional oversight will prevent governments from abusing their power (Pozen 2016:245). The absence of these safeguards will only result in mass surveillance being used as a tool of repression and exclusion (Mahapatra 2021:1). It can also mitigate the risks of the function of mission creep[7] (Maras 2012:67), which is rooted in fear of the abuse of power by governmental authorities (Galantonu 2016:59).

The core problem of mass surveillance comes down to the question of "Quis custodiet Ipsos custodes?" This translates into who watches the watchmen? (Raab 2017:83). Thus, although laws can be made to keep the government in check, technological change outpaces the capability of lawmakers, judges, and overseers (Raab 2017:95) to keep up with a regulation that includes privacy concerns (Raab 2017:96). Therefore, unless privacy concerns are addressed, they will proliferate into potentially intractable problems (Hammond-Errey 2022:21). The over-dependence on national security results in a dangerous imbalance within the security system, and it also threatens democracy because it decreases the security of society retroactively. Hence, "more security might mean less security when society does not need more security but better security" (Pavone, Gomez & Jaquet-Chifelle 2016:240). Lord Acton states that "power tends to corrupt, and absolute power corrupts" (Acton Institute 2022). Moore (2011) claims that 'if information control can yield power and mass surveillance results in total information awareness that radically expands that power'. Because of this, it is a necessary to question trading the right to privacy for security. Citizens have the right to be protected against the state's excessive intrusion of their liberties, freedoms and rights (Trood & Bergin 2015:7). Benjamin Franklin once said: "Any society that would give up a little liberty to gain a little security will deserve neither and lose both" (Levi & Wall 2004:206). Ultimately, the arguments presented by those in favour and against mass surveillance do

[7]The gradual or incremental extension of a mission, project or intervention beyond its intended focus, goals or scope, a ratchet effect due to original victory.

not show how to effectively balance national security and privacy; hence, little attention is given to solving or mitigating issues regarding mass surveillance.

3.5 NATIONAL SECURITY VERSUS PRIVACY IN SOUTH AFRICA

South Africa's Constitution articulates the individual's right to privacy and upholds that the individual has the "right to personal autonomy and is free from interference or disturbance of the individual's private life" (Constitution 1996). Moreover, the Constitution safeguards the informational right to privacy, concluding that the individual's information cannot be disclosed without consent (Currie 2008). However, the broad conceptualisation of national security in democratic South Africa, understood as freedom from fear and want, has resulted in the securitisation of an array of issues. Securitisation is understood as the process whereby the state transforms political issues into security issues enabling the state to adopt extraordinary measures to protect security. According to the Copenhagen school of thought, securitisation occurs by socially constructing security issues through analysing who or what is being secured and from what. Issues become securitised or treated as security issues through "speech-acts which do not simply describe an existing security situation, but bring it into being as a security situation by successfully representing it as such." (Williams 2003:513). Desai (2018) argues that the broad understanding of national security has allowed the justification and the expansion of the mandate of the intelligence services. Burchell (2009:8) equates the securitisation of the "public and private spheres of life" to the lack of suitable checks and balances. Therefore, in South Africa, the privacy versus national security debate occurs in an environment where the securitisation discourse has legitimised surveillance differently than during the era of the apartheid government. Thus, the following chapter will analyse South Africa as a case study to examine the relationship between privacy and security.

3.6 CONCLUSION

This chapter has shown how mass surveillance has become a tool to provide national security; it has grown to the point where every sphere of life is monitored. Some justify this because the security environment has changed. It requires the expansion of surveillance and the trade-off between security and privacy. However, this violates the

fundamental right of the privacy of individuals. Thus, the state's misuse of power and the lack of transparency and accountability have created conflict between national security and privacy. When applying it to the social contract, mass surveillance continues to threaten the relationship between the state and its citizens. This is because the continuous violation of citizens' privacy threatens the trust in government and democracy as a whole. The extent to which information about individuals is collected occurs at an entirely different scale than anything possible and imaginable before; this presents a significant threat to the social contract between the state and citizens. The current use of technology coupled with the extensive reach of mass surveillance has weakened the social contract between the state and its citizens. This is because it erodes the individual's right to privacy and human dignity. The next chapter will assess the relationship between national security and individual privacy in South Africa from 1994 to 2021.

CHAPTER 4: NATIONAL SECURITY VERSUS THE RIGHT TO PRIVACY IN SOUTH AFRICA BETWEEN 1994 AND 2021

4.1 INTRODUCTION

The following chapter examines the relationship between national security and privacy within South Africa from 1994 to 2021. This will be done to determine whether the relationship between these concepts is indeed complex. It will also assess whether mass surveillance has become a tool that is used to ensure South Africa's national security, yet has led to the violation of the individual's privacy. The history of South Africa's security environment along with the country's surveillance legislation will be discussed. The purpose is to determine the effectiveness of this legislation in protecting the individual's right to privacy and whether trade-offs between national security and privacy are made. Also, it is necessary to determine if this has led to the strengthening or weakening of the relationship between the state and citizens according to the social contract theory. To begin, it is necessary to briefly review the historical context of national security during apartheid.

4.2 TRANSFORMATION OF SOUTH AFRICA'S NATIONAL SECURITY

4.2.1 Role of Colonisation and Apartheid

The concept of surveillance was instrumental in the colonial conquest of South Africa. Mass surveillance took place through the introduction of passbooks to enslave Africans and the indigenous Khoikhoi during the eighteenth century. The age of mining (1867) facilitated the panoptic surveillance of workers through the invention of closed compounds and technologies such as skin branding[8], photography[9], and fingerprinting[10] (Kwet 2020:20). Under the apartheid government, mass surveillance took place through implementing a strict regimented racial order. This linked race with the centralisation of

[8]The process in which a mark, usually an ornamental pattern or a symbol, is burned into the skin of a living person, and the resulting scar ensures that it is permanent. This was done as a punishment or to impose masterly rights over enslaved people.
[9]Photographs were used to create racial and physical stereotypes of different groups of colonised people.
[10]Fingerprinting was a reaction to Britain's belief of their supposed 'superiority' and its resulting racism. It served as a personal identification because the ridge arrangement on every finger is unique to every human being and does not change.

surveillance controls which ensured that races were separated and would be easier to monitor (Mutung'u 2021:163). Moreover, intelligence such as communication surveillance was gathered by using the police and special forces, and the aforementioned pass laws were implemented (Africa 2009). When P.W. Botha came into power in 1978, his administration centred the primary role of the government around the security structures, known as the "Total Onslaught" concept (Van Heerden 2019:48). This meant that the executive power was centralised within the Botha presidency, and policy-making involved military personnel, which meant that South Africa became significantly militarised (Van Heerden 2019:48). Thus, the colonial and apartheid era implemented various surveillance methods to control the movement of people of colour, specifically their economic and political activities.

Consequently, white elites within the public and private spheres were able to administer a dystopian surveillance state that humiliated and brutalised Africans for centuries (Kwet 2020:20) The secrecy culture of the secret services within modern South Africa can be traced back to its history with the establishment of the Union of South Africa in 1910. White power was characterised and consolidated through the creation of security institutions which amalgamated the former colonies and Boer Republics. The South African Police Service (SAPS) and the Union Defence Force (UDF) were tasked with integrating the different security cultures into one. The purpose was to maintain the racial exclusion that characterised South Africa during the twentieth century. Seegers (1986) argues that the formation of these institutions was the beginning of the system of state secrecy in South Africa.

The main objective of the intelligence services within this period was to protect the colonial regime and ensure that potential anti-colonial resistance was identified and addressed early on (Africa & Kwadjo 2009:64). The apartheid regime similarly used the intelligence services, particularly the military and police, to identify and target political activists (Duncan 2018:57). The P.W. Botha-led regime focused on promoting special operations units within the intelligence agencies to combat perceived revolutionary threats. Thus, these units conducted multiple covert operations against the liberation movements within and outside the country; these included engaging in "dirty tricks against their enemies,

spreading disinformation about them and engaging in kidnapping, arrest, torture, poisoning and assassination" (Duncan 2018:59). Moreover, Germany and the United Kingdom (UK) provided the apartheid regime with communications surveillance equipment, although South Africa faced an arms embargo by the United Nations in 1977 (Duncan 2018:60). There are few surviving records of the South African intelligence services under the apartheid regime. The Truth and Reconciliation Commission (TRC) exposed testimony by a former official who claimed that the intelligence services destroyed over 44 tons of records before the country's first democratic elections (Africa & Kwadjo 2009:68). Therefore, the key to the colonial and apartheid rule was that it operated under a veil of secrecy. This allowed surveillance mechanisms and social control to prevail. It is important now to evaluate the shift from such security practices to the current security dynamics in democratic South Africa.

4.2.2 National Security Post-1994

Ultimately, the end of the apartheid era introduced significant changes to the security dimension of the country. Transformations focused on creating a new society based on values grounded in "human dignity, equality, and security", which were originally articulated in the Freedom Charter (1955). In contrast to the apartheid model that militarised all facets of national policy, the new method demilitarised the concept of security to focus more on human security (Cock & Mckenzie 1998). In order to move away from a state-centred approach to security, the human security concept became the dominant discourse. This was to avoid the fear and scepticism caused by the apartheid regime. National security is addressed within Constitution and the White Paper on Intelligence; both of which communicate human security sentiments. Section 198 of the Constitution is concerned with national security and states that it must "reflect the resolve of South Africans" (Constitution 1996). Section 200 of the Constitution places the emphasis on the key role of the defence force namely defending and protecting the "territorial integrity and people of the Republic" (Constitution 1996). This should occur in adherence with the Constitution and international law principles. The right to privacy is articulated within Section 14 of the Constitution and emphasises the individual's right to autonomy:

> 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;
> (d) the privacy of their communications infringed.

The Constitution also provides the informational right to privacy; this means that the informed consent of the individual and expression is needed before the information is disclosed (Currie 2008). Furthermore, the national security environment of South Africa also witnessed significant changes within the intelligence structures after 1994, which is observed by the adoption of the White Paper on Intelligence (1994). The adoption of the White Paper on Intelligence took place during the Interim Constitution (Act 200 of 1993) and the transformation of the intelligence institutions. Thus, the core of the White Paper on Intelligence (1994) was to restructure the intelligence dispensation during the post-apartheid era. Cock and Mackenzie (1998) note that the narrow focus of national security adopted by the previous minority government was no longer feasible as it represented an undemocratic society (Cock & Mckenzie 1998). Buzan (1991:29) states that internationally the focus was broadened to be more inclusive and consider threats to environmental, socio-economic and political aspects, which involved “more than the mere concentration of state power”. Accordingly, the White Paper on Intelligence (1994) represented a move away from the traditional military emphasis on national security. The two policy documents vital to refocusing the South African military post-apartheid are the White Paper on Defence (1998) and the Defence Review (1998). Greg Mills claimed that “South Africa’s 1994 transition to democracy meant, among other changes, adopting a new approach to defence with the creation of the South African National Defence Force (SANDF)” (Daniels 2019:1). In 2011, the Defence Review Committee (DRC) was formed. The purpose was to assess the country’s defence policy in order to be able to face essential and rapid changes and adapt to these changes in the strategic environment.

The review was done to formulate a modern force that is flexible and balanced. It is a force that uses advanced technology, and can operate and face the changing nature of the defence sector internationally (Daniels 2019:4). According to the 1998 and 2015 Defence Reviews, the role of the defence force in attaining South Africa's national security goals to advance its international, regional, and national interests is greatly emphasised. Similarly, the White Paper on Defence (1996) states that national security is an "all-encompassing, broadened concept". It is mainly concerned with moving away from the high level of state militarisation towards a consideration of individual security ensuring that citizens can live in peace safety and freedom (Van Heerden 2019:4). The White Paper on Defence marks a break from the repressive and aggressive strategies that the National Party government implemented (Cock & Mckenzie 1998).

The Constitution stipulates that South Africa's national security ensures the advancement of its "sovereignty, democracy, national values and freedoms, and political and economic independence" (South Africa 1996). The White Paper on Defence articulates that national security in the country will be "sought primarily through efforts to meet the political, economic, social and cultural rights and needs of South Africa's people, and through efforts to promote and maintain regional security" (South Africa 1996). Therefore, following the declarations mentioned above, it can be maintained that South Africa associates its national security closely to its domestic and regional environment. South Africa's National Defence College created a model which highlights the country's national security; it is known as the "national security quintet". The national security quintet highlights several dimensions which form part of the country's national security; these are "national values, national interests, national power, national identity, and national will" (Bester 2019:12). The Constitution concludes that South Africa's national values are "human dignity, the establishment of equality and the protection of human rights and freedoms"; this includes principles such as "non-sexism and non-racialism" as national values. The Defence Review states that South Africa's national interests are:

> "Those cardinal interests that, if threatened or removed, would compromise the sovereignty, independence, survival, continuance or liberty of the Republic and therefore are considered vital for the functioning of the state, the security and well-

> being of the people and the preservation of the South African way of life" (South Africa 2015:3-4).

Moreover, "universal adult suffrage, a national common voters' roll, regular elections and a multi-party system of democratic government ensures accountability, responsiveness and openness" (South Africa 1996). These are the national values that the country seeks to uphold. It also links people's development through uplifting them and their well-being to achieve freedom from fear and want. National power is considered the "unified application of its political, diplomatic, informational, economic, social and defence domains" (South Africa 2015:3). Therefore, these sectors are considered to be part of the state's power. It will be utilised to address threats to democracy and the state's national interest through "cross-government, multi-agency and regional cooperation" (South Africa 2015:3-5). The aspects of the national security quintet show that national security within South Africa is linked to human security, which focuses on the individual. Democratic South Africa's conceptualisation of security is broadly defined; this has led to an increase in the securitisation of various issues resulting in "massive expansion within the intelligence services and mandate" (Desai 2018). Moreover, the lack of checks and balances has led to the securitisation of more domains of the public and private realm (Burchell 2009:8). South Africa also has international obligations to protect the right to privacy in adherence to the International Covenant on Civil and Political Rights (ICCPR). All states that abide by the Covenant recognise, per the Charter of the United Nations, the equal inalienable rights and the inherent dignity of all humans. These are the foundation of peace, justice and freedom in the world. Article 17 of the ICCPR states that:

> 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.

South Africa has a rich jurisprudence when applying the principle of proportionality in limiting fundamental rights. The Human Rights Committee understands the ICCPR's Article 17 as ensuring that states are aware that "any interference with privacy must be

proportional to the end sought and be necessary in the circumstances of any given case" (Barrie 40:2013). The courts have adopted a broad interpretation of proportionality:

> is a safeguard for the individual, over and above traditional methods of controlling the state's administration. It involves a balancing act between the competing interests and objectives of the state… Proportionality demands that when an individual's rights are affected or threatened by state action, only such action shall be countenanced which is suitable, necessary and not out of proportion to the gains to the community (Barrie 40:2013).

Ultimately, the transformation made by South Africa in shifting form a traditional state-focused approached of national security towards a human security-centered one highlights the importance that South Africa places on individual rights. This includes the individual's right to privacy which is grounded within the Constitution and legislation. Therefore, against this backdrop, the intelligence security structure of South Africa post-1994 was restructured.

4.2.3 Changes to South African Intelligence Services post-1994

The new intelligence services came into being in 1995 with the amalgamation of the National Intelligence Services (NIS). It included the South African Secret Service (SASS); the National Intelligence Agency (NIA); the Transkei Intelligence Service (TIS); the Bophuthatswana Intelligence and Internal Service (BIIS); the Department of State Security (DIS); the Venda National Intelligence Service (VINS); and the Pan African Security Service (PASS) (Africa 2012:107). In order to make provision for the amalgamation, new pieces of legislation were tabled; the Intelligence Services Act 40 0f 1994 was adopted. This confirmed that the unification of the intelligence service was "to regulate the establishment, organisation and control of the National Intelligence Agency and the South African Secret Service; and to provide for matters connected in addition to that" (Van Heerden 2019:51). Furthermore, the National Strategic Intelligence Act 39 of 1994 aimed to:

> Define the functions of members of the National Intelligence Structures; to establish a National Intelligence Co-ordinating Committee and to define its

> functions in respect of intelligence relating to the security of the Republic, and to provide for the appointment of a Coordinator for Intelligence as chairperson of the National Intelligence Coordinating Committee, and to define his or her functions; and to provide for matters connected in addition to that (Van Heerden 2019:51).

In 2009, the intelligence services underwent another restructuring to improve operational effectiveness, centralise the budget, update the administrative process and refocus its intelligence priorities (Cwele 2009:1). Accordingly, the State Security Agency (SSA) was created, which combined all the former civilian intelligence structures; these are: the Electronic Communications (Pty) Ltd; The South African National Academy of Intelligence (SANAI); The National Communications Centre (NCC); The National Intelligence Agency (NIA); the South African Secret Service (SASS); and the Office for Interception Centres (OIC) (News24 2009:1 & SSA 2016:1). The restructuring of the intelligence services occurred against the backdrop of new democratic security, which was facing a changing security environment with new threats to consider.

4.2.4 New Security Threats in South Africa Post-1994

During the years 1994 and 2009, South Africa faced various domestic threats to its security. It included “serious crimes such as murder, attempted murder, rape, assault GBH (assault causing grave bodily harm), aggravated robbery, commercial crime and drug-related crimes” (Pienaar 2014:84). The Institute for Economics and Peace (2009:11) and the Centre for the Study of Violence and Reconciliation (2009:3) issued an important statement. It stated that within the first few years of democracy, South Africa met “extreme levels of serious crime”. Between 1994 and 2009, over 395 807 attempted murder cases were recorded. In 2003, the United Nations Office on Drugs and Crime (UNODC) stated that South Africa faced a severe problem with high levels of rape cases and other forms of sexual assault. “The situation appears [to be] at its worst in SA, with the reported rates of rape among the single highest in the world” (UNODC 2003:11). During 1994 and 2007, more than 51 998 rape cases were reported to SAPS, on average “142 people were raped per day in South Africa over the first thirteen years of democracy” (Pienaar 2014:94).

According to SAPS (2007:224), the total number of rapes during the time mentioned above period was 675 974.

Other violent cases included assault cases; SAPS (2003:30 & 2009:5) claimed that between 1994 and 2009, a total of “3 578 632 cases of assault” averaged at 654 cases daily. Moreover, crime was significantly high between 1994 and 2009, and ‘more than 4 million residential burglaries were reported in South Africa’ (Pienaar 2014:100). Leggett (2002:3) claims that in 1994, South Africa experienced an “influx of chemicals that international isolation during [the] apartheid years had kept out”. This allowed drugs like heroin and cocaine to “increase in popularity, since the first democratic elections”. The period between 1994 and 2009 witnessed a “total of 975 650 drug cases” being reported (Pienaar 2014:105). Furthermore, migration to South Africa created tensions between citizens and foreign nationals. In 2010 during the Budget Vote, Minister Siyabobga Cwele highlighted xenophobic attacks “against foreign nationals as a security concern” (Cwele 2010). The draft Defence Review (South Africa 2012:75) noted that foreign migrants see South Africa as a destination due to “perceived opportunities and stability in contrast with instability and deprivation in some areas of the continent”. Therefore, the Draft Defence Review emphasised that “high levels of illegal migration into Southern Africa pose a serious threat to South Africa’s national security and stability” (South Africa2012:75). Epidemic diseases also have an impact on the nation’s well-being. South Africa noted that the “pandemic of HIV/AIDS, [and] outbreaks of a communicable disease including re-emerging diseases such as tuberculosis, diarrhoea and pneumonia which interact in vicious feedback loops with malnutrition and HIV” represent a significant threat to the social well-being of the country (South Africa 2012:74).

Currently, in 2022 the unemployment rate stands at “63,9% for those aged 15–24 and 42,1% for those aged 25–34 years, while the current official national rate stands at 34,5%” (Statistics South Africa 2022). Over the years, high poverty and unemployment rates have often sparked violent service delivery protests. It also increased the tension between citizens and foreigners, causing violent xenophobic attacks (Mamabolo 2015). In July 2021, South Africa experienced riots which resulted in devasting violence and shut down the country’s ports and roads. It also led to the deaths of 350 people (Africa 2022). It

caused massive economic damage as infrastructure was destroyed, and malls and stores were looted (Africa 2022). It cost the economy over R50 billion (Cele & Wilson 2021). President Cyril Ramaphosa characterised the riots as an "insurrection and a calculated, orchestrated effort to destabilise the country, sabotage the economy, and undermine constitutional democracy" (Givetash 2022). According to the Defence Review, the most serious threats to South Africa are "crime, natural and man-made disasters, breakdowns of essential services, the plundering of resources, protests, [and] civil disobedience/unrest" (South Africa 2015:D-14).

The above-mentioned security threats focused on domestic threats. South Africa also faces external threats. The current regional reality which threatens the country's national security is the terrorist attacks in Cabo Delgado, Mozambique (Defence Web 2021). Ahlu Sunna Wal Jammaa (ASWJ) is an insurgency group functioning in the northern province of Mozambique. The militia group's name means "people of the Sunnah community", and it is also referred to as "Al-Shabab" or "Ansar al-Sunna Islamist". Since October 2017, the group has been responsible for attacks and atrocities. It has caused the deaths of 'over 3 100 people and displaced more than 850 000 people', causing a humanitarian crisis (SABC 2022). The Defence Review (2015) claims that terrorism signifies a number of threats to South Africa's national security. These include the "possibility that terror groups could use [the] South African territory to attack another state" (South Africa 2015:2-29). The country can also be seen as a "conduit or transit zone for the movement of terror groups or to attack foreign target[s] on South African soil" (South Africa 2015:2-29). Furthermore, it can threaten South Africa's 'vital interests, either domestically or externally' (South Africa 2015:2-29). The new security threats that South Africa faced presented the need to address the threats through mechanisms to protect the country's national security; these include legislation for mass surveillance.

4.3 SURVEILLANCE LEGISLATION IN SOUTH AFRICA FROM 1994 TO 2021

4.3.1 Legislation Implemented from 1994 to 2020

The end of apartheid and the move to democracy in South Africa marked the implementation of several new laws which dealt with information, security, and privacy.

The intelligence agencies in South Africa are ruled by the following Acts that were adopted in 1994: the Intelligence Services Act 38 of 1994; National Strategic Intelligence Act 39 of 1994; and the Intelligence Services Control Act 40 of 1994. These laws signify the oversight and operational tools to enforce domestic and foreign surveillance. Some laws which create the basis for surveillance are the Financial Intelligence Centre Act 38 of 2001 (FICA) and the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004. The Financial Intelligence Centre Act 38 of 2001 (FICA) was implemented to combat threats and fight financial crime such as “money laundering, fraud, tax evasion, terrorist financing activities and identity theft”. Moreover, the Cybercrimes Act 19 of 2020 has recently been passed to “create offences of unlawful interception of data, messages, computers and networks involving hacking, ransomware attacks and cyber extortion”. The legislation that mainly relates to domestic surveillance is the Regulation of Interception of Communications and Provisions of Related Information Act 70 of 2002 (RICA), which was adopted due to 9/11. As a direct result of the 9/11 attacks, RICA is responsible for regulating domestic communication within South Africa (South Africa 2002). The Regulation of Interception of Communications and Provisions of Related Information Act 70 of 2002 replaced the Interception and Monitoring Prohibition Act 77 of 1992 (IMPA). The leading role of RICA is governing lawful interceptions of policing; this ensures national security. The Regulation of Interception of Communications and Provisions of Related Information Act 70 of 2002 controls direct and direct communications such as “emails, mobile phone transmissions and communications that produce data, text, visual images or a combination of these” (South Africa 2002). Notably, the monitoring and interception of these communications occur by using extremely sophisticated technology. Importantly, RICA requires companies to store metadata; this details individuals’ interests, reading or travelling habits, and their associates or friends. (Schuster et al. 2017:77). It can also identify the sender, receiver, time (Conway et al. 2017:313), date, duration, and communication channel (Schuster et al. 2017:77). Furthermore, it can determine religion, sexual preferences, political leanings and so forth (Bernal 2016:253). Several shortfalls exist within RICA; this includes the Parliamentary committee, which oversees intelligence services (Privacy International & Right2Know & Association for Progressive Communications 2016:3). The committee has

a mandate to deliver a public report discussing the manner in which RICA is applied. However, the data accessed cannot provide how many individuals' communications have been intercepted—thereby allowing mass surveillance to occur. This is because there is no indication of the extent of the interception or violation of privacy. After all, individuals are unaware that their communications have been intercepted.

Duncan (2018), highlights that the reports written by judges demonstrate the oversight challenges that occur when surveillance is requested. Only the number of warrants is released, but this could account for several individuals, meaning that the number of individuals whom the interception impacts, is not disclosed because of a lack of transparency. Moreover, the report fails to provide a reason for interception and the success that it has with regard to investigating or preventing crimes (Privacy International & Right2Know & Association for Progressive Communications 2016:3). Thus, the lack of reporting mechanisms to disclose the statistics on the collection and use of metadata proves to be another shortcoming of RICA. This is because the RICA judge is tasked with writing the parliamentary reports and hearing the applications of surveillance reports. However, the applications lack sufficient information that the judge requires. Moreover, the judge is solely responsible for multiple requests. Furthermore, the extreme dependence on continuously using threats to national security as a basis to intercept the communications of journalists or protest organisers poses a problem (Mutung'u 2021:173). This is dangerous as it can limit journalists' and protest organisers' right to privacy and their freedom of expression and speech, which is safeguarded by the Constitution and is fundamental within a democracy. Consequently, Duncan (2018) states that RICA fails to provide transparency, even though it offers oversight mechanisms as operational oversight still occurs within institutional arrangements. It is therefore, ineffective in providing transparency of the process used to intercept communications.

Furthermore, the Office for Interception Centres (OIC) can be used by law enforcement through interception warrants. The OIC was established in line with RICA, and its primary duty is reporting to the Minister of Intelligence services. The office acts as a centralised service for law enforcement agencies involved in addressing national security threats. The OIC's duties include reporting its quarterly responsibilities to the SSA. However,

surveillance reports are never published openly; thus, the public cannot scrutinise them even though the Intelligence Service Act 65 of 2002 permits public criticism (South Africa 2002). Public criticism would allow individuals to form part of the operational oversight process and ensure that state agencies adhere to regulations. However, due to high levels of secrecy and a lack of transparency within the intelligence services, they cannot be held accountable when interception of individuals' communication occurs. This violates privacy and goes against the regulation that it should be reported. Members of Parliament (MPs) and the Inspector-General of Intelligence possess extensive power to examine the intelligence and counterintelligence actions of all law enforcement agencies and review and investigate public complaints. Ultimately, the lack of notifying citizens of surveillance prevents the public from "questioning the surveillance because they are unaware that that their communications have been intercepted" (Mutung'u 2021:173).

Section 16(5) of RICA lists the valid objectives of surveillance. Section 16(5)(iii) broadens the grounds for reasonable threats, which permits intelligence gathering based on potential threats to safety, public health, and national security (South Africa 2002). Another concern is that communication service providers must retain information about information and metadata. This is concerning since metadata can give one substantial insight into individual behaviour such as phone calls or text messages sent. This includes who was spoken to, the duration of the call, where it occurred and "[…]every phone call or text message you've made or received since" (Hunter 2019). Mutung'u (2021:178) also notes that the OIC is responsible for providing fibre optic cables for service providers' use for communications. This allows the OIC to carry out surveillance without requiring authorisation, and the authorisation can be extended for additional surveillance. Law enforcement agencies can use the section 205 of the Criminal Procedures Act 51 of 1977 to gain access to metadata. Police officers are then able to request a court order in order to access metadata for investigation purposes. Service providers who give this information are not required to appear in Court. Swart (2017a) highlights that the "request does not have to be made before a RICA judge; this allows law enforcement officers to gain orders from other courts". This resulted in unreported communication surveillance outside parliamentary oversight and judicial safeguards. Therefore, it can be argued that RICA, due to its ambiguity regarding the metadata collection, is unable to sufficiently

protect the individual's privacy within the digital age. Mutung'u (2021:181) states that the above results from "the judicial authorisation being cloaked in secrecy, denying the protection of those rights under surveillance". It also indicates that mass surveillance does not adhere to the necessity principle[11], which only limits the individual's right to privacy in serious circumstances. Although RICA was implemented to balance civil liberties such as privacy, justice, and national security, it has largely been unsuccessful in providing proper basic international human protections (Right2Know 2016).

As Snowden has shown though his exposé of the NSA surveillance, the lack of accountability leads to abuses. The evidence in South Africa indicates a high rate of under-regulated mass surveillance. The interceptions do not necessitate a warrant, and the Act has no founding statute. Duncan (2018:13) indicates that "it is operating on an entirely separate but parallel track to the targeted legal intervention process of RICA". The Regulation of Interception of Communications and Provisions of Related Information Act 70 of 2002 does not notify subjects that their communications have been intercepted. Right2Know (2016:23) has concluded that those who have had their communication intercepted are not made aware of this interception, even when a request has failed or after an enquiry has concluded. As RICA is the only legislation that explicitly addresses communication interceptions, any interception of communications that occurs outside the boundaries of RICA is considered unlawful; RICA criminalises this as an unlawful interception. The Acts mentioned earlier all improve surveillance within South Africa. This is especially true of RICA, the primary surveillance legislation governing surveillance. However, as discussed, many discrepancies exist within the Act as many violations of individuals' privacy occur. In order to improve personal information rights, the 2013 POPI Act was implemented.

4.3.2 Recent Legislation adopted in 2021

The Protection of Personal Information (POPI) Act 4 of 2013 offers the necessary "regulations and guidelines regarding collecting and processing personal information" (South Africa 2013). It came into effect on 1 July 2020 but was given a 12-month grace

[11] The limitation of a fundamental right such as personal data protection must occur if strictly necessary. Necessity will be accepted based on objective evidence to assess the proportionality of limitation.

period which ended in June 2021 (Bhagattjee 2021). The POPI Act is now entirely in effect and consists of eight principles; namely:

- The collection of personal information must be fair and lawful towards the subject.
- The collected information can only be used with the subject's consent and for the intended purpose. There is a limitation of processing; processing more information than approved data is not allowed. The party in charge of collecting information must guarantee that it is not misleading, of quality, accurate and complete. While the processing of information ought to occur transparently, both the Information Regulator and the data subject should agree and be aware of the data collection. Moreover, the party that is in charge of the collection of information must implement security measures. These measures must prevent the "loss, destruction, damage, and the unauthorised access or processing of the data", therefore information technology asset disposition (ITAD). It refers to the "practice of how and where to dispose of IT hardware". It includes, "upgrading, or otherwise getting rid of computer equipment" and assists in the disposal needs of organisations (Horizon 2021). Information technology asset disposition should be embraced to safeguard the organisation's information technology assets which will avert the exposure and breach of personal information. This will result in complying with the regulations. The data subject should participate by accessing the stored data and correcting information if necessary (Bhagattjee 2021).
- Lastly, the party responsible for processing the personal information should implement measures that guarantee that their activities comply with the POPIA principles (Desmond 2021).

The POPI Act is a significant shift for data protection in South Africa; unlike RICA, the POPI Act provides fines and punishments when one fails to comply with the Act, which will be considered an offence. Failing to comply is not the only way to violate the law; interfering or "hindering, influencing or obstructing" with the Regulator is regarded as an offence, including lying under oath and failing to attend hearings. Chapters 10 and 11 of the POPI Act discuss the enforcement of punishments and consequences of not complying with the POPI Act. Non-compliance is considered interfering with

safeguarding the personal information of a data subject. The POPI Act provides penalties when a violation occurs; this includes receiving a fine or imprisonment (or both). Fines can be set by the regulator and should not exceed R10 million, while prison time can be set at ten years or up to 12 months, depending on the sections that have been violated. Therefore, these checks and balances safeguard privacy protection; however, because the POPI Act has recently been implemented, the effectiveness still needs to be evaluated (Olsen 2022). Despite legislation which governs surveillance in South African, violations of privacy continue to occur. The POPI Act represented a new dimension of regulating privacy interferences; however, it has only recently come into effect, and thus its effectiveness is yet to be examined. Nonetheless, even with surveillance legislation in place, the violation of privacy continues to occur within South Africa.

4.4 SURVEILLANCE ABUSES IN SOUTH AFRICA

4.4.1 Misconduct of South African Intelligence Agencies

Project Avani is the 2005 revelation of misconduct within the South African intelligence services. It revealed that the agency acted outside its mandate, caused mainly by internal struggles of the leading party (the African National Congress) (Van Heerden 2019:6). It revealed that there were several instances where the intelligence services operated outside the boundaries of the Constitution, with 13 people's conversations being illegally intercepted through the mass interception capabilities of the National Communications Centre (NCC). It consisted of "ANC members, opposition party members, public officials and people in business". A formal investigation was launched after "Saki Macozoma, a member of the ANC's executive, lodged a complaint" to the former Minister of Intelligence, Ronnie Kasrils, to inspect communication interceptions by the NCC (Swart 2017a). This is attributed to the concept of national security not being clearly defined, which led to unscrupulous intelligence operatives understanding national security in a way which permitted them to act beyond the mandate. The Inspector-General of Intelligence Report (2006:18) claimed that Project Avani represented a moment where South Africa's young democracy could not allow instances for national security to be used as a justification for abuse and for the disregard of the Constitution. The Inspector General of Intelligence

Report (2006) was created by Mr Ronnie Kasrils and ran simultaneously with the Matthews Commission (2008:7) to improve the control mechanisms of civilian intelligence. The purpose was to align these control mechanisms with Constitution. The Commission's report (2008:48) confirmed the "supremacy of the Constitution and the rule of law". Therefore, the report argued against intelligence operatives acting outside the law and using illegitimate mechanisms such as intrusive means to infringe on the individuals' rights. The South African Law Reform Commission (2005) found that these methods were unconstitutional except where appropriate channels were used per the law of general application. The current legislation in South Africa permits the interception of communication by intelligence services for search and entry purposes. However, invasive measures such as infiltrating an organisation, implementing physical and electronic surveillance, or recruiting informants are not approved. According to Desai (2018), all of these are not regulated by legislation; thus, it is considered unconstitutional.

In 2010, the *Sunday Times* had investigated cases of government corruption. This resulted in the interception of the newspaper's communications to disrupt its investigation and reveal its sources. Police were able to acquire judicial approval to undertake the interception of journalists' mobile phone communications. The officers adopted fictional names to intercept communications under the false pretences that it was to investigate a criminal syndicate. As a result of this, the *Sunday Times* took the case to court. The result of the court case was that the "two officers were found guilty of violating RICA's requirements" (Privacy International & Right2Know & Association for Progressive Communications 2016:3).

Moreover, between 2008 and 2011, the parliamentary oversight committee reported an increase of 170 per cent in the number of warrants being issued for interception. Ultimately, the low threshold to justify surveillance (reasonable grounds) has created an environment plagued by with weak oversight; this has led to the abuse and violation of the right to privacy (Privacy International & Right2Know & Association for Progressive Communications 2016:2). Reports of unlawful surveillance continue to emerge. In 2013, the *Mail & Guardian* reported that the NCC has the "capacity for mass interception of communications and is carrying out mass interception of communications within South

Africa" (Privacy International & Right2Know & Association for Progressive Communications 2016:4). Moreover, the report highlighted that the agency could 'mass monitor telecommunications and conversations, including text messages, emails and data' (Privacy International & Right2Know & Association for Progressive Communications 2016:4). This occurred without the judicial authorisation to safeguard national security. Between 2008 and 2015, more than 315 were recorded, with 2015 accounting for 752 of those interceptions; this indicated that interceptions had only increased. Duncan (2018) attributes the increase in interceptions to the 2014 inclusion of a "financial reporting centre in the RICA framework". In contrast to this, Klaaren (2015) states that it has been the result of the administration of the OIC, which is used as a framework to intercept ordinary crimes. Ultimately, the interceptions that the OIC reports compared to the orders issued by judges reveal that the scope of orders is way too broad and goes against the proportionality principle.

In 2017, the *Daily Maverick* investigated how law enforcement agencies in South Africa frequently used Chapter 3 of the Constitution section 205 and the Criminal Procedure Act 51 of 1977 which grants them access to call data information (Swart 2017b). Section 205 aids law enforcement to apply to high court judges, magistrates or regional courts to gain records, the investigation revealed that many law enforcement agencies took advantage of this. This is because RICA permits it under section 15 (Privacy International 2019). The Right 2 Know Campaign questioned this. As a result, the leading mobile providers within South Africa, namely Vodacom, Telkom, Cell C, and MTN made a shocking statement. It was revealed that they "collectively disclosed over 70 000 subscribers call records" when law enforcement requested them under section 205 (Swart 2017b). Ultimately, the intelligence services act beyond their mandate and communication interceptions occur without oversight or transparency of the reasons behind their actions; moreover, surveillance legislation is being misused, and intelligence agencies misuse their power which little regard for the individual's right to privacy.

4.4.2 The Politicisation of the South African Intelligence Services Post-1994

In 2018, the *Daily Maverick* published an article claiming that when Cyril Ramaphosa becomes President, he would inherit several headaches from former President Jacob

Zuma. “His to-do-list will have to include the country’s intelligence service, the State Security Agency (SSA). Not only has it become highly politicised during Zuma’s reign, but it has also declined in performance and, by implication, in usefulness” (Marais 2021:4). Thus, the Ramaphosa presidency had to face cleaning up the organisation and initiating a systematic refocusing exercise. As a result, in 2018, President Ramaphosa appointed a high-level review panel to the Security State Agency. By 2019, the panel accounted the problems in the SSA to the politicisation of the ANC. This was caused by the growing “contagion of the civilian intelligence community by the factionalism in the party”, which had been worsening since 2009 (Daniels 2019:8). In a doctrinal shift from 2009, the intelligence community shifted away from what is specified within the White Paper on Intelligence and the Constitution, which focused on human security. Instead, it moved back towards a narrow state focus.

The unification of the South African Secret Service and the National Intelligence Agency (NIA) failed to achieve its objectives and did not adhere to its existing policy. In addition, effective accountability is stifled by the high levels of secrecy in the SSA. Although, to a certain degree, specific matters are vital to be kept a secret, such as lawful investigations and the name of agents, in comparison to other democratic countries, the South African Intelligence community is much less transparent (Nathan 2017). Therefore, the lack of transparency results in high levels of secrecy, leading to the risk of an abuse of power and less public scrutiny. Lastly, Marais (2021:4) states that the abuse of resources within the SSA has allowed it to become a “cash cow” for those “inside and outside the agency”. Consequently, Nathan (2017) concludes that scandals regarding the use of unauthorised surveillance on businesspersons and politicians reflect an oversight gap within surveillance operations. It reveals that the agency is politicised, corrupt and has undoubtedly turned its back on the principles granted within the Constitution: the right to privacy. Furthermore, the Crime Intelligence Division (CID), which is a unit that falls under the SAPS, also faces allegations of abusing power. The CID controls intelligence gathering with regard to criminal activity and supports police investigations to ensure practical crime-fighting initiatives.

The CID also has the power to use surveillance to conduct “covert and undercover operations” (Privacy International 2019). Furthermore, it provides resources to monitor political activity and community organisations that are involved in protests. The unit has faced several corruption scandals and organisational instability. Since 2017, the watchdog known as the Independent Police Investigative Directorate launched several criminal prosecutions against former officials. These officials were accused of abusing state resources and being involved in corruption. This includes claims that the intelligence slush funds were used to “influence the elections for the party leadership of the African National Congress” (Benjamin 2015). Senior leadership has also faced severe criminal charges, with the former Criminal Intelligence head Mdluli being fired. Duncan (2021) claims that the CID is in disarray because it is unregulated. In his book *The Presidents Keepers*, journalist Jacques Pauw claims that Crime Intelligence has “little honour, no moral compass, [and] a complete lack of integrity” (Pauw 2017:338). Therefore, intelligence agencies within South Africa operate under a veil of secrecy which fosters corruption and the abuse of resources and power. This is why individuals fear that the powers of the state will be used against them. As a result, the social contract between the state and its citizens becomes weakened. Consequently, individuals choose to take the state to court when individual privacy is threatened.

4.4.3 AmaBhunghane Case (4 February 2021)

The AmaBhunghane case came about because of the discovery made by Stephen (Sam) Sole, an investigative journalist and executive director of the AmaBhunghane Centre for Investigative Journalism. Sole discovered that he was the subject of the state’s surveillance in accordance to RICA’s provisions. Initially, Sole suspected that his communications were being intercepted; therefore, Sole sent an information request to the Inspector-General of Intelligence. However, the Inspector- General declined the information request. He argued that there was no evidence to support that any wrongdoing had occurred and that, instead, everything adhered to the regulatory framework. However, seven years after this occurred, Sole’s conversation transcripts were annexed to a case that involved former President Jacob Zuma. It immediately highlighted the basis upon which an interception order was being held against the

journalist and the period of this interception (Mutung'u 2021:175). In response to this, Sole acquired another information request. The request revealed that a judge had "issued an interception warrant in 2007, which was renewed in 2008" (Hofmeyr 2021). Sole claimed in an interview with Privacy International that the main problem is getting behind the secrecy:

> The problem is to get behind the veil of secrecy. The courts are important in terms of gaining redress, but you can only go to Court if you know what has happened […] In terms of the current regime, you never know that you've been spied on, you never know that surveillance has taken place because it's kept secret (Privacy International 2021b).

As a result of this, Sole instituted a case to contest various parts of RICA; these include: "not notifying people that they are under surveillance; the manner in which RICA interceptions are stored and processed; the mandatory data retention of RICA; the lack of procedural justice concerning appointing the RICA judge; and lastly, no protection is provided for journalists and their sources" (Privacy Internationala 2021 & Mutung'u 2021:175). Thus, Sole accuses RICA of being unconstitutional as it does not provide the necessary safeguards which protect the right to privacy (Hofmeyr 2021).

In 2021, the Constitutional Court made a ruling with regard to: the "*AmaBhunghane Centre for Investigative Journalism NPC and Another v Minister of Justice and Others*'; and the '*Minister of Police v AmaBhunghane Centre for Investigative Journalism NPC and Others*". The consequence of the case is that RICA was found to be unconstitutional. It failed to provide obligatory safeguards to protect the individual's right to "privacy, freedom of expression, access to the courts, and legal privilege" (Hofmeyr 2021). Moreover, it made no provisions to notify subjects that they were under surveillance. It also gives members of the unregulated executive the discretion to renew the term of a selected judge, which brings the judge's independence into question.

The Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 lacks in providing measures to ensure the management and custody of information that is collected through surveillance. Furthermore, RICA cannot provide an adversarial process to ensure that a subject is

protected against state surveillance during the ex parte process. Lastly, no provisions are made in the case of exceptional circumstances, such as when lawyers or journalists are the subjects of surveillance (Hofmeyr 2021). Thus, before reaching its judgement, the Constitutional Court (CC) had to assess the abovementioned aspects to determine the constitutional validity of RICA. The CC kept the apartheid history of the country in mind. This history was plagued with the government invading the privacy of individuals through searches, seizures, and spy activities. It did so through several means and intercepting the communications of individuals.

In contrast, the CC emphasised that the key to the new South Africa is that the Constitution guarantees the individual's right to privacy. However, Section 14 of the Constitution, which has to do with surveillance and the interception of a person's communication under RICA, encroach on the right to privacy. Therefore, the CC had to consider if the limitation of this right was justifiable and reasonable and whether it contains the appropriate safeguards to lessen the risk of unnecessary intrusions. As a result, RICA was found to be unconstitutional because it does not provide the safeguards for an independent judicial authorisation of interception. The absence of safeguards which specifically deal with interception directions is attained and sought on an ex parte basis. There is a lack of appropriate measures to ensure that the obtainment of data through intercepting communications is managed in a lawful manner and not interfered with unlawfully. Bulk surveillance, on a legal basis, is required to be authorised on the basis of legislation; yet no other law authorises it. Therefore, the CC concluded that the bulk surveillance practices are "invalid and unlawful, as no law authorises it" (Hofmeyr 2021). The High Court gave parliament two years to correct the defects of RICA (Sonjica 2021); however, the Constitutional Court extended this by giving parliament three years to carry out this undertaking (Sarkar 2021). Until the review by parliament takes place, temporary provisions have been adopted; this "interim relief" has been given by the High Court and accepted by the CC. It should be applied to post-surveillance by notifying journalists and lawyers of surveillance. This will align RICA with the values of accountability and transparency stipulated in the Constitution (Nicholls 2021).

However, in the meantime, RICA continues to be used, and the privacy of the individual continues to be violated. This is because RICA is misused and goes beyond its scope of crime prevention (Luck 2014). The common law of South Africa distinguishes the right to confidentiality as an independent personality right. The courts have included this through the philosophy of *dignitas*. Cohen (2000:3) argues that confidentiality is acknowledged in the private sphere. However, the "scope of personal begins to shrink significantly when a person moves into communal activities and relations, such as social interaction and business". The Constitution relates privacy to dignity; however, RICA fails to uphold the human rights and freedoms granted within a democratic government. As mentioned above, South Africa relates its national security to human rights; however, this is contradictory as it uses the very notion of national security to violate the rights it seeks to protect. Moreover, because the South African intelligence agencies operate in secrecy due to a lack of transparency and a misuse of RICA, the individual's right to privacy continues to be violated. Despite this, South Africa continues to invest in mass surveillance initiatives.

4.4.4 Adoption of Biometric Technologies

At an ideological level, Feldstein (2019) claims that pro-surveillance development partners are the drivers of surveillance in South Africa. According to Bosch and Roberts (2021), collaborations with China and Russia within intelligence research have played a significant role in advancing domestic intelligence. This advancement was made through building intelligent cities with surveillance capabilities and social media surveillance. South Africa's collaboration is concerning because Russia uses surveillance to censor citizens and bring media under state control (Sherman 2022). Similarly, China has created an Orwellian high-tech surveillance state who censors the Internet to monitor and suppress public criticism (Human Rights Watch 2020b). Both countries are cases of the state using its power against citizens and breaking the social contract. Thus, South Africa working alongside countries is negligible and concerning when considering the social contract. Moreover, South Africa also produces surveillance technology and is considered the birthplace of VASTech, a surveillance technology business. Initially, South Africa was thought to fund the company; however, in 2011, the state implicated itself as it was

revealed that it had supplied the Libyan government with surveillance technology (McLaughlin 2016). In 2013, WikiLeaks exposed VASTech's brochures which endorsed three products: "the Zebra; the Badger; and the Satellite Signal Analyser". The brochures revealed that the Zebra could "monitor and record all voice emails, SMSes, MMSes and faxes on landline and mobile networks connected to it". The Zebra permits the analysis of information and the ability of law enforcement to "go back in time" and "identify targets and discern relationships which may have their origins years into the past" (McLaughlin 2016). The metadata of these communications is taken and reveals when the communication took place, the duration and the parties involved. This data is stored online for "extended periods", as the brochure does not indicate how long the data can be kept.

On the other hand, the Badger can monitor internet activity, namely "web-based email services and social media". The Satellite Signal Analyser and the Badger can "intercept, store and analyse satellite communications" (Swart 2015a). However, when asked to comment about its products, VASTech refused on the grounds of client confidentiality. The *Mail & Guardian* has claimed that the South African government continues to fund the company and is supporting a new software programme called "Next" (Swart 2015a). It is unclear how much the government has contributed to the programme or what it has been designed for, but it is clear that the links between the private sector and government run deep. Privacy International continues to press the South African government, who is well aware that the technology is being used for mass surveillance, to halt their funding of the company. However, the government continuously refuses to answer such questions (McLaughlin 2016).

More recently, the South African government has adopted biometric technologies for identification of citizens and to allow citizens access to government services, which can be seen through social welfare grants and the increased implementation of Closed-Circuit Television (CCTV) by the state and the private sector. Therefore, new technology has supported the government's ability to undertake surveillance. However, some argue that extensive mass surveillance tools like CCTV, biometric identification, and artificial intelligence are not always required. Also, it is not proportionate to the extent it is being

executed. Black Sash (2019) states that the South African Social Security Agency (SASSA) uses “fingertips, face photographs and biometrics” in identifying beneficiaries of social welfare. However, the distribution of social welfare is “outsourced to third-party businesses without indicating how the beneficiaries’ personal information will be used” (Black Sash 2019). Local governments widely use CCTV in big cities to mitigate crime. Although parts of privately owned CCTV are highlighted within the POPI Act, the Act does not address public surveillance.

While various cities are implementing facial recognition and verification technology, it is important to note that biometric technology is highly susceptible to function creep[12](Allen & Van Zyl 2020:1). In 2018, The City of Cape Town had “more than 1 500 CCTV cameras”, leading all other municipalities. Of these cameras, 626 were dedicated to detecting and preventing crime (Swart 2018). Drones were also acquired for this purpose. This was done assuming that the cameras would make the city safer. Nevertheless, Swart (2018) claims that indicators show that, in the long run, the “hidden costs of 24/7 mass surveillance outweigh the ability to improve our lives”. However, other municipalities within South Africa continue to spend millions of rand on crime prevention activities such as CCTVs. This is even though researchers at the South African Cities Network (SACN) question the effectiveness of such initiatives. Their research found that the maintenance cost of cameras cripples municipalities’ security and safety budgets and removes money from other safety and security initiatives. Not only is it ineffective, but the implementation of CCTVs also conflicts with the laws of the POPI Act. The South African Cities Network (SACN) states that:

> South Africans are trapped in a cycle of crime and violence, fear of crime, and profit-driven messaging that suggests that private security technologies centred on CCTV surveillance systems are essential to their safety and security while inadequate evidence supports this. On the contrary, despite the widespread use of CCTV, crime continues to climb steeply (BusinessTech 2022).

[12] Transpires when information is used for a different purpose than the original specified purpose.

The issue of who is given access to sensitive biometric data is another essential aspect to consider. This is important because if security agents can attain entry to data on centralised databases that do not require a judge to provide a reference, it can lead to challenges with communications-based technologies such as mobile phones, under RICA, judges are required to issue a warrant which was a point that the information regulator of South Africa raised.

The POPI Act includes data gained through facial recognition; nevertheless, CCTV surveillance demonstrates a blind spot to the regulations in place. Although CCTV regulations implement controls to determine the location of cameras when it involves vulnerable groups such as children, little consideration is given to balancing privacy and security (Nathan 2017:9). Also, researchers have found that there exists no link between existing laws which are entrusted to regulate surveillance. The POPI Act does not reference a CCTV code; no legal provisions are made to guarantee that a balance is reached between the necessity for CCTV camera surveillance and the right to privacy. Additionally, the POPI Act permanently excuses the act of surveillance based on national security and crime-fighting; this allows huge room for misuses. The installation of CCTV cameras in the country continues shortly after privacy assessments are completed beforehand; both the participation and opinion of the public are “allowed throughout the rollout of CCTV measures, and its purpose is to ensure the protection of the public” (Nathan 2017:10).

The National Coordinator of the Right to Know, Murray Hunter, has stated: “These capabilities violate ordinary people’s constitutional right to privacy. South Africa’s laws do not acknowledge the existence of the government’s mass surveillance capabilities”. The right to privacy is not protected against mass surveillance in South Africa. Hunter also claimed that “we can only hope that the spooks actually obey whatever rule book they have written for themselves on this” (Swart 2015a).

The past 20 years of investigations, leaks, and revelations point to the inability of the intelligence services to effectively transform themselves since the democratic transition took place in South Africa (Nathan 2017). This has allowed for comparisons of the intelligence agencies of the apartheid era and the new intelligence agencies. Nathan

(2017) argues that South Africa's current intelligence service shares many commonalities with its apartheid predecessors. There is a genuine concern that South Africa might drift into digital authoritarianism as the violation of privacy has become normalised. The fact that it is happening digitally has made it easier for government to get away with it. Some even compare the use of cameras as being the digital equivalent of the aforementioned internal passports or passbooks, which was implemented by the apartheid-era system (Hao & Swart 2022). Ultimately, technology promoting mass surveillance, such as the above-mentioned biometric technologies, has allowed unregulated surveillance by the South African government. This severely violates the individual's right to privacy. Furthermore, other technologies continue to enter the security market, such as "grabbers" and spyware, which can be used for mass surveillance purposes (discussed below).

4.4.5 The Use of IMSI catchers (Grabbers) and Spyware

Extensive evidence indicates that SAPS, along with other intelligence agencies, use IMSI (International Mobile Subscriber Identity-Catcher) catchers, also called "grabbers". This refers to a wide grouping of devices that "mimic a cell tower's operation to entice mobile phone users to surrender their identifiable data, like the SIM card number (IMSI)". Privacy International (2019) claims that in recent years the IMSI technology has evolved to be "highly sophisticated" and can "intercept voice, SMS and data" communications. Several media reports which have recorded on-and-off the record comments by police officers claim that South African state agencies buy and use such technology. The *Mail & Guardian* newspaper released an investigative report in 2015 which produced evidence of police using "grabbers". Likewise, an anonymously-sourced report in the Afrikaans newspaper *Rapport* in 2018 accused the Defence Intelligence Division of "procuring a mobile surveillance van from a Chinese supplier which allegedly included "grabber" technology" (Privacy International 2019). This goes again the stipulations of RICA, which forbids the private use, sale or ownership of such technology. However, it is unclear if authorities have been adhering to the legal process required by RICA, which is to "apply for judicial authorisation" when using 'grabbers' (Swart 2015b). The failure to get authorisation would make the use of this technology against the law; nonetheless, when the Right 2 Know Campaign tried to verify this through information requests, they were

denied (Memdutt 2019). Because “grabbers” can conduct surveillance not regulated by RICA or any other law, it is unclear how lawful the technology is. In 2015, the Joint Standing Committee stated they would “revisit RICA with a view of whether any changes would be required to strengthen the Act in the likely event that the Judge is not sufficiently empowered to deal with matters such as grabbers” (Privacy International 2019).

Furthermore, South Africa is also accused of using spyware for mass surveillance. Although unconfirmed, evidence suggests that the South African government has used spyware (Privacy International 2019). FinFisher is a known “trojan software” created by a British surveillance company called Gamma Group. It is sold by “FinFisher GmbH” in Germany (Marquis-Boire et al. 2013). The spyware can be installed on a device; it can record keystrokes and audio; it can take screenshots and various other invasive types of data collection (Vermeulen 2013). The spyware was first discovered in South Africa when Wikileaks recorded that representatives from the FinFisher visited the country between 2012 and 2013. In 2013, researchers from the Citizen Lab discovered the company’s presence on South African servers. Additionally, the investigative show *Carte Blanche* stated that in 2015 the “South African Revenue Service (SARS) could have used FinFisher for covert intelligence” (Vermeulen 2015). The absence of appropriate oversight mechanisms allows the government to implement surveillance measures which violate the individual’s right to privacy.

4.4.6 Parliamentary Oversight Failures

The Intelligence Services Act 65 of 2002, articulates that all “state security structures, along with their oversight bodies, are accountable to the Parliament’s Joint Standing Committee on Intelligence (JCSI)” (South Africa 2003). The committee is closed, and the members are subjected to strict security clearances. According to parliamentary rules, the committee functions behind closed doors by default. Therefore, before any documentation can be made public, the opening of meetings can only occur through a resolution by the JCSI; however, this rarely occurs (Privacy International 2019). The Matthews Commission and the Right 2 Know Campaign have called out the JSCI, arguing that the committee operates with a lack of transparency and avoids public participation. This is because it prevents the committee from being scrutinised by the public, which

leads to security structures being protected (Privacy International 2019). Therefore, the absence of proper oversight mechanisms results in governments using their power against citizens by limiting the rights of citizens, such as the right to privacy.

4.4.7 COVID-19 and the Right to Privacy

The rapid spread of COVID-19 [13] forced governments to implement initiatives usually reserved for natural disasters, wars or depressions. Thus, the pandemic caused a global upheaval, leading to governments taking 'extreme measures to limit the human cost and economic disruption' (Eggers et al. 2020). In 2020, the World Health Organization (2020) reported more than 3 million global deaths. In 2022, more than 6 million have been killed due to COVID-19 (Murphy & Wu 2022). Therefore, to address the threat of COVID-19, South Africa implemented geolocation data to mitigate the virus's spread. This was done for the purpose of contact tracing which was immediately met with resistance due to privacy concerns. Thus, the Department of Health was instructed to adopt contact tracing regulations in order to protect the privacy of individuals whose information would be part of the database for contact tracing. In order to oversee the contact tracing database, South Africa appointed a COVID-19 judge who was responsible for reporting on all actions taken during the period of contact tracing and the period after the pandemic. Thus, South Africa's first response to the pandemic was to increase government power by accessing citizens' data (Taylor et al. 2020:249). By March 2020, the beginning of the country's lockdown, the Minister of Communications and Digital Communications adopted certain "directions". These served as "instructions for mobile operators to provide mobile data as required by the public sector to manage COVID-19" (Taylor et al. 2020:250). However, this provided no limitations to data collection purposes, the accessibility of the data by the private sector and how data protection would be ensured. Ultimately, the directions went against what the Bill of Rights stipulated. However, they remained in place as a state of disaster was implemented instead of a state of emergency, which would have led to a complete suspension of citizens' rights (Taylor et al. 2020:250). The adoption of these regulations, which allowed telecommunications providers and

[13] COVID-19 is an acute respiratory illness in humans as a result of the coronavirus. It can result in severe symptoms, in some cases, death. The virus was identified in China in 2019 and was declared a global pandemic in early 2020.

health authorities to gain access to geolocation data for the purpose of contact tracing, caused huge concerns. Therefore, academics argued that the “rights of people [in the] midst of an epidemic must be considered in both the textual setting of the South African Constitution and their socioeconomic setting” (Pepper & Botes 2020). Human Rights Watch, along with 100 other human rights groups, has “urged governments to respect privacy and humans when using digital technologies to contain the pandemic” (Human Rights Watch 2020a). This led to the government amending the regulations through the Disaster Management Act 57 of 2002.

Notably, COVID-19 regulations were adopted in an incomplete data-protection landscape because, at the time, the POPI Act was not entirely in effect yet. The Information Regulator Pansy Tlakula stated: “Rights to privacy and access to information are at stake with contact tracing”. However, she supported its undertaking because it was deemed necessary to contain the spread of COVID-19. Nonetheless, the regulations adopted included a degree of privacy considerations when collecting data. It did so by ensuring that the parties responsible for the collection were held accountable, that the data collected was accurate and used only for a specific purpose. Also, the retention of data was to be limited to the state of disaster (Taylor et al. 2020:251).

The COVID-19 pandemic highlights the difficulty of weighing up when to justify moments of crisis as a reason to infringe on the civil liberties of citizens, especially the right to privacy. As noted, the social contract states that the government is entrusted to provide security; however, this does not mean that they should use that power and authority against citizens in an unfair or unjust way. Brinkley (2006:26) argues that those living through times of crisis should note “that civil liberties are not a gift from the state that the state can withdraw when they become inconvenient”. The individual’s right to privacy is fundamental as it also protects human dignity, which is understood as a multi-faceted concept that recognises that humans have intrinsic or inherent worthiness. Because of this, other humans and society should treat them with a degree of concern and respect. Therefore, to respect human beings, the right to privacy is granted; thus, violating this right denies the individual the space to establish their relationship with society and the state. For this reason, Mavedzenge (2020:19) states that the right to privacy is core to

"human beings' existence and human dignity". Therefore, a proportionated balance should be reached "between the state's duty to protect national security and the obligation of the state to respect the individual's privacy". Ultimately, notwithstanding the state's responsibility and efforts to defend national security, the right to privacy should not be "disproportionately restricted as the enjoyment of various other rights depends on it" (Mavedzenge 2020:20). Arguably, a society can only flourish and develop when the individuals who make up the society are allowed to prosper and develop; however, this can only happen when individuals are given the space or environment which enables them to develop their capabilities (Mavedzenge 2020:19). Therefore, the main objective of national security should be to create a safe environment where individuals are free to realise their human potential in order to benefit from their own personhood and society. In this sense, national security cannot be protected at the expense of privacy because it destroys the nation's ability to flourish and develop. Protecting privacy is just as crucial as protecting national security, as the main objective is to provide an environment where individuals can enjoy freedoms such as privacy and prosper within all spheres of life. Mavedzenge (2020:36) argues that the individual's right to privacy is a "precondition to the enjoyment of various other fundamental rights, such as preserving human dignity". Therefore, when individuals' privacy is eroded, they are deprived of other rights, such as dignity, which defeats the goal of national security. South Africa's Constitution links privacy to human dignity; however, privacy violations continue to occur. Thus, this section highlighted the problematic nature of trading off privacy in the name of security, as the individual's right to privacy is just as important as security.

4.5 CONCLUSION

This chapter has shown that mass surveillance has been vital in promoting South Africa's national security. After 1994, South Africa was able to change its approach to national security from a state-centric approach to a human-focused approach. This created the expectation that it would prioritise the individual's right to privacy; however, the above-mentioned surveillance legislation highlights various cases of abuse with regard to surveillance. These include unregulated surveillance and the abuse of power by surveillance agencies due to a lack of transparency and oversight. This has undoubtedly

fostered an environment whereby the social contract theory between citizens and the state has weakened. South Africa has continuously violated the constitutionally granted right to privacy which forms part of its national security and has a human security focus. Therefore, the irony is that although the country's national security discourse has experienced a unique transformation, it fails to adhere to and uphold the changes it has implemented since 1994. Thus, in order to address this failure, several mechanisms will have to be implemented. Ultimately, South Africa links its national security to human security. However, its primarily been focused on ensuring the state's security which has caused insecurity for the individual by eroding the individual's right to privacy by adopting mass surveillance practices which only benefit the state. This allows the relationship between national security and privacy within South Africa between 1994 and 2021 to be characterised as contradictory and complex. Therefore, the last chapter will discuss recommendations to safeguard individuals' privacy while ensuring national security.

CHAPTER 5: CONCLUSION

5.1 INTRODUCTION

This research investigated mass surveillance's role in creating tension between national security and the individual's privacy, mainly how this occurs within South Africa. It focused on the relationship between the state and citizens, specifically the responsibility a state has to provide national security but also to uphold the individual's right to privacy. The final chapter evaluates and summarises the data deliberated in the preceding chapters. The chapter concludes by stressing the importance of research with regard to mass surveillance and its impact on national security and privacy within the South African context in the digital age. It also provides recommendations for policymaking.

5.2 RELEVANCE AND STRUCTURE OF THE STUDY

The research problem that this study addressed was the relationship between national security and privacy (using South Africa as the case study). The problem that arose was that too much security enforced by the state results in the insecurity of the individual. This is due to the said security measures violating the individual's right to privacy. However, too much privacy can lead to potential insecurity in the state (mainly when individual actions result in actual threats to the state). This is a problem because the state is obligated to ensure national security. Therefore, this has led to various questions. When, if ever, do national security priorities trump the rights of the individual and, if so, in what circumstances is it acceptable? Why is the trade-off between national security and privacy so problematic? Lastly, what necessary safeguards and accountability mechanisms can be adopted to balance national security and privacy in South Africa? Thus, the main research question that the study asked was how the relationship between national security and the individual's privacy in South Africa between 1994 and 2021 could be characterised? Furthermore, the study aimed to critically determine how mass surveillance has evolved into a tool of national security in South Africa and how it affected the individual's right to privacy. Moreover, the role that technology played in creating tension between national security and individual privacy in South Africa was scrutinised.

The relevance of this study is that as technology evolves, the relationship between privacy and national security becomes more complex. This is because privacy causes the insecurity of the state and the imposing of national security initiatives results in the insecurity of the individual's privacy. The main challenge facing South Africa as constitutional democracy is that the country's definition of national security as human security has allowed for the securitisation of mass surveillance. This has, in turn, violated the individual's right to privacy. Thus, this study intended to increase the knowledge and understanding regarding mass surveillance and how it adds to the complex relationship between national security and the individual's right to privacy. This is an under-researched aspect within South Africa. In order to achieve this, the study followed this structure:

Chapter 1 introduced the research and how the study would be conducted. The research theme was highlighted to specify and outline the study. The theoretical framework was briefly addressed, forming the study's foundation. It presented an overview of the literature addressing national security, privacy and mass surveillance concepts. It defined the research problem by analysing the complex relationship between privacy and national security in order to investigate the extent to which mass surveillance creates tension between these two concepts. The chapter also described the research design and methodology that the study will use and the structure of the chapters.

Chapter 2 introduced the theoretical framework intended to understand the research. The social contract was used to understand and explain the relationship between the state and citizens. The chapter then analysed the various interpretations of the social contract theory by Thomas Hobbes, John Locke, Jean-Jacques Rousseau, and John Rawls. The chapter evaluated what would threaten the relationship between the state and citizens. Moreover, the chapter's theoretical understandings established that violating individuals' privacy to preserve national security threatens the relationship between the state and citizens.

Chapter 3 examined the development of mass surveillance as a tool used to provide national security. It also explored justifications for using mass surveillance for national security. The chapter furthermore highlighted privacy concerns regarding mass

surveillance to ensure national security. It showed how mass surveillance had become a tool to provide national security within the world. The arguments presented in this chapter highlighted how technology has created tension between national security and privacy. It did so by providing arguments that support the use of mass surveillance to protect national security and the arguments which claim that this results in the violation of the individual's right to privacy. Ultimately, the complex relationship between national security and privacy has weakened the social contract between government and citizens.

Chapter 4 provided a comprehensive discussion on the security transformation within South Africa. It also analysed how the concept of national security evolved towards a human-centric focus in South Africa as it adopted a human security focus with regard to national security. Furthermore, it considered the surveillance legislation within the country that is responsible for the protection of privacy. Lastly, it evaluated the effectiveness of this legislation and how it fails to protect the individual's privacy. Chapter 4 characterised the relationship between national security and privacy in South Africa between 1994 and 2021 as contradictory and complex. It discussed how South Africa had used mass surveillance mechanisms to provide national security. Although the country transformed its security environment to adopt a human-security focus, the tension between national security and privacy remains high. The various initiatives that were undertaken to ensure the individual's privacy has been unsuccessful as privacy violations continue. Although the country faces several security threats, this does not permit the violation of individuals' privacy. Therefore, although South Africa linked its national security to human security, its main focus is ensuring the security of the state, which has caused the insecurity of the individual by implementing mass surveillance methods which continuously violate the individual's right to privacy. This allows one to characterise the relationship between national security and privacy within South Africa between 1994 and 2021 as contradictory and complex. Because South Africa continues to trade-off between privacy and national security, which is problematic as it occurs without the necessary oversight, transparency and adherence to the law. This undoubtedly weakens the social contract between citizens and the government. This is because the South African government uses the power of the state against citizens.

Chapter 5 summarised and highlighted the main findings of the research. It also discussed the structure and relevance of the study. This chapter also presents several recommendations and highlights areas for further study. The purpose is to address what safeguards can be implemented to balance national security and the individual's right to privacy.

5.3 FINDINGS AND RECOMMENDATIONS

South Africa prioritises its primary role as ensuring national security, while civil liberties also play a vital part in South Africa's democracy. This is per the constitution, which relates national security to the rights and liberties granted to citizens. Although this is clearly articulated, national security concerns have taken priority over other state objectives. This is evident in the country's use of mass surveillance to address such threats. The rise and evolvement in technology have allowed the use of mass surveillance to an imaginable extent. It has placed the individual's right to privacy on the back burner.

As the threats to national security continue to evolve, states must keep up with the changing security environment to combat threats. South Africa links its security to its domestic and regional environment; thus, the threats it faces, such as terrorism, have prompted it to adopt surveillance measures to ensure the nation's protection and well-being. Legislation has been adopted to undertake measures which allow mass surveillance for national security. However, these methods have resulted in the violation of privacy due to the unlawful interception of communications, unregulated surveillance, intelligence agencies lacking transparency and effective oversight mechanisms, and the abuse of power. The surveillance legislation implemented in South Africa fails to regulate unlawful surveillance; it operates in an environment plagued with corruption and the abuse of power, which has led to failure in preserving the constitutionally given right to privacy. Therefore, the relationship between national security and privacy can be characterised as complex. Although the country has linked its national security to human security, it continues to violate the individual citizen's right to privacy, which fosters a lack of trust in the government; this essentially threatens the state's social contract with its citizens.

Notwithstanding, this study concludes that surveillance laws that effectively protect privacy are necessary for South Africa. Furthermore, it finds that national security concerns require surveillance by the government to deal with threats effectively; however, transparency will be vital to ensuring that the government does not abuse this power. The lack of specific privacy laws results in ineffective surveillance legislation. Coupled with this is the lack of presence of an appropriate framework which serves as an oversight mechanism that clearly defines unlawful violations of privacy and how intelligence agencies should use the premise of national security. This will only result in more privacy issues. Moreover, when mass surveillance is used, the scale of surveillance should be proportionate to what is needed, especially in the case of CCTVs as mentioned in Chapter 4. The City of Cape Town is implementing cameras which are costing the government millions. Furthermore, adopting and implementing 'grabbers', CCTVs and spyware indicate that surveillance laws in South Africa should be reassessed as RICA is unlawful and the POPI Act does not regulate CCTVs. This highlights gaps within South Africa's surveillance legislation which should be addressed.

Activities that pertain to individual privacy require the public's input to be monitored and scrutinised; therefore, it is vital to involve citizens in the process of developing surveillance laws. This will create a better relationship between the government and citizens. Therefore, citizens should play a part in the policymaking process regarding surveillance as it impacts them directly; this will strengthen the social contract between the government and citizens. Also it will prevent the government from abusing their power. Notably, the role of government to protect national security should not be underplayed. This is because threats of terrorism should never be disregarded. Also it should not be concluded that these threats would never occur. In these circumstances, it is clear that the government has to adopt intrusive measures, such as limiting privacy, to address such issues. Therefore, in order to ensure the government does not abuse this power, proper checks and balances should be implemented within government structures and agencies. This is to ensure that when intrusive activities are adopted, they are adopted in a transparent manner. The purpose is to lessen abusive practices and the infringement on liberties such as the right to privacy. Thus, the critical issue is implementing checks and balances with regard to how individuals' information is gathered through mass

surveillance. The main concern should be about what happens once the information is processed. This is because citizens fear that the state will use this power to gather information against them. As a result, surveillance laws should be created to ensure that suitable checks and balances are implemented in order to avoid the abuse of information due to mass surveillance. An all-inclusive approach should be adopted to develop an appropriate framework. All relevant role players, namely government, citizens, and civil society, should be consulted.

5.4 AREAS FOR FURTHER RESEARCH

This study has shown how mass surveillance has significantly impacted the complex relationship between national security and privacy; thus, the use of mass surveillance for national security purposes unavoidably impacts individual citizens' right to privacy. Therefore, other areas within this topic need to be researched further. These include the following aspects:

- A comprehensive study must be made of citizens' perception of mass surveillance and its impact on their privacy.
- Mechanisms must be introduced to improve transparency when mass surveillance is implemented and minimises the individual's right to privacy.
- An integrated surveillance approach must be implemented between state intelligence agencies.
- The gaps within surveillance legislation must be reviewed.

In summary, the primary principle governing national security in South Africa is that it should reflect the resolve of citizens to be free from fear and want. Also, it should contribute to citizens' quest to seek a better life. This highlights a human security focus. Finally, this study sought to contribute to the body of knowledge regarding the complex relationship between national security and privacy. It also highlighted how mass surveillance creates tension between the two, especially in the case of South Africa. This objective was accomplished by using the social contract theory and analysing the relationship between mass surveillance, national security, and privacy.

BIBLIOGRAPHY

PRIMARY SOURCES

African National Congress. 1955. *Freedom Charter.*

Cwele, S.C. 2010. Budget vote speech delivered to the National Assembly, Cape Town, 05 May.

South African Law Reform Commission. 2005. Privacy and Data Protection, Pretoria.

South African Police Service (SAPS). 2003. *South African Police Service Annual Report 2002/2003,* Pretoria: Government Printer.

South African Police Service (SAPS). 2007. *South African Police Service Annual Report 2006/2007,* Pretoria: Government Printer.

South African Police Service (SAPS). 2009. *South African Police Service Annual Report 2008/2009,* Pretoria: Government Printer.

South Africa, Republic of.1992. Interception and Monitoring Prohibition Act 127 of 1992. Pretoria: Government Printers.

South Africa, Republic of. 1995. *The White Paper on Intelligence*. Pretoria: Government Printers.

South Africa, Republic of. 1996. *The White Paper on Defence*. Pretoria: Government Printers.

South Africa, Republic of. 1996. *Constitution of South Africa*. Pretoria: Government of South Africa.

South Africa, Republic of. 2000. *Promotion of Access to Information Act 2 of 2002*. Pretoria: Government Printers.

South Africa, Republic of. 2001. *Financial Intelligence Centre Act 38 of 2001.* Cape Town: Government Printers.

South Africa, Republic of. 2001. *Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.* Cape Town: Government Printers.

South Africa, Republic of. 2003. *Intelligence Services Act 65 of 2002,* Pretoria: Government Printers.

South Africa, Republic of.2012. *South African Defence Review*. Pretoria: Government Printers.

South Africa, Republic of.2012. *Protection of Personal Information Act 4 of 2013*. Cape Town: Government Printers.

South Africa, Republic of. 2015. *The South African Defence Review,* Pretoria: Government Printers.

SECONDARY SOURCES

Acton Institute. 2022. Lord Acton Quote Archive. *Acton Institute.* Internet: https://www.acton.org/research/lord-acton-quote-archive. Accessed 24 July 2022.

Africa, S. & Kwadjo, J. 2009. Changing Intelligence Demand in Africa. African Security Sector Network & Global Facilitation Network for Security Sector Reform. Centre for Contemporary Cultural Studies.

Africa, S. 2022. South Africa's deadly July 2021 riots may recur if there's no change. *The Conversation*. Internet*:* https://theconversation.com/south-africas-deadly-july-2021-riots-may-recur-if-theres-no-change-186397. Accessed 4 September 2022.

Allan, H. 2022. What the History of the word "insurrection" says about Jan 6. *Time.* Internet: https://time.com/6137604/history-insurrection-jan-6/. Accessed 4 September 2022.

Allen, K. & van Zyl, I. 2020. *Who's watching who? Biometric surveillance in Kenya and South Africa,* ENACT.

Al-Rodhan, N. 2018. The Social Contract 2.0: Big Data and the Need to Guarntee Privacy and Civil Liberties. *Openmind BBVA*.Internet:https://www.bbvaopenmind.com/en/humanities/beliefs/the-social-contract-2-0-big-data-and-the-need-to-guarantee-privacy-and-civil-liberties/. Accessed 20 July 2022.

Amiradakis, M. J. 2016. Social networking services: A digital extension of the surveillance state? *South African Journal of Philosophy*, 35(3):281-292.

Amit, M, Kimhi, H., Bader, T., Chen , J., Glassberg, E. & Benov, A.. 2020. Mass-surveillance technologies to fight coronavirus spread: the case of Israel. *Nature Medicine,* 26:1160–1169.

Amnesty International. 2020. COVID-19, surveillance and the threat to your rights. *Amnesty*.Internet: https://www.amnesty.org/en/latest/news/2020/04/covid-19-surveillance-threat-to-your-rights/. Accessed 4 September 2022.

Aondohemba, S. & Shaapera. 2015. Evaluating the social contract theoretical ideas of Jean Jacques Roussea: An analytical perspective on the state and the relevance to contemporary society. *African Journal of Political Science and International Relations,* 9(2):36-41.

Arinze, A. I. 1995. Human Development Report 1994 by the United Nations Development Programme (UNDP), New York. *CBN Economic and Financial Review,* 33(1): 84-89.

Arun, C. 2014. Paper-Thin Safeguards and Mass Surveillance in India. *National Law School of India Review*, 26(2):105-114.

Bambauer, D. E. 2013. Privacy Versus Security. *The Journal of Criminal Law and Criminology*. 103(3):667-685.

Barrie, G. 2013. The application of the doctrine of proportionality in South African courts. *Southern African Public Law,* 28(1): 40-57.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D. & Walker, R.B.J. 2014. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology*, 8:121-144.

Bajpai, K. 2000. *Human Security: Concept and Measurement,* New Delhi: Jawaharlal Nehru University.

Benjamin, C. 2012. Mdluli's tangled web. *Corruption Watch.* Internet:. https://www.corruptionwatch.org.za/mdlulis-tangled-web/. Accessed 20 August 2022.

Bernal, P. 2016. Data gathering, Surveillance and Human Rights: Recasting the Debate. *Journal of Cyber Policy,* 1(2):243-264.

Bester, P. C. 2019. *Emerging challenges in terrorism and counterterrorism: A national security perspective*, The Hague: The Hague University of Applied Sciences, Faculty of Public Management, Law and Safety.

Bhagattjee, P. 2021. South Africa - Data Protection Overview. *Data Guidance.* Internet: https://www.dataguidance.com/notes/south-africa-data-protection-overview. Accessed 13 May 2022.

Bigo, D., Hernanz, N., Jeandesboz, J., Carrera, S., Ragazzi, F., Parkin, J., Scherrer, A. 2013. *National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law,* European Parliament.

Black Slash. 2019. *Black Sash Submission UN General Assembly on Digital Technology, Social Protection and Human Rights,* Black Sash.

Bosch, T. & Roberts, T. 2021. *Digital Rights in Closing Civic Space: Lessons from Ten African Countries,* Brighton: Institute for Development Studies.

Boucher, D. & Kelly, P. 1994. *The Social Contract from Hobbes to Rawls.* London: Routledge.

Bowan, N. 2020. After 7-year wait, South Africa's Data Protection Act enters into force. *IAPP.* Internet:https://iapp.org/news/a/after-a-7-year-wait-south-africas-data-protection-act-enters-into-force/. Accessed 14 May 2022.

Brinkley, A. 2006. *Civil Liberties in Times of Crisis,* New York : Bulletin of the American Academy.

Burchell, J. 2009. The Legal Protection of Privacy in South Africa: A Transplantable Hybrid. *Electronic Journal of Comparative Law,* 13(1):1-26.

BusinessTech. 2022. Cities in South Africa are blowing millions on surveillance networks – but are they even working? *BusinessTech.* Internet: https://businesstech.co.za/news/government/602948/cities-in-south-africa-are-blowing-millions-on-surveillance-networks-but-are-they-even-working/. Accessed 4 August 2022.

Bryman, A. 2012. *Social Research Methods.* Fourth edition. Oxford: Oxford University Press.

Burchell, J. 2009. The Legal Protection of Privacy in South Africa: A Transplantable Hybrid. *Electronic Journal of Comparative Law*, 13(1):1-26.

Buzan, B. 1991. *People, States and Fear: An Agenda For International Security Studies in the Post-Cold War Era.* Warwick: Harvester Press Group.

Caluya, G. 2010. "The post-panoptic society? Reassessing Foucault in surveillance studies." *Social Identities*, 16(5): 621–633.

Campbell, J. 2014. South Africa: What Does "Service Delivery" Really Mean?. *Council on Foreign Relations.* Internet:https://www.cfr.org/blog/south-africa-what-does-service-delivery-really-mean. Accessed 4 September 2022.

Cawthra, G. 2013. *National Security and The Right to Information: The Case of South Africa,* Southern African Consultative Conference on National Security and Right to Information Principles, University of the Witwatersrand.

Cavelty, M. D. & Leese, M. 2018. Politicising Security at the Boundaries: Privacy in Surveillance and Cybersecurity. *European Review of International Studies*, 5(3):49–69.

Cayford, M. & Pieters, W. 2018. The effectiveness of surveillance technology: What intelligence officials are saying. *The Information Society*, 34(2): 88-103.

Cele, S. & Wilson, L. 2021. South Africa Economy Set to Take $3.4 Billion Hit From Riots. *Bloomberg.* Internet: https://www.bloomberg.com/news/articles/2021-07-20/south-african-economy-set-to-take-3-4-billion-hit-from-riots. Accessed 26 July 2022.

Centre for the Study of Violence and Reconciliation. 2007. *The Violent Nature of Crime in South Africa: A concept paper for the Justice, Crime Prevention and Security Cluster,* Johannesburg: Commissioned by the Department for Safety and Security

Clarke, R. A. & Knake, R. K. 2010. *Cyber War: The Next Threat to National Security and What to do About it*. New York: HarperCollins Publishers.

Cock, J. & Mckenzie, P. 1998. The 1996 Defence White Paper: An Agenda for State Demilitarisation?. In: *From Defence to Development: Redirecting Military Resources in South Africa.* Cape Town: David Philip Publishers: 41-60.

Cohen, T. 2000. 'But for the Nicety of Knocking and Requesting a Right of Entry': Surveillance Law and Privacy. *The Southern African Journal of Information and Communication*, 1:1-18.

Conway, M., Macdonald, S., Jarvis, L., Lehane, O. & Nouri, L. 2017. *Terrorist's Use of the Internet: Assessment and Response.* Amsterdam: IOS Press BV.

Cruywagen, V., 2022. Richard Mdluli, former Crime Intelligence boss, forces another delay over legal costs in corruption case. *Daily Maverick.* Internet: https://www.dailymaverick.co.za/article/2022-04-20-richard-mdluli-former-crime-intelligence-boss-forces-another-delay-over-legal-costs-in-corruption-case/. Accessed 20 August 2022.

Currie, I. 2008. The concept of privacy in the South African constitution: reprise*. Journal of South African Law*, 3: 549-557.

Daniels, P. 2019. *National Security Strategy Development: South African Case Study*. s.l: African Centre for Strategic Studies.

Davis, R. N. 2003. Striking the Balance: National Security vs Civil Liberties. *Brooklyn International Journal of Law,* 29(1):175-234.

Defence Web. 2019. RICA unconstitutional and invalid. Defence Web. Internet: https://www.defenceweb.co.za/security/civil-security/rica-unconstitutional-and-invalid/.Accessed 4 June 2022.

Desai, A. 2018. Cybercrime, Cyber surveillance and State Surveillance in South Africa. *Acta Criminologica: Southern African Journal of Criminology*, 31(3):150-160.

Desmond, P. 2021. South Africa: Constitutional Court upholds declaration of invalidity of RICA. *De Rebus.* Internet: https://www.derebus.org.za/data-privacy-laws-in-south-africa/. Accessed 17 May 2022.

Duncan, J. 2018. *Stopping the Spies: Constructing and resisting the surveillance state in South Africa.* Johannesburg: Wits University Press.

Duncan, J. 2021. Why SAPS Crime Intelligence is a hot mess. *Daily Maverick.* Internet:https://www.dailymaverick.co.za/article/2021-02-01-why-saps-crime-intelligence-is-a-hot-mess/. Accessed 20 August 2022.

Dworkin, A. 2015. *Surveillance, Privacy, And Security: Europe's Confused Response To Snowden,* European Council on Foreign Relations.

Eggers, W. D., O'Leary, J. & Chew, B. 2020. Governments' response to COVID-19: From pandemic crisis to a better future. *Deloitte.*Internet: https://www2.deloitte.com/us/en/insights/economy/covid-19/governments-respond-to-covid-19.html. Accessed 4 September 2022.

Ergun, D. 2018. *National Security vs. Online Rights and Freedoms in Turkey: Moving Beyond the Dichotomy,* Centre for Economics and Foreign Policy Studies.

Etzioni, A. 2014. NSA: National Security vs. Individual Rights. *Intelligence and National Security,* 30(1): 1-35.

Feldstein, S. 2019. The Global Expansion of AI Surveillance, Washington: Carnegie Endowment for International Peace.

Finkelstein, E. A. et al. 2017. Tradeoffs Between Civil Liberties and National Security: A Discrete Choice Experiment. *Contemporary Economic Policy,* 35(2): 292–311.

Fjäder, C. 2014. The nation-state, national security and resilience in the age of globalization. *Resilience*, 2 (2): 114-129.

Foucault, M. 1977. *Discipline and punish: the birth of the prison, trans*. Alan Sheridan. Harmondsworth: Penguin.

Galantonu, D. 2016. The Big Brother Fear: Four Perspectives on Surveillance. *American Intelligence Journal,* 33(1):59-64.

Gellman, B. & Adler-Bell, S., 2017. The Disparate Impact of Surveillance.*The Century Foundation.* Internet:https://tcf.org/content/report/disparate-impact-surveillance/?session=1. Accessed 10 November 2022.

George, F. C. 2014. Civil Liberties vs National Security: The Enduring Tension. *Notre Dame Journal of Law*, Ethics & Public Policy, 19(8):219-232.

Givetash, L. 2022. South African Police Arrest 20 People for Instigating July 2021 Riots. *VOA.* Internet: https://www.voanews.com/a/south-african-police-arrest-20-people-for-instigating-july-2021-riots-/6698903.html. Accessed 4 August 2022.

Goitein, E. & Patel, F. 2020. *A Presidential Agenda for Liberty and National Security*, New York: Brennan Center for Justice.

Goldman, E. O. 2001. New Threats, New Identities and New Ways of War: The Sources of Change in National Security Doctrine. *Journal of Strategic Studies*, 24 (2): 43-76.

Goold, B. J. & Neyland, D. 2009. *New Directions in Surveillance and Privacy.* Portland: Willian Publishing.

Gürses, S., Kundnani, A. & Van Hoboken, J. 2016. Crypto and empire: the contradictions of counter-surveillance advocacy. *Media, Culture and Society,* 38(4):576-590.

Hagen, J. & Lysne, O. 2016. Protecting the digitised society—the challenge of balancing surveillance and privacy. *The Cyber Defense Review,* 1(1): 75-90.

Hammond-Errey, M. 2022. *Big data and national security: A guide for Australian policymakers*: Lowy Institute for International Policy.

Hampton, J. 1980. Contracts and Choices: Does Rawls Have a Social Contract Theory? *The Journal of Philosophy,* 77(6):315-338.

Hao, K. & Swart, H. 2022. South Africa's private surveillance machine is fueling a digital apartheid: As firms have dumped their AI technologies into the country, it's created a blueprint for how to surveil citizens and serves as a warning to the world. *MIT Technology Review.* Internet: https://www.technologyreview.com/2022/04/19/1049996/south-africa-ai-surveillance-digital-apartheid/. Accessed 14 May 2022.

Harrisburg, K. 2021. Africa urged to wake up to growing state surveillance threat. *Reuters.* Internet: https://www.reuters.com/article/us-africa-privacy-lawmaking-idUSKBN2HB1J6. Accessed 17 May 2022.

Hlase, E. P. 2018. *The Securitisation of Cyberspace in South Africa: The Tension between National Security and Civil Liberties,* Pretoria: Department of Political Sciences University of Pretoria.

Hobbes, T. 1651. *Leviathan* London: Penguin.

Hofmeyr, A., 2021. An end to secret state surveillance under RICA. *Dispute Resolution.* Internet:https://www.cliffedekkerhofmeyr.com/en/news/publications/2021/Dispute/Dispute-Resolution-Alert-16-February-2021-An-end-to-secret-state-surveillance-under-RICA.html#:~:text=The%20CC%20agreed%20on%20this,confirmed%2C%20as%20set%20out%20above.Accessed 13 November 2022.

Horizon. 2021. A Guide To IT Asset Disposition: What Is ITAD?. *Horizon Technology.* Internet: https://horizontechnology.com/news/a-guide-to-it-asset-disposition-what-is-itad/. Accessed 4 September 2022.

Hosein, G. & Altshuller, . M. 2017. Privacy And Security In A Digital Age: An Interview With Dr. Gus Hosein. *Harvard International Review,* 38(3):67-71.

Huiskes, K. 2021. Remembering September 11: The September 11 Terrorist Attacks, the day that defined the beginning of the 21st Century for Americans. *Miller Center.* Internet: https://millercenter.org/remembering-september-11/september-11-terrorist-attacks.Accessed 4 August 2022.

Human Rights Watch. 2020a. Mobile Location Data and Covid-19: Q&A. *Human Rights Watch.* Internet: https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa. Accessed 4 September 2022.

Human Rights Watch. 2020b. China's Global Threat to Human Rights.*Human Rights Watch Organisation.* Internet: https://www.hrw.org/world-report/2020/country-chapters/global.Accessed 14 November 2022.

Hunter, M. 2019. Op-ed: Surveillance stats reveal spooks' cell phone bonanza. *Right 2 Know Campaign.* Internet: https://www.r2k.org.za/2017/09/21/op-ed-surveillance-stats-reveal-spooks-cell-phone-bonanza/. Accessed 4 September 2022.

Institute for Economics and Peace. 2009. *Global Peace Index: 2009 Methodology, Results & Findings,* Sydney: Institute for Economics and Peace.

Iranddoost, D. H. 2018. *Cybersecurity: A National Security Issue?,* E-International Relations.

Jones, J. 2009. The Birth of Big Brother: Privacy Rights in a Post-9/11 World. *Politics, Bureaucracy and Justice,* 1(1):17-21.

Klaaren, J. 2015. *Three National Security Legislative Regimes in South Africa,* Internet*:* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2866912. Accessed 22 May 2020.

Kleinig, J., Miller, S., Mameli, P., Salane, D. & Schwartz, D. 2011. The Underlying Values and their Alignment. In: *Security and Privacy.* ANU Press:151-223.

Krause, K. & Williams, M. C. 1996. Broadening the Agenda of Security Studies: Politics and Methods. *International Studies Review*, 40 (2): 229-254.

Kumar, R., 2011. *Research Methodology: A Step-by-Step Guide for Beginners.* Third ed. London: SAGE.

Kurth, H. A. 2020. South Africa's Protection of Personal Information Act, 2013, Goes into Effect 1 July. *The National Law Review,* XII(164):1-4.

Kwet, M. 2020. *Surveillance in South Africa: From Skin Branding to Digital Colonialism,* New Haven:The Cambridge Handbook of Race and Surveillance

Larson, L. 2020. Story maps.
Internet:https://storymaps.arcgis.com/stories/1882937c0c1742ae90d96f69def2e5e8. Accessed October 20 2020.

Laskar, M. E. 2013. *Summary of Social Contract Theory by Hobbes, Locke and Rousseau,* LL.M Symbiosis Law School.

Lena, D. & Cable, J., 2017. The advent of surveillance realism: public opinion and activist responses to the Snowden leaks. *International Journal of Communication,* 11: 763-781.

Leggett, T. 2002. *Monograph 69: Drugs and Crime in South Africa: A Study in Three Cities,* Pretoria: Institute for Security Studies.

Levi, M. & Wall. 2004. Technologies, Security, and Privacy in the Post-9/11 European Information Society. *Journal of Law and Society,* 31(2):194-220.

Lieshout, M. V., Friedewald, M., Wright, D. & Gutwirth, S. 2013. Reconciling privacy and security. *Innovation: The European Journal of Social Science Research,* 26(1-2) 119-132.

Locke, J. 1689. *Two Treatises of Civil Government.* London: Awnsham Churchill.

Lopach, J. J. & Luckowski, J. A. 2006. National Security and Civil Liberty: Striking the Balance. *The Social Studies*, 97(6): 245-248.

Mabanga, S. P. 2013. *South Africa's official external threat perceptions: 1994-2012, Masters diss., University of Pretoria. Retrieved online at: http://hdl.handle.net/2263/43680.*

Mahapatra, S. 2021. Digital Surveillance and the Threat to Civil Liberties in India. *German Institute of Global and Area Studies (GIGA)*, 3:1-12.

Marais, N. 2021. *Building a Fit for Purpose South African Intelligence Service,* Brenthurst Foundation.

Maras, M.-H. 2012. The social consequences of a mass surveillance measure: What happens when we become the 'others?. *International Journal of Law, Crime and Justice*, 40:65-81.

Marquis-Boire, M., Marczak, B., Guarnieri, C. & Scott-Railton, J. S.-R. 2013. *For Their Eyes Only: The Commercialization of Digital Spying,*The Citizen Lab.

Mavedzenge, J. A. 2020.. The Right to Privacy v National Security in Africa: Towards a Legislative Framework Which Guarantees Proportionality in Communications Surveillance*. African Journal of Legal Studies,*12:360-390.

McLaughlin, J. 2016. South African spy company used by Gadaffi touts its NSA like capabilities: The South African company best known for selling Muammar Gaddafi's regime spy equipment is now claiming it can intercept communications on a scale that rivals a government spy agency.*The Intercept.* Internet:https://theintercept.com/2016/10/31/south-african-spy-company-used-by-gadaffi-touts-its-nsa-like-capabilities/. Accessed 18 May 2022.

Memdutt, V. 2019. Does govt have 'Grabber' technology? We demand answers!. *Right2Know.* Internet: https://www.r2k.org.za/2015/09/03/surveillance-device/. Accessed 20 August 2022.

Milanovic, M. 2015. Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. *Harvard International Law Journal,* 56(1):81-146.

Moore, A. D. 2011. Privacy, Security, And Government Surveillance: Wikileaks and The New Accountability. *Public Affairs Quarterly*, 25(2):141-156.

Moore, M. 2018. *Democracy Hacked: Political Turmoil and Information Warfare in the Digital Age*. London: One World.

Morgenthau, H. J. 1952. Another "Great Debate": The National Interest of the United States. The *American Political Science Review*, 46 (4): 961-988.

Mouritz, T. 2010. Comparing The Social Contracts Of Hobbes and Locke. *The Western Australian Jurist,* 1:123-127.

Murphy, J. & Wu, J. 2022. Map: Track coronavirus deaths around the world. *NBC News.* Internet: https://www.nbcnews.com/news/world/world-map-coronavirus-deaths-country-covid-19-n1170211. Accessed 4 September 2022.

Mutung'u, G. 2021. *Surveillance Law in Africa: a review of six countries: South African Country Report,* Institute of Development Studies.

Nathan, L. 2017. Who's keeping an eye on South Africa's spies? Nobody, and that's the problem.*The Conversation.* Internet: https://theconversation.com/whos-keeping-an-eye-on-south-africas-spies-nobody-and-thats-the-problem-84239. Accessed 18 May 2022.

Neidleman, J. 2012. *The Social Contract Theory in a Global Context,* E-International Relations.Internet:https://www.e-ir.info/2012/10/09/the-social-contract-theory-in-a-global-context/. Accessed 20 May 2022.

Nicholls, D. 2021. Unfettered state surveillance to end: RICA declared unconstitutional. *Harringtons Johnson Wands Attorneys.* Internet: https://www.hjw.co.za/newsandmedia/unfettered-state-surveillance-to-end-rica-declared-unconstitutional. Accessed 6 August 2022.

Nuechterlein, D. E. 1976. National interests and foreign policy: A conceptual framework for analysis and decision-making. *Review of International Studies,* 2(3):246 - 266.

Nye, J.1999. Redefining the National Interest. *Foreign Affairs,* 8(4):22-35.

Obama, B. 2013. *Statement by the President.* Washington D.C, The White House: Office of the Press Secretary.

Olsen, N. 2022. South Africa's POPI Act. *Privacy Policies.* Internet: https://www.privacypolicies.com/blog/popi-act/#Condition_7_Security_Safeguards. Accessed 4 August 2022.

Omand, D. 2013. Securing the State: National Security and Secret Intelligence. *Institute for National Strategic Security, National Defense University,* 4(3):14-27.

Pavone, V., Gomez, E. . S. & Jaquet-Chifelle, . D.-O. 2016. A Systemic Approach to Security. *Democracy and Security,* 12(4):225-246.

Pauw, J. 2017. *The President's Keepers: Those keeping Zuma in power and out of prison.*Tafelberg.

Pepper, M. S. & Botes , M. 2020. Analysis: Balancing privacy with public health during COVID-19: how well is South Africa doing? *University of Pretoria*.Internet: https://www.up.ac.za/news/post_2906497-analysis-balancing-privacy-with-public-health-during-covid-19-how-well-is-south-africa-doing. Accessed 4 Septemeber 2022.

Perez, T.K. 2020. Does National Security outweigh the Right to Privacy.The Perspective. Internet:https://www.theperspective.com/debates/living/national-security-outweigh-right-privacy/. Access October 20 2020.

Pienaar, L. E. 2014. *Serious Crime as a National Security Threat in South Africa Since 1994,* PhD diss., University of Pretoria. Retrieved online at: http://hdl.handle.net/2263/46070.

Pozen, D. E. 2016. Privacy-Privacy Tradeoffs. *The University of Chicago Law Review*, 83(1):221-247.

Pratt, M. K. 2022. What is a cyber attack?. *TechTarget.* Internet: https://www.techtarget.com/searchsecurity/definition/cyber-attack.Accessed 4 September 2022.

Privacy International. 2014. South African Government still funding VASTech, knows previous financing was for mass surveillance. *Privacy International.* Internet: https://privacyinternational.org/blog/1308/south-african-government-still-funding-vastech-knows-previous-financing-was-mass. Accessed 15 May 2022.

Privacy International.2016. Right2Know& Association For Progressive Communication. *Submission in advance of the consideration of the periodic report of South Africa, Human Rights Committee, 116th Session, 7 – 31 March*: Association for Progressive Communications.

Privacy International.2016. Right2Know & Association for Progressive Communication. *Suggestions for right to privacy-related questions to be included in the list of issues on South Africa, Human Rights Committee, 114th session, June-July 2015,* Association for Progressive Communications.

Privacy International. 2018. New Privacy International report reveals dangerous lack of oversight of secret global surveillance networks. *Privacy International.* Internet: https://privacyinternational.org/long-read/1742/new-privacy-international-report-reveals-dangerous-lack-oversight-secret-global. Accessed 4 September 2022.

Privacy International. 2019. State privacy South Africa. *Privacy International.* Internet:https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa. Accessed 20 August 2022.

Privacy International. 2021a. South African Constitutional Court declares bulk surveillance powers unlawful. *Privacy International.* Internet:https://privacyinternational.org/news-analysis/4416/south-african-constitutional-court-declares-bulk-surveillance-powers-unlawful. Accessed 17 May 2022.

Privacy International. 2021b. Mass surveillance. *Privacy International Organisation.* Internet: https://privacyinternational.org/learn/mass-surveillance. Accessed November 1 2021.

Qian, I., Xiao, M., Mozur, P. & Cardia, A. 2022. Four Takeaways From a Times Investigation Into China's Expanding Surveillance State: Times reporters spent over a year combing through government bidding documents that reveal the country's technological road map to ensure the longevity of its authoritarian rule.*The New York*

Times. Internet: https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html. Accessed 10 November 2022.

Raab, C. D., 2017. Security, Privacy and Oversight. In: *Security in a Small Nation: Scotland, Democracy, Politics.* Edinburgh: Open Book Publishers: 78-99.

Ram, N. & Gray, D., 2020. Mass surveillance in the age of COVID-19. *Journal of Law and the Biosciences:*1-17.

Rawls, J., 1971. *A theory of justice.* London: Havard University Press.

Ring, T. 2016. *Your Data in Their Hands: Big Data, Mass Surveillance And Privacy,* Computer Fraud and Security.

Ritchie, D. G. 1891. Contributions to the History of the Social Contract Theory. *Political Science Quarterly,* 6(4):656-676.

Roberts, T. 2021. Surveillance laws are failing to protect privacy rights: what we found in six African countries, including South Africa. *Daily Maverick.* Internet: https://www.dailymaverick.co.za/article/2021-11-08-surveillance-laws-are-failing-to-protect-privacy-rights-what-we-found-in-six-african-countries-including-south-africa/.Accessed 12 May 2022.

Rousseau, J.-J. 1893. *The Social Contract or the Principles of Political Rights.* New York: G.P. Putnam's Sons.

Royce, M. 2010. Philosophical Perspectives on the Social Contract Theory: Hobbes, Kant and Buchanan Revisited A Comparison of Historical thought Surrounding the Philosophical Consequences of the Social Contract and Modern Public Choice Theory. *Postmodern Openings,* 4(1):45-62.

SABC. 2022. Mozambique children displaced by terrorism in Cabo Delgado. *SABC.* Internet: http://web.sabc.co.za/sabc/home/channelafrica/news/details?id=d444668b-cfe1-4654 85308c6cea7d6057&title=Over%20400%20000%20Mozambique%20children%20displaced%20by%20terrorism%20in%20Cabo%20Delgado. Accessed 4 August 2022.

Sarkar, S. 2021. “Did RICA do enough?”- South Africa’s top Court highlights inadequate privacy safeguards of RICA; declares it unconstitutional. *SCC online.* Internet: https://www.scconline.com/blog/post/2021/03/31/privacy-2/. Accessed 5 August 2022.

Scheiner, B. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* New York: W.W. Norton and Company.

Schroeder, D. N. 1973. John Rawls and Contract Theory. *Soundings: An Interdisciplinary Journal,* 56(3):338-348.

Schuster, S., Van den Berg, M., Larrucea, M., Slewe, T. & Ide-kostic, P. 2017. Mass surveillance and technological policy options: Improving security of private communications. *Computer Standards & Interfaces,* 50:76-82.

Seegers, A. 1996. *The military in the making of modern South Africa.* London: Tauris.

Shamsi, H. & Abdo, A. 2001. Privacy and Surveillance Post-9/11. *American Bar Association.* Internet *:* https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/human_rights_vol38_2011/human_rights_winter2011/privacy_and_surveillance_post_9-11/. Access November 1 2021.

Sherman, J. 2022. Russia's Internet Censor Is Also a Surveillance Machine. *Council on Foreign Relations*. Internet: https://www.cfr.org/blog/russias-internet-censor-also-surveillance-machine. Accessed 14 November 2022.

Snowden, E. 2019. Permanent Record. London:Metropolitan Books.

Solove, D. J. 2011. *Nothing to Hide: The False Trade Tradeoff between Privacy and Security.* London: Yale University Press.

Sonjica, N. 2021.Constitutional Court declares provisions of Rica unconstitutional.*Sunday Times.* Internet: https://www.timeslive.co.za/news/south-africa/2021-02-04-constitutional-court-declares-provisions-of-rica-unconstitutional/. Accessed 6 August 2022.

Stahl, T. 2016. Indiscriminate mass surveillance and the public sphere. *Ethics and Information Technology*, 18: 33-39.

Stansberry, K., Anderson , J. & Rainie , L. 2019. *Experts Optimistic About the Next 50 Years of Digital Life, Pew Research Center*.Internet: https://www.pewresearch.org/internet/2019/10/28/experts-optimistic-about-the-next-50-years-of-digital-life/. Accessed 15 May 2022.

Swart, H. 2015a. Say nothing – the spooks are listening. *Mail & Guardian.*Internet:https://mg.co.za/article/2015-12-17-say-nothing-the-spooks-are-listening/. Accessed 10 May 2022.

Swart, H. 2015b. How cops and crooks can 'grab' your cellphone – and you. *Mail & Guardian.* Internet:https://mg.co.za/article/2015-11-29-how-cops-and-crooks-can-grab-your-cellphone-and-you/.Accessed 20 August 2022.

Swart, H. 2017a. Op-Ed: Big Brother is watching your phone call records. *Daily Maverick.* Internet:https://www.dailymaverick.co.za/article/2017-05-10-op-ed-big-brother-is-watching-your-phone-call-records/.Accessed 15 May 2022.

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

enforcement-pulls-70000-subscribers-call-records-each-year-and-thats-a-minimum-estimate/#.WfCO40zMxTY. Accessed 20 August 2022.

Swart, H. 2018. Controlling Cape Town: The real costs of CCTV cameras, and what you need to know.*DailyMaverick.* Internet:https://www.dailymaverick.co.za/article/2018-10-05-controlling-cape-town-the-real-costs-of-cctv-cameras-and-what-you-need-to-know/.Accessed 4 August 2022.

Swingler, H. 2018. State surveillance grows, accountability lags .*University of Cape Town.* Internet:https://law.uct.ac.za/articles/2018-10-17-state-surveillance-grows-accountability-lags. Accessed 4 September 2022.

Taylor, L., Sharma, G., Martin, A. & Jameson, S. 2020. *Data Justice and Covid-19: Global Perspectives.* London: Meatspace Press.

Trood, R. & Bergin, A. 2015. *Creative tension: Parliament and national security,* Australian Strategic Policy Institute.

Ullman, R. H. 1983. Redefining Security. *International Security*, 8 (1): 129-153.

Underwood, B. & Saiedian, H. 2021. Mass surveillance: A study of past practices and technologies to predict future directions. *Security and Privacy.* 4(142): 1-23.

United Nations. 2015. *Universal Declaration of Human Rights*. Paris:United Nations.

Ünver, H. A. 2018. Politics of Digital Surveillance, National Security and Privacy. *Centre for Economics and Foreign Policy Studies*. 2:1-23.

United Nations Office on Drugs and Crime. 2020. Key issues defining terrorism.*UNODC.* Internet: https://www.unodc.org/e4j/en/terrorism/module-4/key-issues/defining-terrorism.html. Accessed 4 September 2022.

Upadhyav, A. 1993. Rawlsian Concept of Two Principles of Justice. *The Indian Journal of Political Science,* 54(3):388-397.

Van Heerden, J. 2019. *An evaluation of the concept of national security as determined by the South African Constitution and its interpretation by the State Security Agency,* Masters diss., North West University. Retrieved online at: https://repository.nwu.ac.za/bitstream/handle/10394/33835/Van%20Heerden%20JG%2010218823.pdf?sequence=1%26isAllowed=y.

Vermeulen, J. 2013. Spyware servers in SA: more details emerge. *My Broadband.* Internet: https://mybroadband.co.za/news/security/86437-spyware-servers-in-sa-more-details-emerge.html. Accessed 20 August 2022.

Vermeulen, J. 2015. How secret SARS unit spied on South Africans: report. *My Broadband.* Internet: https://mybroadband.co.za/news/security/119370-how-secret-sars-unit-spied-on-south-africans-report.html. Accessed 20 August 2022.

Waltz, K. 1979. Theory of International Politics. Boston: McGraw-Hill.

Waters, S. 2018. The Effects of Mass Surveillance on Journalists' Relations With Confidential Sources. *Digital Journalism,* 6(10): 1294-1313.

Watt, E. 2017. The right to privacy and the future of mass surveillance. *The International Journal of Human Rights*, 21(7):773-799.

Williams, M. C. 2003. Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly,* 47:511–531.

Williams, P.D. (ed). 2013. *Security Studies: An introduction*. 2nd Edition Houndmills: Palgrave Macmilliam.

Wolfers, A. 1952. "National Security" as an Ambiguous Symbol. *Political Science Quarterly*, 67 (4): 481-502.

World Health Organisation. 2022. The true death toll of COVID-19: estimating global excess mortality. *World Health Organisation.* Internet: https://www.who.int/data/stories/the-true-death-toll-of-covid-19-estimating-global-excess-mortality. Accessed 4 September 2022.

Zalnieriute, M. 2015. An international constitutional moment for data privacy in the times of mass surveillance. *International Journal of Law and Information Technology*, 23:99-133.

APPENDIX A: ETHICAL CLEARANCE

Faculty of Humanities
Fakulteit Geesteswetenskappe
Lefapha la Bomotho

2 March 2022

Dear Miss A Cartwright

Project Title:	Examining the relationship between national security and the individual citizen's right to privacy in South Africa between 1994 and 2021
Researcher:	Miss A Cartwright
Supervisor(s):	Prof VL Graham
Department:	Political Sciences
Reference number:	17226997 (HUM014/0222)
Degree:	Masters

Thank you for the application that was submitted for ethical consideration.

The Research Ethics Committee notes that this is a literature-based study and no human subjects are involved.

The application has been approved on 27 January 2022 with the assumption that the document(s) are in the public domain. Data collection may therefore commence, along these guidelines.

Please note that this approval is based on the assumption that the research will be carried out along the lines laid out in the proposal. However, should the actual research depart significantly from the proposed research, a new research proposal and application for ethical clearance will have to be submitted for approval.

We wish you success with the project.

Sincerely,

Prof Karen Harris
Chair: Research Ethics Committee
Faculty of Humanities
UNIVERSITY OF PRETORIA
e-mail: tracey.andrew@up.ac.za