

UNIVERSITY OF THE WESTERN CAPE

FACULTY OF LAW
DEPARTMENT OF MERCANTILE AND LABOUR LAW

A mini-thesis submitted in partial fulfillment of the requirements for the LLM degree
in Mercantile Law in the Department of Mercantile and Labour Law, Faculty of Law,
University of the Western Cape

**The Protection of Personal Information in Smart Cities:
Lessons for South Africa from the European Union and the
United States**

UNIVERSITY *of the*
WESTERN CAPE

By:

Faisal Idris Sheikh

Student No:

4080307

Supervisor: Dr T Kondo

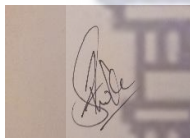
July 2023

DECLARATION

I, Faisel Idris Sheikh hereby declare that this dissertation is original. It has never been presented to any other university or institution. Where other people's ideas have been used, proper references have been provided. Where other people's words have been used, they have been quoted and duly acknowledged.

Student Name: Faisel Idris Sheikh (4080307)

Signature:



Date: 30 June 2023



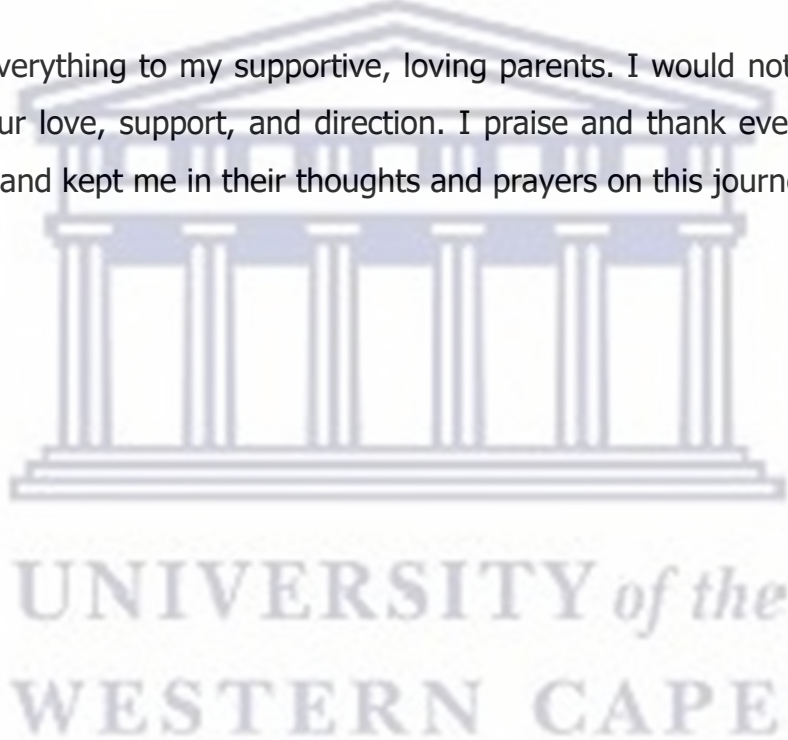
UNIVERSITY *of the*
WESTERN CAPE

ACKNOWLEDGEMENTS

In the name of Allah (God), Most Gracious, Most Merciful. Without Allah's help, I would not have reached this far. I express my gratitude to Amka and everyone who contributed to the successful completion of this project.

I am indebted to Dr. Tinashe Kondo for his expert and invaluable assistance with this project. I thank my family and friends who were always inquiring about my well-being and who were always willing to lend a hand.

Finally, I owe everything to my supportive, loving parents. I would not be where I am now without your love, support, and direction. I praise and thank everyone who have wished me well and kept me in their thoughts and prayers on this journey.



DEDICATION

I wish to dedicate my work to my parents for all their love and moral support. I also wish to dedicate my work to all young law students who are enthusiastic about smart cities and data protection. There is still a substantial amount of effort that is required to ensure that sustainable practices are adopted and applied. I hope that this work contributes to that dialogue.



KEYWORDS

Artificial Intelligence

Big data

Data protection

GDPR

Information Communication Technology

Personal information

POPIA

Privacy

Smart cities



TABLE OF CONTENTS

DECLARATION.....	i
ACKNOWLEDGEMENTS.....	ii
DEDICATION	iii
KEYWORDS	iv
CHAPTER 1.....	1
INTRODUCTION AND BACKGROUND.....	1
1.1 INTRODUCTION.....	1
1.2 BACKGROUND TO THE STUDY	3
1.3 RESEARCH QUESTION.....	11
1.4 RESEARCH OBJECTIVES	11
1.5 BENEFITS OF THE STUDY.....	12
1.6 METHODOLOGY	12
1.7 LIMITATIONS AND DELIMITATIONS	13
1.8 LITERATURE REVIEW.....	13
1.9 OVERVIEW OF THE STUDY.....	18
CHAPTER 2.....	20
CONCEPTUAL FRAMEWORK: THE DATA PRIVACY PRINCIPLES AND PRIVACY BY DESIGN.....	20
2.1 INTRODUCTION.....	20
2.2 TERMINOLOGIES, KEY REFERENCES AND DEFINITIONS	21
2.2.1 Smart cities.....	22
2.2.2 Mobile applications	25

2.2.3 Data	26
2.2.4 Big data	26
2.2.5 The Internet of Things.....	28
2.2.6 Data breaches.....	29
2.2.7 Profiling and Information matching.....	30
2.2.8 The cloud and cyber attacks	30
2.2.9 Ubiquitous Surveillance.....	32
2.3 DATA PROTECTION BY PRIVACY BY DEFAULT	33
2.4 PRIVACY BY DESIGN	34
CHAPTER 3.....	38
INTERNATIONAL FRAMEWORK ON DATA PROTECTION	38
3.1 INTRODUCTION.....	38
3.2 THE EVALUATION OF THE CONCEPT OF THE RIGHT TO PRIVACY	39
3.3 RIGHT TO PRIVACY IN INTERNATIONAL INSTRUMENTS	40
3.3.1 The Universal Declaration of Human Rights.....	40
3.3.2 The International Covenant on Civil and Political Rights	41
3.3.3 The Convention on the Rights of the Child	42
3.4.1 European Convention on Human Rights of 1950.....	43
3.4.2 American Convention on Human Rights of 1969	43
3.4.3 African Charter of Human and People’s Rights of 1981	45
3.4.4 African Charter on the Rights and Welfare of the Child of 1990	46
3.4.5 The African Union Framework for Human Rights and Privacy	46
3.5 PRIVACY AND DATA PROTECTION IN SUB-REGIONAL FRAMEWORKS IN SUB- SAHARAN AFRICA.....	49

3.6 SOFT LAW: INTERNATIONAL IMPERATIVES	50
3.6.1 The Agenda 2030 For Sustainable Development.....	51
3.6.2. The Agenda 2063-The Africa We Want	51
3.7 CONCLUSION.....	52
CHAPTER 4.....	54
SOUTH AFRICA'S LEGAL FRAMEWORK GOVERNING DATA PROTECTION.....	54
4.1 INTRODUCTION.....	54
4.2 THE NATIONAL GROWTH STRATEGY	54
4.3 SOUTH AFRICA'S DATA PRIVACY PRIOR TO THE ENACTMENT OF THE POPI ACT	56
4.3.1 Constitutional protection of privacy.....	56
4.3.2 Protection of Privacy Under Common Law	59
4.3.3 Limitations to the protection of data privacy under the common law and the Constitution	60
4.4 SUBORDINATE DATA PROTECTION LEGISLATION	61
4.4.1 Promotion of Access to Information Act No. 2 of 2000	61
4.4.2 The Electronic Communications and Transactions Act No. 25 of 2002	62
4.4.3 National Credit Act 34 of 2005.....	62
4.5 THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013	63
4.5.1 Specific Data Protection: A summary of the POPIA	64
4.5.2. POPIA Purpose and Application	65
4.5.3. Key terms Employed in the POPIA.....	66
4.5.4. Conditions for the legitimate Processing of Personal Data	67
4.6 SOFT LAW	71
4.6.1 The Integrated Framework for Urban Development.....	71

4.6.2 The District Development Model	71
4.6.3 Smart-specific policies, initiative and guidelines	73
4.7 CONCLUSION.....	73
CHAPTER 5.....	75
COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS IN VARIOUS JURISDICTIONS	75
5.1. INTRODUCTION.....	75
5.2. DATA PROTECTION IN THE U.S.....	75
5.2.1. The U.S. Constitution's Fourth Amendment.....	76
5.2.2. Sectoral laws.....	77
5.3 DATA PROTECTION IN THE EU	84
5.3.1 INTRODUCTION.....	84
5.3.2. Changes to the EU Data Protection Framework	86
5.3.3 Definitions	87
5.3.4 Extraterritorial Application.....	88
5.3.5. Data Subject's Rights.....	88
5.4 IS THERE A LACK OF ACCOUNTABILITY?	90
5.5 CONCLUSION.....	91
CHAPTER 6.....	92
SMART CITY FRAMEWORK	92
6.1 INTRODUCTION.....	92
6.2 IDEAL FRAMEWORK FOR SMART CITIES	93
6.2.1 The Integrated Framework for Urban Development.....	93
6.3 EXAMPLES OF SMART INITIATIVES IN SOUTH AFRICA	94

6.4 PRIVACY CONSIDERATIONS FOR SMART CITIES	96
6.5 SAFEGUARDING PRIVACY IN SMART CITIES.....	97
6.6 LESSONS THAT CAN BE LEARNED FROM LOCAL AND INTERNATIONAL INITIATIVES.....	98
6.7 CONCLUSION.....	100
CHAPTER 7.....	101
CONCLUSION AND RECOMMENDATIONS	101
7.1 OVERVIEW	101
7.2 CONCLUSION.....	102
7.3 RECOMMENDATIONS	103
7.3.1 Recommendations on Technological Foresight.....	103
7.3.2 Recommendations for Reform	104
7.3.3 Governance and implementation Foresight.....	106



CHAPTER 1

INTRODUCTION AND BACKGROUND

1.1 INTRODUCTION

Innovative technologies are being employed in both public and private sectors alike.¹ Since the beginning of the 21st century, the use of these technologies has grown in both volume and type.² E-commerce services have also developed utilising these technologies, complemented by the use of devices such as smartphones, tablets and computers. The integration of these technologies has even moved into homes.³

Modern technologies are being used to control homes, run appliances, amongst other purposes. Many of the devices in this ecosystem can be connected to the internet.⁴ Nowadays, one can switch on their air-conditioning system away from home using a mobile application. The same goes with closed-circuit television systems (CCTV) which can be monitored and controlled remotely using of an application enabled by wireless technologies (for example, WIFI).⁵

The use of these technologies within the homes is of vital importance in the modern economy.⁶ This is particularly important because of the rise of what are known as “smart cities”.⁷ These technologically enabled modern areas utilise various types of electronic

¹ Gutwirth S et al *Reinventing Data Protection?* 9 ed (2009) 5.

² Kitchin R 'The Real-Time City? Big Data and Smart Urbanism' (2014) 79(1) *GEOJ 1* (hereafter: "Smart Urbanisation").

³ Hiller J and Blanke J 'Smart Cities, Big Data, and the Resilience of Privacy' (2017) 68(2) *HLJ 2*.

⁴ Koops B 'The trouble with European data protection law' (2014) 4(4) *IDPL* 250.

⁵ Ziegeldorf JH Morchon OG and Wehrle K 'Privacy in the Internet of Things: threats and challenges.

Security and Communications Networks' (2014) 7(12) *Wiley Online Library* 2728.

⁶ Schönberger MV & Cukier K *Big Data: A Revolution that Will Transform how We Live, Work, and Think* 6 ed (2013) 8.

⁷ Moir E *et al*, United Kingdom Government Office for Science- *What Are Future Cities? Origins, meanings, and uses* (2014) 4-33 (hereafter *Future Cities*).

methods. With internal migration on the rise globally, and semigration a common feature, new cities are emerging.⁸ It is estimated that by 2050, cities will account for 70% of the world population.⁹ The development of these cities as smart cities could aid in growing efficiency and lowering costs within these cities. Furthermore, if the technology is used creatively, this could lead to more sustainable cities.¹⁰

It would be interesting to ascertain how the data in these smart cities will be protected.¹¹ A smart city entails the movement of vast amounts of data, which if intercepted or mishandled, can bring about many different challenges.¹² Furthermore, the question of who can be data controllers to the data also emerge.¹³ The issue of data privacy has therefore become a contentious issue globally.¹⁴ This has seen numerous jurisdictions developing data privacy laws.¹⁵ It is against this background that this thesis explores the regulation of smart cities focusing on the connections thereof with data privacy laws.¹⁶

-
- ⁸ Clavell GG (Not So) Smart Cities - The societal drivers and impact of smart environments, Privacy and Emerging Sciences and Technologies (2012) 40(6) *Oxford University Press* 27.
- ⁹ United Nations Department of Economic and Social Affairs 'World Urbanization Prospects: The 2014 Revision, Highlights, United Nations, Department of Economic and Social Affairs, Population Division' available at <http://esa.un.org/unpd/wup/Highlights/WUP2014-Highlights.pdf> (accessed 5 October 2021).
- ¹⁰ European Commission 'smart and sustainable cities' available at http://ec.europa.eu/regional_policy/sources/thefunds/instruments/doc/jessica/jessica_horizontal_study_smart_and_sustainable_cities_en.pdf (accessed 5 September 2021).
- ¹¹ Lever A *et al* *On privacy, Thinking in Action*, series editors: Simon Critchley 1 ed (2012) 5.
- ¹² International Business Machines Corporation 'Analysing the future of cities' available at https://www.ibm.com/smarterplanet/us/en/smarter_cities/overview/index.html. (accessed 6 October 2021).
- ¹³ Neethling J *et al* *Law of Personality* 2 ed (2005) 276. Also see Roos A 'Core principles of data protection law' (2006) 39(1) *CILSA* 104.
- ¹⁴ Greenleaf 'Global Data Privacy Laws 2013: 99 Countries and counting' (2013) *Privacy Laws and Business International Report* 10' available at <http://ssrn.com/abstract=2305882> (accessed 7 October 2021).
- ¹⁵ Roos A 'Data Protection: explaining the international backdrop and evaluating the current South African position' (2007) 124 *SALJ* 402.
- ¹⁶ *Article 8 of the Charter of Fundamental Rights of The European Union 2000/C 364/01* (hereafter referred to as *the Charter*). This change is reflected in the General Data Protection Regulation (hereafter referred to as *GDPR*) which records its purpose in *art 1(2)* in relation to the right to the protection of personal data in particular but refers also to all fundamental rights and freedoms which would, of course, continue to include the right to privacy protected under *art 7 of the Charter*.

1.2 BACKGROUND TO THE STUDY

As earlier discussed, the impact of computer technologies on the protection of personal information has been a cause for concern.¹⁷ However, what is under discussion in many jurisdictions is the question of what principles should be applied to resolve this challenge.¹⁸ This is especially important given the commodification of data in the modern economy.¹⁹ Data has, in a sense, become the “liquid gold” of this generation, with data being sold off to third parties to be mined. Others have likened its attributes as having a commercial value comparable to monetary currency.²⁰

With the growth and popularity of data, so has the processing capabilities of this commodity developed. Data can now be collected, stored and analysed at previously unimaginable scales. As a result, pundits have coined this millennium as the 'big data' era. The term “big data” refers to a collection of “high-volume, high-velocity, and diverse information assets²¹” that are analysed using advanced analytics to enable cost-effective, efficient, evidence-based, and frequently automated decision making.²² The European Union Data Protection Working Party conceptualises it as:

"[A] broad term that encompasses a large number of data processing operations, some of which are well-defined, while others remain obscure, and many more are expected to be

¹⁷ Chertoff M *Exploding Data: Reclaiming Our Cyber Security in the Digital Age* 1 ed (2018) 4. Also see Duncan J *Stopping the Spies: Constructing and resisting the surveillance state in South Africa* 1ed (2018) 7.

¹⁸ Information and Privacy Commissioner of Canada: Ontario *Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers on Information and Privacy* (2011) 2.

¹⁹ Kitchin R 'The Real-Time City? Big Data and Smart Urbanism' (2014) 79(1) *GEOJ* 1.

²⁰ Hancke G & de Carvalho de Silva B 'The Role of Advanced Sensing in Smart Cities' (2013) 13(1) *Sensors* 394.

²¹ Gonschorek A 'How Luno Uses Data to Make Product Decisions' available at <https://www.offerzen.com/blog/how-luno-uses-data-to-make-product-decisions>. (accessed 7 October 2021).

²² Gandomi A & Haider M 'Beyond the Hype: Big Data Concepts, Methods, and Analytics' (2015) 35(2) *International Journal of Information Management* 137 and Townsend B & Thaldar D 'Navigating Uncharted Waters: Biobanks and Informational Privacy in South Africa' (2019) 35(4) *South African Journal on Human Rights* 329.

developed in the near future".²³

Big data therefore has the potential to uncover unique and unexpected correlations and stimulate innovation. Some scholars believe that big data has the ability to provide for our modern economies. This notwithstanding, it has also been noted that some of the benefits can be undermined by fundamental data protection principles²⁴ which have largely remained unchanged since they were first articulated in the 1980s.²⁵ This problematic given the widespread changes in data that have taken place since then.

This is further complicated by the fact that, despite the cross-border nature of data usage, there are no uniform global rules for its treatment. As with many concepts, they are currently regulated at a national level. Despite moves for multilateralisation, there have been many challenges. The issue of sovereignty remains a key issue with many states refusing to cede their law-making capabilities to a supranational body. While there has been success in some areas such as international trade law, this remains a sticking point in other areas. For instance, for the last century, negotiations for a multilateral instrument on foreign investment have not realised any success. This is bizarre given the connections between these two fields.

Perhaps the largest collaboration on data regulation has been in the European Union (EU). Their data protection regulation, the General Data Protection Regulation (GDPR) (2016)²⁶ is a pioneer and leader in this area. Other jurisdictions have extensively

²³ European Commission *Article 29 Data Protection Working Party Statement on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU* (WP 221 of 16 September 2014) 3.

²⁴ European Data Protection Supervisor ("EDPS") *Opinion 8/2016 on the Coherent Enforcement of Fundamental Rights in the Age of Big Data* (2016) 2.

²⁵ Organisation for Economic Cooperation and Development (*hereafter "OECD"*) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) has been updated in 2013, but the data protection principles remain unchanged: OECD, *The OECD 'Privacy Framework'* (2013) 4. As to earlier national data protection legislation enacted in the 1970s see 'OECD, *Thirty Years After the OECD' Privacy Guidelines* 16–17 available at <https://www.oecd.org/sti/ieconomy/49710223.pdf>. (accessed 9 October 2021).

²⁶ *European Union Directive* (*hereafter referred to as "Directive"*) 2016/680 of the European Parliament and

borrowed from this document, making it a blueprint or model for data protection. The GDPR came into effect on the 25th May 2018. The GDPR replaces the 1995²⁷ Data Protection Directive. However, the fundamental principles of data protection remain identical. The GDPR also establishes a streamlined 'one-stop shop' enforcement structure in the form of the European Data Protection Board (EDPB). This body is a "leading supervisory authority" for establishments located within the EU that conduct cross-border data transfers within the EU or to jurisdictions with adequate privacy safeguards.²⁸

In the United States of America (US), there is no one document that governs data privacy at a federal level.²⁹ Regulation in the United States therefore entails a complex framework of sector specific and medium-specific laws. This involves regulations across various sectors such as health, finance, credit and telecommunications. These jumbled up provisions span into the hundreds, available at a federal and a state level. For instance, at a federal level, the Federal Trade Commission Act empowers the Federal Trade Commission to take measures designed to protect consumers. This *inter alia* entails measures crafted to enforce federal privacy and data protection regulations. At a state level, one can also note the various piecemeal legislations that are available. For instance, in California there is the California Online Privacy Protection Act (CalOPPA)³⁰ which regulates privacy policy in California.

There are also voluntary compliance frameworks in the US. For instance, in response to

of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing *Council Framework Decision 2008/977/JHA* OJ L 119 (2016) (EU General Data Protection Regulation; "GDPR").

²⁷ *Directive 95/46/EC* of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) OJ 1995 L 281/31(1995).

²⁸ Articles 56 and 60 of the *General Data Protection Regulation 2016/679*.

²⁹ While changes are expected in this area, privacy is currently regulated at the state level (in some states, such as California) and through a variety of sector-specific laws. For a general overview, see California Department of Justice, 'Privacy Laws' (2019) available at <https://oag.ca.gov/privacy/privacy-laws> (accessed 6 October 2021).

³⁰ *The Online Privacy Protection Act of 2003*.

the Cambridge Analytica scandal, California enacted the California Consumer Privacy Act (CCPA) (2018).³¹ Corporations in the US may voluntarily comply with the Privacy-Shield framework³² or standard contractual terms governing data transfers between the US and the European Union (EU).

In South Africa, privacy is a protected right under common law and under s 14 of the Constitution of South Africa.³³ The Constitution declares the right to privacy a fundamental human right. The constitutional³⁴ right to privacy includes "informational privacy",³⁵ which is defined as a person's right to control and decide when, how, and under what circumstances their personal information may be disclosed to the public.³⁶ Data protection is critical for ensuring an individual's right to privacy.³⁷

In South Africa, the common law right to privacy was recognised in *O'Keefe v Argus Printing*³⁸, where the court determined that the right to dignity includes the right to privacy.³⁹ South African courts recognised the right to privacy as a distinct personality right for the first time in this case. The Constitutional Court later affirmed this recognition in *Bernstein & others v Bester*⁴⁰, with Ackerman J holding that privacy refers to a person's truly personal aspects, not to every aspect of his or her personal knowledge and

³¹ *The California Consumer Privacy Act of 2018*.

³² United States Department of Commerce 'EU-U.S. Privacy Shield Framework Principles' available at <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg> (accessed 6 October 2021). Also see United States Department of Commerce, 'Swiss-US Privacy Shield Framework' available at <https://www.trade.gov/td/services/odsi/swiss-us-privacyshield-framework.pdf>. (accessed 3 September 2021).

³³ The Constitution of the Republic of South Africa, 1996 (hereafter "*Constitution*").

³⁴ Section 14(d) of the Constitution provides that 'everyone has the right to privacy, which includes the right not to have the privacy of their communications infringed.'

³⁵ Currie I & De Waal JD, '*The Bill of Rights handbook*' 6 ed (2013) 302.

³⁶ *National Media Ltd v Jooste* [1996] 2 All SA 510 (A).

³⁷ Michalsons 'Data Privacy or Data Protection in South Africa' available at <https://www.michalsons.com/blog/data-privacy-in-south-africa/150>. (accessed 8 October 2021).

³⁸ *O'Keefe v Argus Printing and Publishing Co Ltd* [1954] 3 All SA 159 (C) (hereafter "*O'Keefe v Argus Printing*").

³⁹ Para 248 and para 249 of the court judgement in *O'Keefe v Argus Printing*.

⁴⁰ Para 79 of the court judgement in *Bernstein & others v Bester & others NNO* 1996 (2) SA 751 (CC) (hereafter *Bernstein & others v Bester & others*).

experience.⁴¹

Academics in South Africa criticised the Bernstein decision. Neethling⁴² argues that Ackerman J's restrictive interpretation of privacy ignores other private facts about a person that deserve protection.⁴³ A broader approach to data protection is necessary because, while small amounts of data may not be considered private under the Bernstein standard, the accumulation of small amounts of data may be of such a nature that the individual wishes to keep it private.⁴⁴

The imperative to modernise South African data protection legislation is motivated by a desire to advance social and economic development.⁴⁵ To attract foreign investment, it will be critical to enact and strictly enforce adequate data protection legislation.⁴⁶ The majority of foreign investors rely on data, and these investors require the assurance that the processing of their data is regulated and thus protected, deterring any unauthorised disclosure of their data.

In an attempt to bring South Africa in line with international prescripts, the South African Law Reform Commission ("SALRC") published a Discussion Paper⁴⁷ ("SALRC Discussion Paper") on privacy and data protection in which it recommended that formal legislation on the protection of personal information be enacted in order to safeguard the right to privacy. The SALRC Discussion Paper contained the proposed draft legislation that was ultimately signed into law on 19 November 2013 and known as the Protection of Personal Information Act 4 of 2013 ("POPIA").

⁴¹ Para 79 of the court judgement in *Bernstein & others v Bester & others*.

⁴² Neethling J 'The concept of privacy in South African Law' (2005) 122 (1) *SALJ* 18 – 28

⁴³ Neethling J 'The concept of privacy in South African Law' (2005) 122 (1) *SALJ* 20.

⁴⁴ Neethling J 'The concept of privacy in South African Law' (2005) 122 (1) *SALJ* 20.

⁴⁵ South African Law Reform Commission Discussion Paper 109 (Project 124) '*Privacy and data protection*' (2005) 40.

⁴⁶ Luck R 'POPI – Is South Africa keeping up with international trends' (2014), *De Rebus* 46. See also Roos A 'Core principles of data protection law' (2006) 39(1) *CILSA* 104.

⁴⁷ South African Law Reform Commission Discussion Paper 109 (Project 124) '*Privacy and data protection*' (2005). See also Roos A 'Data Protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *SALJ* 433.

Data protection is governed by the Protection of Personal Information Act 4 of 2013 (POPIA).⁴⁸ POPIA took effect on the 1st of July 2020 and included a one-year grace period for compliance.⁴⁹ This period has since ended but provision has been made for companies to still apply the Information Regulator to furnish reasons why they cannot still comply and request an extension. By regulating the processing⁵⁰ of personal information⁵¹ by public and private bodies, POPIA aims to give effect to the Constitutional right to privacy.⁵²

POPIA introduces a raft of new provisions that are of interest to this mini-thesis. One such provision that has taken effect is section 39, which establishes an impartial and independent body known as the Information Regulator with the authority to exercise certain powers and perform certain duties and functions under POPIA.⁵³ The Information

⁴⁸ *Protection of Personal Information Act 4 of 2013* ("POPIA").

⁴⁹ In Proclamation R21 of 2020 GG 43461 of 22 June 2020 the President announced the commencement of *ss 2–38; ss 55– 109; s 111; and s 114(1), (2) and (3)* POPIA with effect from 1 July 2020. In terms of *s 114(1)*, all processing must be brought into conformity with the Act within one year from that date.

⁵⁰ According to section 1 of POPIA, 'processing' refers to 'any operation or activity, whether automated, involving personal information, including (a) collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use; (b) dissemination via transmission, distribution, or making available in any other form; or (c) merging, linking, as well as restriction, of personal information.

⁵¹ In terms of *s 1* of POPIA 'personal information' means 'information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –

- (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- (b) information relating to the education or the medical, financial, criminal or employment history of the person;
- (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- (d) the biometric information of the person;
- (e) the personal opinions, views or preferences of the person;
- (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- (g) the views or opinions of another individual about the person; and
- (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;'

⁵² Preamble to POPIA.

⁵³ Preamble to POPIA.

Regulator is responsible to the National Assembly and is bound solely by the Constitution.⁵⁴ The Information Regulator was established on 1 December 2016 and is responsible for monitoring and enforcing compliance with the provisions of POPIA and the Promotion of Access to Information Act 2 of 2000 by public and private bodies.⁵⁵

The Act is intended to accomplish the following objectives:

- (a) to give effect to the constitutional right to privacy by safeguarding personal information processed by a responsible party;
- (b) to regulate the manner in which personal information may be processed, subject to certain legal requirements and international standards;
- (c) to provide individuals with rights and remedies to protect their personal information from unauthorised processing; and
- (d) to establish an information regulator (hereinafter the "Regulator") to promote, enforce, and carry out the Act's provisions.⁵⁶

The success of this document is that supersedes all other legislation unless the other legislation establishes more extensive or onerous conditions for lawful processing of personal information than those specified in the Act.⁵⁷

However, there are still a number of teething problems with POPIA. For instance, because data protection legislation is relatively new in South Africa, it is still untested in the courts and through implementation. The challenges are also not only with substantive provisions, but also with the institutional framework.⁵⁸ South Africa's information regulator is marred by a number of challenges. Most notably, it is struggling to keep up with rising data breach incidents and is suffering from significant funding

⁵⁴ Sections 39(a), 39(b) and 39(d) of POPIA.

⁵⁵ Section 40(1)(b) of POPIA.

⁵⁶ Section 2(a) – (d) POPIA.

⁵⁷ Section 2(a) – (b) POPIA.

⁵⁸ Roos A 'Data Protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124(2) *SALJ* 423 (hereafter *Ross*).

constraints. Compliance is monitored by the South African Information Regulator to ensure that sensitive consumer information does not fall into the wrong hands.⁵⁹ Furthermore, as with many of the statutory institutions, the Information Regulation is also hamstrung by the issue of resourcing. At the heart of budget proposals from South Africa's national treasury is an admission that the country's debt will never stabilise. Budgets and medium-term budgets in previous years, with one brief exception, repeatedly promised debt stabilisation even as previous years' promises were broken.⁶⁰

Nonetheless, the implementation of POPIA has started in earnest. Many companies have already overhauled their data privacy mechanisms, implementing measures such as cyber security. This has had a cost implication to many firms. Accordingly, many firms have to budget for this data reform processes, sacrificing other key needs.⁶¹

While POPIA creates new opportunities for data regulation, it also has key implications for the regulation of smart cities. This is especially important given the recent announcement by President Cyril Ramaphosa for the building of the Lanseria Smart City. This will be the first smart city in democratic South Africa based on "best practice" in urban sustainability and the principles underpinning the smart city"⁶². The city aims to advance urban sustainability beyond current planning, engineering, and urbanisation paradigms to more appropriate levels of sustainability and innovation. The city will be built surrounding the Lanseria International Airport, north of Johannesburg, in a project which is expected take around 25 years to complete.⁶³ Two other cities, namely the

⁵⁹ eNews Channel Africa 'SA Information Regulator battling to cope', available at <https://www.enca.com/news/sa-information-regulator-battling-cope> (accessed 7 October 2021).

⁶⁰ eNews Channel Africa 'Budget shows Treasury is short of ideas to fix SA's economic woes', available at <https://www.enca.com/analysis/budget-shows-treasury-short-ideas-fix-sas-economic-woes> (accessed 7 October 2021).

⁶¹ Daily Maverick 'Cybersecurity: South African companies are ripe for hackers', available at <https://www.dailymaverick.co.za/article/2021-08-01-cybersecurity-south-african-companies-are-ripe-for-hackers/>. (accessed 7 October 2021).

⁶² Business tech news '3 smart cities planned for South Africa' (hereafter "*3 Smart Cities planned for SA*") available at <https://businesstech.co.za/news/technology/477240/3-smart-cities-planned-for-south-africa/> (accessed 7 October 2021).

⁶³ Business tech news *3 Smart Cities planned for SA*.

Durban Aerotropolis and the Mooikloof Mega City are also planned.⁶⁴

It therefore becomes pertinent to explore how data privacy within these new cities will be navigated. The mini-thesis will consider a number of documents such as POPIA the Promotion of Access to Information Act (hereinafter "PAIA")⁶⁵, the Electronic Communications and Transactions Act (hereinafter the "ECTA")⁶⁶ and the National Credit Act (hereinafter the "NCA").⁶⁷

1.3 RESEARCH QUESTION

The central question to be considered in this mini-thesis is: What are the challenges and opportunities to data privacy in smart cities in the South African context?

1.4 RESEARCH OBJECTIVES

Answers to the following sub-inquiries will provide building blocks towards finding answers to the central research question:

- Determining possible privacy issues in smart cities;
- To ascertain the extent of the *sui generis* right to data privacy recognised and protected under the South African legal framework;
- To determine the principles of the PbD approach and its relation to the principle of accountability;
- Analyse Smart Privacy principles and its application as part of the South African smart city projects; and
- Recommend possible lessons that South Africa can learn from the regulatory frameworks (constitutional and statutory) for the protection of data privacy in EU and the US.

⁶⁴ Business tech news *3 Smart Cities planned for SA*.

⁶⁵ Act 2 of 2000.

⁶⁶ Act 25 of 2005.

⁶⁷ Act 32 of 2005.

1.5 BENEFITS OF THE STUDY

Privacy is the state of being unobserved by the public and can be defined as existing within an individual's truly private realm. When an individual leaves the inner sanctum of the private realm and enters the public realm, it becomes more difficult to protect the individual's privacy.⁶⁸ Due to a lack of regulation and data principles, personal information is easily accessible to anyone in the public domain, where it can be disseminated and exploited by multiple parties on a global scale.

It is critical, therefore, that the right to privacy and personal information be regulated and that this legal framework be constantly reassessed by courts considering technological advancements. This dissertation examines data protection laws in the EU and the US, focusing on what lessons can South Africa learn from the two jurisdictions within the smart city ecosystem. It is against this backdrop, this paper will be useful to academics, practitioners, lawmakers, students in the space of privacy and smart cities. Hopefully, it will illuminate key issues around smart cities as the government seeks to build and operationalise these cities.

1.6 METHODOLOGY

This is a desktop study that utilises both primary and secondary sources. In terms of primary sources, the mini-thesis considers legislation, case law and other international instruments. Secondary sources such as journal articles, textbooks, reports and internet sources are also canvassed. Given the purpose of the study, analytical and comparative research methodology are employed. Comparatively, two jurisdictions are employed. These are chosen because of the developments in these jurisdictions. The US was chosen because it is home to many of the world's technology 'giants,' including the mobile app ecosystem's dominant firms, Google, Apple, and Facebook. Due to the absence of a

⁶⁸ Davey R and Jansen LD *Social Media in the Workplace 1ed* (2017) 40.

federal privacy statute in the United States and the impossibility of comparing the position in all 50 states, two of the most influential US statutes, the COPPA⁶⁹ and the CCPA, have been chosen for comparison. CalOPPA is briefly mentioned in California, as are other pertinent federal statutes. On the other hand, The EU was chosen for a detailed comparative study because the GDPR is the most recent and comprehensive privacy regulation instrument, it has broad extra-territorial application and affects a large number of South African application developers, and European law contains extensive regulatory guidance and case law on data privacy.

1.7 LIMITATIONS AND DELIMITATIONS

- It is important to note that the study is limited by available data. Smart cities are a relatively new innovation and there is a dearth of information on the topic.
- While, ideally, it would have been appropriate to include an African comparator, there has not been a lot of developments on the continent in this regard. This is perhaps a gap for future studies.

1.8 LITERATURE REVIEW

Smart cities are a relatively new concept with considerable appeal for many governments. While the appeal of technologies in smart cities is understandable, and some of the enthusiasm for the contribution that technology can make to building better cities is entirely justified (e.g., open data, urban computing, integrated operations centres, RFID, sensors, and system integration offer limitless possibilities), many of the

⁶⁹ COPPA was chosen for in-depth examination because its novel provisions provide a useful model for comparing it to POPIA and formulating possible amendments. Additionally, there is a substantial body of literature, regulatory reports, and enforcement actions pertaining to COPPA. The state of California's online privacy laws were chosen because technology companies based in the United States, and specifically in the state of California, hold a dominant position in the field of mobile application development.

policies, approaches, discourses, and technologies that fall under the “smart” umbrella are yet to address social, ethical, and privacy concerns.⁷⁰

For the first time in an international legal instrument, a right to protection of an individual's private sphere against intrusion by others was enshrined in Article 12 of the United Nations Universal Declaration of Human Rights.⁷¹ The right to data protection is one of the rights guaranteed by Article 8 of the European Convention on Human Rights (ECHR)⁷² The right to personal data protection is included among the rights protected within the ambit of Article 8.⁷³ It guarantees the right to respect for private and family life, as well as for one's home and correspondence, and establishes the conditions under which this right may be restricted.

South Africa's Constitution is the supreme law of the country, and any conduct or law that conflicts with it is invalid.⁷⁴ The Bill of Rights, which is contained in Chapter 2 of the Constitution, contains the enshrined rights that apply to the executive, legislature, state organs, and natural and juristic persons.⁷⁵

The incorporation of fundamental rights into the Constitution strengthens their protection and elevates them to a higher status by virtue of their application to all law.⁷⁶ Thus, any law or action taken by the state, or an individual may be evaluated in light of an enshrined fundamental right. A limitation of a fundamental right may occur only if it complies with the requirements of section 36 of the Constitution's limitation of rights clause.⁷⁷

⁷⁰ Clavell GG (Not So) *Smart Cities - The societal drivers and impact of smart environments, Privacy and Emerging Sciences and Technologies* (2012) 40(6) *Oxford University Press* 27-28.

⁷¹ United Nations General Assembly, 'Universal Declaration of Human Rights' (10 December 1948), 217 A (III), available at <http://www.refworld.org/docid/3ae6b3712c.html> (accessed on 7 October 2021).

⁷² Council of Europe, 'The European Convention on Human Rights', ROME, 4 November 1950.

⁷³ Council of Europe, 'The European Convention on Human Rights', ROME, 4 November 1950.

⁷⁴ Section 2 of the Constitution.

⁷⁵ Section 8(1) and Sec 8(4) Constitution.

⁷⁶ *SALRC PDP Report 20 par (2011)*.

⁷⁷ *Section 36 of the Constitution* states that: "(1) The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom."

As a result of our Constitution's recognition of the right to privacy, the legislature and executive branch are prohibited from passing legislation or taking actions that infringe on or unreasonably limit the right to privacy. Additionally, Roos argues that the government is required to enact legislation to ensure an adequate level of data privacy protection where the common law is insufficient.⁷⁸ One could also argue that the government has a constitutional obligation to prioritise the enactment of the remaining provisions of the POPI Act, as it will become clear later in this study that the common law is woefully inadequate to protect data privacy in the context of personal information processing.⁷⁹ One cannot help but concur with Roos' assertion that South Africa lacks the "political will" to see the POPI Act through to completion.⁸⁰

Initially, it appears as though the Constitutional Court interpreted the constitutional right to privacy more restrictively (referred to as an informational right to privacy). In *Bernstein v Bester*,⁸¹ the Constitutional Court applied a more stringent definition of privacy, limiting it to a person's "inner sanctum" (e.g. family life, sexual preference and home environment). Ackermann J stated the following:⁸²

"Privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly."

Neethling argues that this concept is too narrow because it excludes other private facts about an individual that are also deserving of protection.⁸³ In *Hyundai Motor Distributors (Pty) Ltd v Serious Economic Offences and Others*,⁸⁴ the informational right to privacy

⁷⁸ Roos 2007 SALJ 423.

⁷⁹ Roos 2004 124(2) SALJ 433 PER 91.

⁸⁰ Roos 2004 124 (2) SALJ 433 PER 91.

⁸¹ Neethling J 'The concept of privacy in South African Law' (2005) 122 (1) SALJ 19 (hereafter *Neethling 2005 122 (1) SALJ*).

⁸² *Bernstein & Others v Bester & Others NNO 1996 (2) SA 751 at 789 par [A]*.

⁸³ Neethling 2005 122 (1) SALJ 20.

⁸⁴ *In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others 2001 (1) SA 545 (CC) 557 Par [16]*.

was interpreted to apply in instance where an individual has the ability to choose what information to disclose to the public and their reasonable expectation that such a choice will be respected.

A significant factor driving data into private silos is the absence of universal open or proprietary standards for data exchange. The EU is attempting to address this by funding efforts to develop interoperable protocols for private technology suppliers operating in smart cities, particularly in fields such as energy and, more broadly, IoT systems.⁸⁵

In the worst-case scenario, a smart city may devolve into a private data fiefdom for a monopolistic technology or telecommunications provider. Sadowski, an Arizona University researcher specialising in the future of cities, asserts that a paradigmatic example of a “top-down” smart city, Songdo in South Korea, “is as much a Cisco Systems city as it is a South Korean city, because Cisco Systems controls the majority of the contracts for the hardware and software that power it”⁸⁶. In the EU, these concerns, and uncertainties about who owns and how to control “big data”⁸⁷, and suppliers are also made aware of the issue as a potential source of contention for cities and citizens: for example, one industry speaker admitted that “what we do with the data we collect and who owns it are the central issues confronting smart cities”.⁸⁸

⁸⁵ See Ercim news available at <http://ercim-news.ercim.eu/en98/special/moving-towards-interoperable-internet-of-things-deployments-in-smart-cities>. (accessed 6 October 2021).

⁸⁶ Hieroglyph ‘Interview: Jonathan Sadowski on the Future of Cities’ (October 14 2014) available at <https://hieroglyph.asu.edu/2014/10/interview-jathan-sadowski-on-the-future-of-cities/> (accessed 7 October 2021).

⁸⁷ See EU EDPS ‘*Opinion on privacy and competitiveness in the age of big data*’ (26 March 2014); ICO (UK) ‘*Big data and data protection*’ July 2014; Article 29 EU Data Protection Working Party ‘*Statement on Big data*’, September 2014, 14/EN WP 221; ‘*Big Data and Smart Devices and Their Impact on our Privacy*’, n XX.

⁸⁸ Taylor V, head of M2M, quoted in Wright E and Devlin D ‘Smart Cities – Power to the Citizens? *Computers and Law*’ (16 April 2015) available at <http://www.bonddickinson.com/insights/publications-and-briefings/smart-cities-power-citizens> (accessed 7 October 2021).

As such, this mini-thesis echoes, but perhaps with greater concern, Goodman's⁸⁹ conclusion that all conceptions of smart cities share two characteristics: "They emphasise public-private partnerships and place information and communication technologies (ICT) at the heart of smart city operation."

The term "privacy by design" refers to a set of seven fundamental principles developed in the 1990s with the primary goal of aligning legal data protection principles with the technological goals of system developers.⁹⁰ Although the term was coined later by Dr Ann Cavoukian,⁹¹ the concept originated in a 1995 joint report of the Canadian and Dutch data protection authorities.⁹²

Privacy by design necessitates that developers take a proactive approach to privacy protection rather than reacting to data breaches.⁹³ Privacy must be set as the default. Privacy must be built into the technology's design.⁹⁴ Privacy settings must not jeopardise the technology's full functionality.⁹⁵ Security measures must safeguard data throughout its lifecycle.⁹⁶ There must be visibility and transparency regarding data practises, as well as respect for user privacy.⁹⁷

⁸⁹ See De Bonis R & Vinciarelli E 'From Smart Metering to Smart City Infrastructure. Could the AMI Become the Backbone of the Smart City?' (2014):The Third International Conference on Smart Systems, Devices and Technologies 3 available at <https://www.mdpi.com/1996-1073/14/14/4310/htm>. (accessed 9 October 2021).

⁹⁰ Cavoukian, 'Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices' (2011) at 2 (hereafter "*The Roadmap for Privacy by Design*") available at <https://www.ipc.on.ca/wpcontent/uploads/resources/7foundationalprinciples.pdf> (accessed 9 October 2021).

⁹¹ Cavoukian A, 'Privacy by Design The 7 Foundational Principles' (2011) 5.

⁹² Information and Privacy Commissioner Ontario Canada and Registratiekamer: The Netherlands, 'Privacy Enhancing Technologies: The Path to Anonymity' (1995) (volume 1) 2.

⁹³ Cavoukian, 'Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices' (2011) 7.

⁹⁴ Cavoukian A 'Privacy by Design The 7 Foundational Principles' (2011) 2-3.

⁹⁵ Cavoukian A 'Privacy by Design The 7 Foundational Principles' (2011) 3-4.

⁹⁶ Cavoukian A 'Privacy by Design The 7 Foundational Principles' (2011) 4.

⁹⁷ Cavoukian A 'Privacy by Design and the Emerging Personal Data' (2012) 16.

1.9 OVERVIEW OF THE STUDY

This mini-thesis comprises of seven chapters including this introductory chapter.

CHAPTER 2: CONCEPTUAL FRAMEWORK: THE DATA PRIVACY PRINCIPLES AND PRIVACY BY DESIGN

This chapter will consist of significant terminologies and data processing practices used within the smart city ecosystem. It will further conduct analysis of privacy issues related to technologies that are used in smart cities, and thus answer the first research sub question. This chapter will further provide analysis of implementation of the concept of Smart Privacy as well as solutions regarding technologies implemented in smart cities through different stages in order to answer the third research sub question.

CHAPTER 3: INTERNATIONAL FRAMEWORK

This chapter will examine the international framework and international instruments such as the International Covenant on Civil and Political Rights (ICCPR) and other relevant conventions such as the African Charter on Human and People's Rights (ACHPR), the United Nations (UN) sustainable development goals and the Agenda 2063.

CHAPTER 4: THE DATA PROTECTION LEGAL FRAMEWORK OF SOUTH AFRICA

This chapter will examine the current and past South African legal framework on data privacy.

CHAPTER 5: COMPARATIVE PERSPECTIVES

This chapter discusses a comparative perspective on smart data privacy principles between the EU and the US.

CHAPTER 6: AN IDEAL FRAMEWORK FOR SMART CITIES IN SOUTH AFRICA

This chapter will provide ideal principles and an ideal framework for the regulation of smart cities in South Africa. This model can potentially be an export model for other countries too.

CHAPTER 7: RECOMMENDATIONS AND CONCLUSION

This chapter will conclude and provide recommendations.



CHAPTER 2

CONCEPTUAL FRAMEWORK: THE DATA PRIVACY PRINCIPLES AND PRIVACY BY DESIGN

2.1 INTRODUCTION

The human population is increasing, and by 2030, it is estimated that 4 billion people will live in cities worldwide.⁹⁸ Therefore, it has become pertinent to address the type of privacy regulation that would be judged appropriately in light of current challenges surrounding smart cities and the massive number of existing smart gadgets.⁹⁹ The term “smart cities”¹⁰⁰ has become the most widely used formulation for the future city.¹⁰¹ Accordingly, the concept of smart cities is rapidly gaining global recognition, replacing and sometimes coexisting with the previously understood formulations of cities.¹⁰² For instance, it could be argued that the term “smart city” has supplanted the concepts such as “sustainable city” and “digital city”¹⁰³ as the preferred term to refer to ICT-driven urban innovation, as well as new modes of governance and urban citizenship.¹⁰⁴

This chapter will establish fundamental concepts, outline the stakeholders in the smart city ecosystem, and define critical data processing concepts and procedures.¹⁰⁵ The chapter will further discuss privacy concerns that are somewhat common with smart city

⁹⁸ United Nations Population Fund, ‘State of World Population 2007: Unleashing the Potential of Urban Growth’, available at <http://www.unfpa.org> (accessed on 5 October 2021).

⁹⁹ United Nations Department of Economic and Social Affairs ‘World Urbanization Prospects: The 2014 Revision, Highlights, United Nations, Department of Economic and Social Affairs, Population Division’ available at <http://esa.un.org/unpd/wup/Highlights/WUP2014-Highlights.pdf>. (accessed 5 October 2021).

¹⁰⁰ Moir E *Future Cities* 5.

¹⁰¹ Moir E *Future Cities* 7.

¹⁰² Moir E *Future Cities* 9.

¹⁰³ Moir E *Future Cities* 21.

¹⁰⁴ Moir E *Future Cities* 33.

¹⁰⁵ The explanations and definitions are derived from scholarly sources, industry documents, and are cross-referenced to applicable statutory terminology. The purpose of this chapter is to provide an overview of significant terms.

technologies and will attempt to address the first research sub question. Not all possible concerns will be discussed in view of length constraints, rather, only a few that the author considered particularly fascinating will be examined in further detail.

2.2 TERMINOLOGIES, KEY REFERENCES AND DEFINITIONS

A “data processor” is a term that refers to a third party that processes personal data on the controller's behalf.¹⁰⁶ The term “personal information”¹⁰⁷ is used in place of “personal data” and “responsible party”¹⁰⁸ is used in place of “data controller”. The term “operator”¹⁰⁹ is used in place of ‘data processor’. However, these phrases have the same fundamental meaning as those mentioned previously. While the international instruments addressed below refer to “principles” of data privacy that must be followed when processing personal data whereas the POPI Act refers to “conditions for lawful processing”.¹¹⁰

¹⁰⁶ Neethling *Law of Personality* (2005) 276. Cf Roos *Core principles of data protection law* (2006) CILSA 104.

¹⁰⁷ ‘Personal information’ in Section 1 of POPIA is defined as: information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to-

- (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- (b) information relating to the education or the medical, financial, criminal or employment history of the person;
- (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- (d) the biometric information of the person; and
- (e) the personal opinions, views or preferences of the person.

¹⁰⁸ ‘Responsible party’ in terms of section 1 of POPIA is defined as: “a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.”

¹⁰⁹ The ‘operator’ in terms of section 1 of POPIA is defined as: “a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.”

¹¹⁰ Chapter 3 of POPIA.

2.2.1 Smart cities

In the early 1990s, cities began labeling themselves as “smart” upon adopting Information and Communication Technology (ICT) infrastructure, embracing e-governance, and aiming to recruit high-tech firms to stimulate economic growth.¹¹¹ The conception of the smart city concept may be traced back to North American “smart growth” theories of the 1990s, which were a community-driven response to alleviate traffic congestion, air pollution, etc. through improved development practices.¹¹² A connection has also been drawn between the adoption of smart cities and the 2005 ratification of the Kyoto Protocol, which was a global commitment by world leaders to limit and reduce greenhouse gas emissions in accordance with predetermined targets.¹¹³

In 1997, the World Forum on Smart Cities anticipated that around 50 000 cities throughout the world will initiate smart city initiatives within a decade.¹¹⁴ Amsterdam, Bangalore, Barcelona, Birmingham, Chicago, Hong Kong, Copenhagen, Seoul, Shanghai, Shenzhen and Vienna are well-known and famous cities from the first two decades of the 21st century. Concerns were expressed, however, regarding the widespread adoption of the smart cities concept.¹¹⁵ For example, Hollands criticised the smart cities movement for its “definitional imprecision”, “many unstated assumptions”, and “self-congratulatory” nature.¹¹⁶ With the large-scale entry of big IT corporations into the industry in 2005, the worldwide discourse on smart cities changed substantially.¹¹⁷ By the 21st century, governments, particularly municipalities, were seen as an unexplored market for companies offering so-called urban technologies.¹¹⁸ For example, in 2011, Vienna,

¹¹¹ Hollands RG ‘Will the real smart city please stand up?’ (2008)12(3) *City* 303-320 (hereafter “*Smart city*”).

¹¹² Hollands RG *Smart city* 307.

¹¹³ Cocchia A ‘Smart City How to Create Public and Economic Value with High Technology in Urban Space’ (2014) 7(3) *Springer* 13-43 2014 7(3) *Springer* 13-43 (hereafter “*Smart City*”).

¹¹⁴ Hollands *Smart city* 305.

¹¹⁵ Hollands *Smart city* 309.

¹¹⁶ Hollands *Smart city* 320.

¹¹⁷ Cocchia *Smart City* 43.

¹¹⁸ Townsend AM ‘Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia’ (2013) *3WW Norton & Company* 1-14 (hereafter: “*Smart Cities: Big Data, Civic Hackers, and the*

Austria's capital, began planning towards sustainability.¹¹⁹ In 2019, Vienna's administration adopted a strategy to make the city more livable by reducing CO2 emissions and energy use planned until 2050.¹²⁰ To realise these goals, different projects in the city applications are developed for example, like traffic lights that automatically detect pedestrians or drones that monitor PV systems and wind parks being designed to achieve these goals.¹²¹

There is presently no universally recognised definition of a "smart city", and much relies on who provides the characteristics: industry, legislators, civil society, and citizens or users are four immediately and plainly distinct stakeholder groups.¹²² According to Kitchin, there the term "smart city" can be classified in to two categories which can be used in conjunction with one another to describe why a city is considered "smart".¹²³ The first category refers to the extent to which smart cities are claimed to link people, data, objects, and processes within a dynamic global infrastructure.¹²⁴ The second category is the extent to which smart cities then utilise this networked infrastructure to increase economic, resource, and political efficiency while allowing for social, cultural, and urban development.¹²⁵

The collection and processing of personal data is not a problem in and of itself; however, it raises data vulnerability, threatens its security, may infringe on the right to privacy, and

-
- Quest for a New Utopia").*
- 119 Stadt Wien –'Smart City – Historie', available at: <https://smartcity.wien.gv.at/site/der-wiener-weg/historie/> (accessed 9 September 2022) (hereafter " Smart City.")
- 120 Stadt Wien *Smart City*.
- 121 Stadt Wien *Smart City*.
- 122 De Santis R *et al*'Smart city: fact and fiction' (2014), Paper No. 54536 2014) *Munich Personal RePEc Archive* 3-6.
- 123 See Kitchin R, 'the programmable city' available at <http://progcity.maynoothuniversity.ie/contributors/rob-kitchin/>. (accessed 19 October 2021).
- 124 De Bonis R and Vinciarelli E 'From Smart Metering to Smart City Infrastructure. Could the AMI Become the Backbone of the Smart City?', *Smart 2014: The Third International Conference on Smart Systems, Devices and Technologies*' (2014) 2.
- 125 United Nations, Bureau International des Expositions, Shanghai 2010 World Exposition Executive Committee 'Shanghai Manual – A Guide for Sustainable Urban Development of the 21st Century', (2010), Chapter 8.

undermines the confidence of the data subject, particularly in online transactions.¹²⁶ As Bygrave and Clarke describe, this new trend in the use and sharing of personal data has heightened concerns about individual privacy and the security of personal data, which have been exacerbated by technological and organisational advances in the processing of personal data.¹²⁷

This concept also clarifies the role of mobile computing (e.g. smartphones) in citizens' interactions with the city and government on the one hand, and in citizens' generation of personal data such as identity, activity, and location on the other.¹²⁸ Cities and their infrastructure are already the most complex structures ever created by humans; combining them with equally complex smart cities solutions, which rely on wireless sensor networks and integrated communications systems, makes them extremely susceptible to power failure, software errors, and cyberattacks.¹²⁹

Load shedding, like corruption, is an unfortunate aspect of the lives of many South Africans¹³⁰. Neves asserts that South Africa has been plagued by load reduction for the past 14 years.¹³¹ In a cabinet reshuffle on 6 March 2023, South African President Cyril Ramaphosa appointed Kgosientsho Ramokgopa as the head of newly formed Ministry of Electricity. ¹³²In his announcement on changes to the national executive, the President

¹²⁶ Lee DJ *et al* 'Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection', (2011) 35(2), *MIS Quarterly* 423-444.

¹²⁷ Clarke R 'Information Technology and Dataveillance' (1988) 31(5) *Communications of ACM* 505-508.

¹²⁸ Kitchin R *Smart Urbanisation* (2014) 79(1) *GEOJ* 2.

¹²⁹ Townsend *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia* (2013) 3-5.

¹³⁰ Neves J 'Load shedding: It can be stopped, says Chris Yelland-here's how' *Biznews* 7 June 2021. <https://www.biznews.com/global-citizen/2021/06/07/load-shedding-stopped-yelland> (accessed 21 May 2022).

¹³¹ Neves J 'Dark History: The real reasons behind load shedding in South Africa' *Biznews* 21 July 2021 <https://www.biznews.com/energy/2021/07/05/load-shedding-sa-history>. (accessed 21 May 2022).

¹³² Energy Capital Power 'Ramaphosa names his electricity minister, Paul Mashatile becomes new deputy president' (hereafter "Loadshedding") 7 March 2023 available at <https://energycapitalpower.com/south-africa-minister-electricity-appointed/> (accessed 17 March 2023).

said the new Minister of Electricity would address the immediate load shedding crisis and reduce its severity in the coming months.¹³³

The Smart Cities Framework (SCF) should be evaluated in light of a variety of South African acts, policies, frameworks, and initiatives affecting human settlements. Efforts to improve South African human settlements are guided by international objectives and agendas.¹³⁴ As discussed in Chapter 3, in accordance with Transforming our World: the 2030 Agenda for Sustainable Development, member states of the United Nations have been required to formulate their agendas and political programs for the next 15 years.¹³⁵ Furthermore, Agenda 2063 - The Africa We Want specifies several goals.¹³⁶

2.2.2 Mobile applications

The word mobile application (or app) refers to a piece of software that runs on mobile wireless devices such as tablets, smartwatches and smartphones.¹³⁷ Through an application processing interface, the mobile app can communicate directly with the device's hardware and operating system (API).¹³⁸ In this dissertation, the term "mobile app" is used generally to refer to all apps, independent of their installation technique, type, or category. In terms of the Electronic Communications and Transactions Act 25 of 2002 (ECTA), a mobile application is an "electronic agent" capable of beginning the collection and subsequent processing of personal information without requiring direct human participation (it serves as an 'automated transaction').¹³⁹ Hence, the study is

¹³³ Energy Capital Power *Loadshedding* (2023).

¹³⁴ Refer to Chapter 3, paragraph 3.7 above for a discussion on SCF, Agenda 2030 and Agenda 2063.

¹³⁵ Refer to Chapter 3, paragraph 3.7.2 above for a discussion on SCF and Agenda 2030.

¹³⁶ Refer to Chapter 3, paragraph 3.7.3 above for a discussion on SCF and Agenda 2063.

¹³⁷ International Telecommunications Union Standardisation Sector (ITU-T).

¹³⁸ Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices* (WP 202, 27 February 2013) 4.

¹³⁹ See section 1 of ECTA: " 'automated transaction' means an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment."

primarily concerned with the legal accountability of those parties, not with the legal role of the mobile app.

2.2.3 Data

Data in natural language refers to facts stated that can be deduced or inferred from others. In Information Processing and Computer Science it refers to signs or symbols, used primarily for communication and processing in computer systems, that typically but not always represent information, agreed facts, or assumed knowledge; and are expressed using agreed characters, codes, syntax, and structure.¹⁴⁰ When using the phrase “data” in a legal context, caution should be exercised as in this sense, “data” and ‘information’ are equivalent, whereas “personal data” and ‘personal information’ refer to data that uniquely identifies an individual (or from which an individual can be identified).¹⁴¹

2.2.4 Big data

Big data, like smart cities, is a buzzword that is frequently used without a distinct definition.¹⁴² McDermott states in her article “*Conceptualising the right to data protection in an era of Big Data*”¹⁴³ that Big Data is notoriously difficult to define, but a number of key characteristics of Big Data have been identified, including: the enormous volume of data, the speed at which it is collected, the variety of data, its relational nature (allowing links to be made to other data sets), and potentially ephemeral nature.¹⁴⁴ For instance,

¹⁴⁰ Checkland P and Holwell S ‘Data, capta, information and knowledge’ in Matthew Hinton (ed), *Introducing Information Management* (Routledge 2006) 48, quoting Maddison R (ed), *Information Systems Development for Managers* (Paradigm 1989) 174.

¹⁴¹ Art 4(1) of GDPR.

¹⁴² See Smart Cities Council ‘Smart cities Financing Guide’ (August 24, 2015) available at <http://smartcitiescouncil.com/resources/smart-cities-financing-guide> (accessed on 18 June 2023).

¹⁴³ McDermott Y ‘Conceptualising the right to data protection in an era of Big Data, Big Data and Society’ (2017) 1 79 (hereafter “*right to data protection*”).

¹⁴⁴ McDermott Y *right to data protection* 80.

data is collected from a variety of sources, including mobile banking transactions, tweets, satellite images, online queries, and online purchase information.¹⁴⁵

Big data is synonymous with smart applications, which provide a rich stream of data and are supported by robust mobile cloud computing solutions that provide the storage and processing capacity required to execute complicated analytics.¹⁴⁶ Big data is considered to be in violation of data privacy rules because data obtained for a certain purpose is processed for an unrelated purpose without the authorisation of the individual to whom the data pertains.¹⁴⁷

Regulators are beginning to address the ramifications of big data, such as the legal and ethical difficulties created by tracking technologies and behavioral profiling based on the obtained personal information.¹⁴⁸ For Instance, in Europe, Article 29 Working Party emphasised the concerns in its February 2013 decision on apps on smart devices, in which it acknowledged that apps can access significantly more information than a regular web browser.¹⁴⁹

In South Africa, the Constitution protects the right to privacy, not the right to personal information protection.¹⁵⁰ This is an essential distinction given the growing concentration of data in the hands of governments and commercial firms that control technological monitoring techniques.¹⁵¹ Nonetheless, in all three jurisdictions, ubiquitous tracking, profiling, data matching, and targeted advertising are acknowledged to be an intrusion

¹⁴⁵ See D Van der Merwe et al *Information Communications Technology Law* 2ed (2016) 366.

¹⁴⁶ Hashem IAT *et al* 'The Rise of "Big Data" on Cloud Computing: Review and Open Research Issues' (2015) 47 *Information Systems* 100–102.

¹⁴⁷ Van der Merwe D *et al* *Information Communications Technology Law* 2ed (2016) 366.

¹⁴⁸ Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising* (WP 171, 22 June 2010) 6–7.

¹⁴⁹ See footnote 23 above. Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices* (WP 202) 27 (2013) 5.

¹⁵⁰ *NM and others v Smith and others (Freedom of Expression Institute as amicus curiae)* 2007 (5) SA 250 (CC) 32 (hereafter "*NM and others v Smith and others*").

¹⁵¹ Duncan J, *Stopping the Spies: Constructing and resisting the surveillance state in South Africa* (2018) 5.

into the personal sphere and a violation of the right to enjoy privacy to which each individual is entitled.¹⁵²

2.2.5 The Internet of Things

The Internet of Things (IoT) refers to the embedding of sensors and mechanisms in common everyday objects such as refrigerators, cars, especially autonomous vehicles, roads, pacemakers, and watches that collect and store information, and also enable the information to be wirelessly transmitted to other objects or machines, typically via the Internet. All of this information is combined to generate what is roughly referred to as “big data”.¹⁵³ The Pew Research Center¹⁵⁴ defines the IoT as a global, immersive, invisible, ambient networked computing environment created through the continued proliferation of smart sensors, cameras, software, databases, and massive data centers in a global information fabric. For example, to analyse data and develop IoT prototypes, the University of Guadalajara created a Living Lab. This Smart City Living Lab demonstrates scalability, modularity, and security.¹⁵⁵

The IoT systems such as smart ambient lighting in a living room or smart thermostats like NEST¹⁵⁶, are frequently designed to be contextually aware of the user's requirements and desires. They are also designed for collecting data about their daily practices and routines while remaining invisible in use and unremarkable to users.¹⁵⁷ In contrast, while consumers may have had the opportunity to read the privacy policy of their Nest

¹⁵² *Khumalo and others v Holomisa* 2002 (5) SA 401 (CC) at 419. Also see Warren S and Brandeis L 'The Right to Privacy' (1890) 4 *Harvard LR* 193–220.

¹⁵³ Perry JS 'What is Big Data? More than Volume, Velocity and Variety, IBM Developer Blog' (2017). available at <https://developer.ibm.com/blogs/what-is-big-data-more-than-volume-velocity-and-variety/>. (accessed 17 July 2022).

¹⁵⁴ See general discussion in Lilian E and Waelde C eds *Law and the Internet* (2009) chs14, 15 and 16.

¹⁵⁵ See Villanueva-Rosales N et al 'Semantic-enhanced Living Labs for better interoperability of Smart Cities solutions' (2016) IEEE International Smart Cities Conference (ISC2), *IEEE*. 1-7.

¹⁵⁶ Ars technica 'What Google can really do with Nest, or really, Nest's data' available at <http://arstechnica.com/business/2014/01/what-google-can-really-do-with-nest-or-really-nests-data/> (accessed 5 September 2022).

¹⁵⁷ Tolmie P *et al* 'Unremarkable computing Proc' (2002) 2 *CHI* 399-406.

thermostat before signing the contract, they will have no such opportunity when their data is collected by the smart road or smart tram they travel on to work, or when they pass the smart dustbin¹⁵⁸ on the street. For example, the city of Singapore uses sensors to detect smokers in prohibited areas and other sensors detect trash thrown out of high-rise windows.¹⁵⁹

2.2.6 Data breaches

The GDPR defines a “personal data breach” as a security breach that results in the accidental or unlawful destruction, loss, modification, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.¹⁶⁰ A data breach occurs when hackers take advantage of lax security measures to gain access to a network and the personal information stored or communicated on it.¹⁶¹ Recent incidents of data breaches involving Facebook¹⁶² and Liberty¹⁶³ have heightened public awareness of the possible impact on consumer privacy, despite the fact that statutory policies¹⁶⁴ and breach notification requirements varied.¹⁶⁵

¹⁵⁸ See British Broadcasting Corporation (hereafter “BBC”) ‘City of London calls halt to smartphone tracking bins’, *BBC News*, 12 August 2013.

¹⁵⁹ IoT World Today – ‘The World’s 5 Smartest Cities’, available at <https://www.iotworldtoday.com/2016/05/18/world-s-5-smartest-cities/>, (accessed 13 September 2022).

¹⁶⁰ See footnote 26. Article 4(12) of the GDPR.

¹⁶¹ Sec 5 of the *Federal Trade Commission Act* of 1914, 15 U.S.C. §§ 41–58 (2018) (FTCA) empowers the commission to investigate unfair and deceptive trade practices.

¹⁶² Isaac M and Frenkel S ‘Facebook Security Breach Exposes Accounts of 50 Million Users’ *NY Times* 28 September 2018 available at <https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html> (accessed 3 November 2021).

¹⁶³ Nieselow T ‘Five Massive Data Breaches Affecting South Africans’ *Mail & Guardian* 19 June 2018 available at <https://mg.co.za/article/2018-06-19-five-massive-data-breaches-affecting-south-africans/> (accessed 3 November 2021).

¹⁶⁴ ‘Security compromises’ in terms of section 21(2) and in section 22(1) of POPIA requires an operator to notify the appropriate party immediately upon discovering a security breach.

¹⁶⁵ See generally Federal Trade Commission, *Data Breach Response: A Guide for Business* (May 2019).

2.2.7 Profiling and Information matching

With individuals carrying smartphones everywhere and sharing their lives on social media, we are already seeing a growing penetration into people's private and public lives by technology that enables data gathering and the associated identification, monitoring, and profiling.¹⁶⁶ Profiling is the automatic evaluation of a user's characteristics. For instance, making predictions about their behavior, and targeting them with interest-based advertising.¹⁶⁷ Profiling is therefore distinct from information-matching systems, which involve comparing several records having references to various data subjects.¹⁶⁸

2.2.8 The cloud and cyber attacks

Cloud computing is defined as a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using internet technologies.¹⁶⁹ Van der Merwe is of the view that a cloud computing service provider can offer several customers on-demand services such as data storage space and software applications.¹⁷⁰ In other words, instead of storing data and software on a user's hard drive, it is now saved on multiple servers that can be placed anywhere in the globe and accessed via the Internet as necessary.¹⁷¹

¹⁶⁶ Radomirovic S 'Towards a model for security and privacy in the internet of things, 1st International, Security Comm. Networks' (2014) 7 *John Wiley & Sons, Ltd* 1–487.

¹⁶⁷ Article 4(4) of GDPR defines 'profiling' as 'any automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person' While the phrase is not defined in POPIA, it is used in the same manner in *section 71*.

¹⁶⁸ POPIA section 1 defines 'information matching' as the comparison of any document containing personal information about ten or more data subjects with one or more documents containing personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action regarding an identifiable data subject.

¹⁶⁹ See 'Gartner Glossary' available at <https://www.gartner.com/en/information-technology/glossary/cloud-Computing>. accessed on 11 July 2019.

¹⁷⁰ Van der Merwe D et al *Information Communications Technology Law* 3ed (2016) 365 (hereafter "*Information Communications Technology Law*").

¹⁷¹ Van der Merwe D *Information Communications Technology Law* 366.

Burdon explains in his book *'Digital Data Collection and Information Privacy Law'* how smart devices impact our lives.¹⁷² Our civilisations are becoming increasingly filled with the smart devices that constitute the "Internet of Things".¹⁷³ As we develop smart structures such as the smart home, store, and workplace, the sensorisation of environmental environments is accelerating. ¹⁷⁴ For example, New York city has a population of approximately 8.5 million inhabitants, automatic water meter reading technology aids homeowners and administrators track water use.¹⁷⁵

The risk of hackers, bugs, and blunders could emerge in sophisticated transportation, e-health, surveillance, and governance systems. What happens in the instance where an entire smart city operating system malfunctions?¹⁷⁶ For example: (1) driverless automobiles may crash, (2) flaws may bring the entire energy infrastructure down, (3) the entire smart city operating system may be subjected to DDOS attacks, and (4) drones may strike passenger flights.¹⁷⁷

Therefore, the blanket constitutional privacy rights and the pre-existing regulations are deemed inadequate and inappropriate for addressing the complexities of privacy issues generated by these advances.¹⁷⁸ The law of tort, common law principles of the law of trust, and contractual obligations are no longer suitable for addressing such difficulties with a negative impact on individual privacy.¹⁷⁹ According to commentators such as Makulilo,¹⁸⁰ this is the beginning of the contemporary understanding of data protection.

¹⁷² Burdon M *Digital data collection and information privacy law*, 1ed (2020) 14 (hereafter "*information privacy law*").

¹⁷³ Burdon M *Information privacy law* 15.

¹⁷⁴ Burdon M *Information privacy law* 16.

¹⁷⁵ Technology magazine – 'Top 10 smart cities in the world [Online],' available at: <https://www.gigabitmagazine.com/big-data/top-10-smart-cities-world>, (accessed 19 September 2022).

¹⁷⁶ BBC 'Heathrow plane in near miss with drone' (hereafter "*Heathrow drone*") available at <http://www.bbc.com/news/uk-30369701> (accessed 5 November 2021).

¹⁷⁷ BBC *Heathrow drone*.

¹⁷⁸ Warren SD and Brandeis LS 'The Right to Privacy, 1890,4 (5) *HLR* 193-220 (hereafter "*Right to Privacy*").

¹⁷⁹ Warren SD and Brandeis LS *Right to Privacy* 198-199.

¹⁸⁰ Makulilo AB *Protection of Personal Data in Sub-Sahara Africa* (published PhD thesis, Universität Bremen, 2012) 1.

Bygrave¹⁸¹ defends this on the grounds that privacy and data protection law is the outcome of pre-existing laws, the most obvious of which are the rules on the right to privacy and protection of personality, as well as the rules on defamation proposed by Warren and Brandeis.

2.2.9 Ubiquitous Surveillance

Human beings tend to believe that technology is capable of resolving all of their problems, from environmental concerns and traffic congestion to sustainable energy usage and trash management. This faith in technology and desire for simple solutions has resulted in an expanded and frequently indiscriminate use of technology across all spheres of administration.¹⁸²

A case in point has been police and law enforcement's widespread use of surveillance technologies such as CCTV, databases, data mining, biometrics, and body scanners.¹⁸³ Thus, surveillance has evolved from systems for monitoring convicts and other undesirables to pervasive systems that employ a diverse array of technologies for altering social behavior and, as a result, affecting social values, most notably privacy.¹⁸⁴

The European Court of Human Rights (EctHR) establishes strong limits on digital surveillance in the case *Liberty v. United Kingdom*.¹⁸⁵ In this case, it was held that the UK government's mass surveillance system, which spied on all telephone calls, faxes, and emails to and from Ireland, violated Article 8 of the ECHR. Relevant domestic law did not

¹⁸¹ Bygrave *Data Privacy Law: An International Perspective* 9.

¹⁸² Van Brakel R and De Hert P 'Surveillance and law in a pre-crime society: Understanding the consequences of technology-based strategies' (hereafter "*Surveillance and law*") (2011) 3 *VUB* 163-192.

¹⁸³ Van Brakel R and De Hert P *Surveillance and law* (2011) 3 *VUB* 164.

¹⁸⁴ Wright D et al 'Sorting Our Smart Surveillance' (2010) 4 (26) *CLSR* 5.

¹⁸⁵ *Liberty v the United Kingdom* (hereafter "*Liberty v the United Kingdom*") application no. 58243/00, judgement of 1 July 2008 para 58.

clearly spell out the manner of intercepting and examining external communications neither did it provide adequate legal protection against power abuse.¹⁸⁶

Additionally, the European Convention on Human Rights requires that a rights-restricting proposal must have a legal basis and adhere to the proportionality rule.¹⁸⁷ It further rejects any intrusion on privacy that is not justified as essential in a democratic society.¹⁸⁸ Therefore, surveillance that is ubiquitous in smart cities may be considered unnecessary in a democratic society if it is carried out without a clear lawful purpose.¹⁸⁹

2.3 DATA PROTECTION BY PRIVACY BY DEFAULT

Article 23 of the Proposed Regulation establishes Privacy by Default by stating that:

“The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.”¹⁹⁰

The EU Regulation establishes two ideas for data privacy: data privacy by design and data privacy by default.¹⁹¹ The former requires that data protection is integrated into products and services from the start, while the latter requires that privacy-friendly default settings are the standard, for example on social networks.¹⁹² Article 8 (b) of the Modernisation Proposal, as mentioned above, contains a similar provision to the data

¹⁸⁶ *Liberty v the United Kingdom* para 59.

¹⁸⁷ Art 5 Modernisation Proposal.

¹⁸⁸ Article 8 of the ECHR.

¹⁸⁹ Van Brakel R and De Hert P *Surveillance and law* (2011) 3 *VUB* 6.

¹⁹⁰ Cavoukian A and Prosch M *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users' Privacy by Design* Research Lab, Information and Privacy Commissioner, Ontario, Canada, December (2010) (hereafter "*Roadmap for Privacy by Design*") 8.

¹⁹¹ Art 23 EU Regulation and the Electronic Communications Act.

¹⁹² Art 23 EU Regulation and the Electronic Communications Act.

protection by design principle, requiring the data controller to "... design data processing operations in such a way as to avoid or at the very least minimize the risk of interfering with those rights and fundamental freedoms."¹⁹³

2.4 PRIVACY BY DESIGN

Article 23¹⁹⁴ states:

"Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."¹⁹⁵

This provision encapsulates the essence of Privacy by Design, which is anticipating and resolving privacy issues in a positive-sum manner prior to them becoming problems.¹⁹⁶

The term "Privacy by Design" (PbD) dates back to October 2010 when Ann Cavoukian, a Canadian Information and Privacy Commissioner, introduced a PbD resolution at the International Conference of Data Protection and Privacy Commissioners in Jerusalem. Ever since, the resolution was adopted unanimously by privacy regulators worldwide, PbD has become an important fundamental component of data protection law.¹⁹⁷ As a relatively new concept, PbD has enormous potential for enhancing accountability, security, and individual rights.¹⁹⁸

¹⁹³ Article 8 (b) of the Modernisation Proposal.

¹⁹⁴ Art 23 EU Regulation & the Electronic Communications Act.

¹⁹⁵ Cavoukian A and Prosch M *Roadmap for Privacy by Design* 8.

¹⁹⁶ Cavoukian A and Prosch M *Roadmap for Privacy by Design* 9.

¹⁹⁷ Cavoukian A 'Ph.D Comments on the European Commission's Comprehensive Approach on personal Data Protection in the EU' 2011 2 (hereafter "Approach on personal Data Protection").

¹⁹⁸ Cavoukian A 'Approach on personal Data Protection' 2.

Rather than a single idea or notion, PbD is a collection of seven guiding concepts or principles that provide a holistic and proactive approach to privacy.¹⁹⁹ PbD principles are universal in nature; as the consultation paper states, they may be applied to technologies, corporate information systems, and processes, as well as to information eco-systems, meta-structures, and even to regulatory and oversight systems.²⁰⁰ The following are the stated principles²⁰¹:

- a) The PbD strategy is proactive rather than reactive; it anticipates and prevents privacy-invading events before they occur.
- b) PbD strives to ensure the highest level of privacy possible by guaranteeing that personal data is safeguarded automatically in any given IT system. Thus, no action on the part of the individual is required to safeguard their privacy; it is built-in by default;
- c) Without jeopardising functioning, privacy is built into the system;
- d) PbD dispels erroneous dichotomies such as privacy vs. security by demonstrating that both can exist concurrently;
- e) PbD is integrated into the system prior to the first piece of information being collected and extends securely throughout the data's lifecycle - solid security measures are critical for privacy from start to finish;
- f) PbD strives to reassure all stakeholders that, regardless of the business practice or technology used, it is actually running in accordance with the stated promises and objectives, subject to independent verification;
- g) Above all, PbD demands architects and operators to prioritise the individual's interests by implementing strong privacy defaults, providing sufficient notification, and empowering users with user-friendly options.²⁰²

After enumerating all pertinent PbD principles, we ascertain that the consequences of technology are difficult to forecast in advance, some effort must be taken from the start

¹⁹⁹ Cavoukian A *Approach on personal Data Protection* 4.

²⁰⁰ Cavoukian A *Approach on personal Data Protection* 4.

²⁰¹ Cavoukian A *Approach on personal Data Protection* 7.

²⁰² Cavoukian A and Prosch M *The Roadmap for Privacy by Design* 9.

of the project, as problems that arise later are difficult and expensive to resolve. A good example of this type of collaboration is the project “Safeguarding Data Protection in an Open Data World”, a collaboration between Delft University of Technology and Tilburg University, which recognised that an imbalance between open data and data protection regulations could stymie the development and implementation of smart cities and thus enlisted a legal researcher to work alongside engineers and designers to develop effective co-design processes.²⁰³

2.5 CONCLUSION

This chapter defined essential ideas and data processing processes within the smart city ecosystem. Despite significant academic and media concern about privacy issues, we only have a “rudimentary” understanding of how personal information is acquired and handled.²⁰⁴ It is critical to consider both the positive and negative implications of each technology used in a smart city in order to ensure transparency and trust striking a balance between the smart city and its residents.²⁰⁵

This chapter further analysed the concept and principles of PbD. Despite authorities having recognised PbD as an important notion, a PbD approach requires explicit articulation in terms of both legally enforceable requirements and software development objectives. This chapter has established that two ideas, namely data minimisation and accountability, are at the core of an effective PbD strategy. To achieve Pb(re)D in the present, complex smart city environment, a comprehensive understanding of the legal principles of data minimisation and accountability is essential. These principles will be addressed in the country-specific chapters that follow, together with the definitions of essential concepts in those jurisdictions, namely: personal information, the responsible

²⁰³ See for general discussion Cavoukian A ‘Privacy by Design The 7 Foundational Principles’ (2011) 2-3.

²⁰⁴ See general discussion in Yabing Liu *et al* ‘Identifying Personal Information in Internet Traffic’ in *Proceedings of ACM Conference on Online Social Networks* (ACM, Palo Alto, USA 2–3 November 2015) (hereafter “*Personal Information*”).

²⁰⁵ Liu *Personal Information* 79.

party, consent (as the principal legal basis for processing), notice, and other legal bases for processing. This section of the study will now briefly discuss the international instruments, regional and sub-regional regulations that have had a significant impact on the POPI Act.



CHAPTER 3

INTERNATIONAL FRAMEWORK ON DATA PROTECTION

3.1 INTRODUCTION

The previous chapter provided the conceptual framework on data processing processes, highlighting privacy issues within the smart city ecosystem. The formal normative basis for data protection laws is derived primarily from catalogues of fundamental human rights set out in certain multilateral instruments, notably the Universal Declaration of Human Rights (hereafter: UDHR),²⁰⁶ the International Covenant on Civil and Political Rights (hereafter: ICCPR)²⁰⁷, as well as the major regional human rights treaties, such as the European Convention on Human Rights and Fundamental Freedoms (hereafter: ECHR)²⁰⁸ and the American Convention on Human Rights (ACCHR).²⁰⁹ Except for the African Charter on Human and People's Rights (hereafter: ACHPR)²¹⁰, all of these instruments expressly recognise privacy as a fundamental human right.²¹¹ This chapter provides a cross-jurisdictional assessment on the development of regulatory instruments (statutes, recommendations and guidelines) of data protection and the right to privacy.

²⁰⁶ United Nations (U.N.) General Assembly resolution 217 A (III) of 10th Dec. 1948 is a non-binding legal instrument.

²⁰⁷ U.N. General Assembly resolution 2200A (XXI) of 16th Dec. 1966; in force 23rd March 1976 is a legally binding covenant on member states.

²⁰⁸ European Treaty Series No. 5; opened for signature 4th Nov. 1950; in force 3rd Sept. 1953. The treaty is legally binding on member states, overseen by an independent international court, which safeguards people's basic rights and fundamental freedom.

²⁰⁹ OAS Treaty Series No. 36; adopted 22nd Nov. 1969; in force 18th July 1978. The treaty mandates member states of the commitment to accept the human rights in the Convention as legally binding.

²¹⁰ OAU Doc. CAB/LEG/67/3 rev. 5; adopted 27th June 1981; in force 21st October 1986. The charter is legally binding on member states.

²¹¹ See UDHR, Article 12; ICCPR., Article 17; ECHR., Article 8; ACHR, Article 11. See also Article V of the American Declaration of the Rights and Duties of Man (O.A.S. Resolution XXX; adopted 1948).

3.2 THE EVALUATION OF THE CONCEPT OF THE RIGHT TO PRIVACY

The Greek philosopher Aristotle described a distinction between the public realm of political events (which he called the polis) and the private world of individual life (termed oikos). This duality may facilitate the prompt identification of "a confidential zone for the citizen."²¹² Warren and Brandeis described an already existing common law right as a steppingstone to the right to be left alone, such as the right to select the amount to which an individual's thoughts, feelings, and emotions may be revealed to others.²¹³ This privilege was founded on the premise of inviolability of the person.²¹⁴

In the decades that followed, the main United Nations General Assembly resolutions reinforced the notion of interdependence of human rights by emphasizing that all human rights are universal, interdependent, and linked. The international community must address human rights on a worldwide scale in a fair and equitable manner, on equal terms, and with equal emphasis.²¹⁵ According to Minkler L and Sweeney S²¹⁶, the vision of a comprehensive human rights system was founded on the notion that all human rights must be realized in order to guarantee the dignity of the human person. In this way, an integral system of human rights is established in which the violation of one of them, be it a civil or political right or an economic, social, or cultural right, hinders the achievement of the others. On the contrast, scholars like Quane HA argue that the interdependence and indivisibility nature of human rights will be guaranteed when the most vulnerable, socially excluded, and marginalized populations are included.²¹⁷

²¹² Michael C and James A 'Comparative Analysis of the Right to Privacy in the United States, Canada and Europe' (2014) 29(2) *Connecticut Journal of International Law* 261.

²¹³ Bratman B 'The Right to Privacy and the Birth of the Right to Privacy'(2002) 69 *Tennessee Law Review* 344 (hereafter "*The Right to Privacy*").

²¹⁴ Bratman B *The Right to Privacy* 69 TLR 349.

²¹⁵ United Nations Vienna Declaration and Programme of Action. Geneva: United Nations; 1993.

²¹⁶ Minkler L and Sweeney S 'On the invisibility and interdependence of basic rights in developing countries' (2011) 33 *HRQ* 351-396.

²¹⁷ Quane HA 'Further dimension to the interdependence and indivisibility of human rights? Recent developments concerning the rights of indigenous peoples' (2012) 25 *HHJ*. 49-83.

Legal scholars utilise a simple binary binding or nonbinding distinction to distinguish between hard and soft law.²¹⁸ Positivist legal experts tend to reject the concept of soft law, arguing that law, by definition, is binding.²¹⁹ In contrast, constructivist scholars focus less on the binding nature of law at the enactment stage and more on the effectiveness of law at the implementation stage, addressing the gap between law-in-the-books and law-in-action; they note how even domestic law varies in terms of its impact on behavior, making binary distinctions between binding "hard law" and nonbinding "soft law" illusory.²²⁰ The role of hard law instruments is to enhance the credibility of state obligations by increasing the cost of reneging, whether through legal sanctions or the consequences to a state's reputation if it is proven to have breached its legal commitments.²²¹ Soft law instruments on the other hand, are less complex and less costly to negotiate.²²² For example, soft law compliments hard law where instruments are consciously utilised to generate support for treaty adoption; to assist in the development of customary international law norms (binding hard law).²²³

3.3 RIGHT TO PRIVACY IN INTERNATIONAL INSTRUMENTS

3.3.1 The Universal Declaration of Human Rights

Article 12 of the 1948 Universal Declaration of Human Rights (UDHR) establishes the right to privacy in modern human rights law: "No one shall be subjected to arbitrary interference with his privacy, family, home, or communications, nor to attack one's honor

²¹⁸ See Klabbers J 'The Redundancy of Soft Law' (1996)65. *NORDIC J INT'L L.* 167- 168 (hereafter "Soft law").

²¹⁹ Klabbers J *Soft law* 67 *NORDIC J. INT'L L.* 381 and 391.

²²⁰ See Trubek D et al *Law and New Governance in the EU and the US* 1 ed (2006) 65-67.

²²¹ George W and Michael A 'Reputation, Compliance, and International Law' (2002) 31 (1) *JSTOR* 108-109 (hereafter "Reputation and Compliance").

²²² George W and Michael A *Reputation and Compliance* (2002) 31 (1) *JSTOR* 111.

²²³ Jeffrey L et al *International law: Norms, Actors and Process* 2d ed (2006) 95.

or reputation." Everyone is entitled to legal protection against such interference or attacks".²²⁴ This is because the right to privacy is paramount to human dignity.

3.3.2 The International Covenant on Civil and Political Rights

In an effort to achieve the aim of human rights law, privacy becomes the major concern. Article 17 of ICCPR of 1966 reaffirms the aforementioned position of privacy as a right entitled to legal protection, stating:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honor or reputation; and
2. Everyone has the right to legal protection against such interference or attacks.²²⁵

The ICCPR clearly provides for the protection of the rights to privacy and all signatories to this UN instrument are bound by its provision.

It is noteworthy, that the international human rights system, as organised at the level of the UN, as well as various other regional human rights systems, have offered guidelines on how states, who bear the primary responsibility for protecting human rights, can develop rights-respecting policies on communication surveillance.²²⁶ On the relationship between the ICCPR's right to privacy and communication surveillance. Diggelmann and Cleis contend that the ICCPR's right to privacy places a primary emphasis on freedom from society and privacy as dignity.²²⁷ Moreover, that the draft history of the right to privacy does not support the assertion that one of the two competing concepts

²²⁴ UN 'Peace, Dignity and Equality on a Healthy Planet,' available at <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (accessed on 3 June 2022).

²²⁵ UN 'Peace, Dignity and Equality on a Healthy Planet,' available at <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (accessed 3 June 2022).

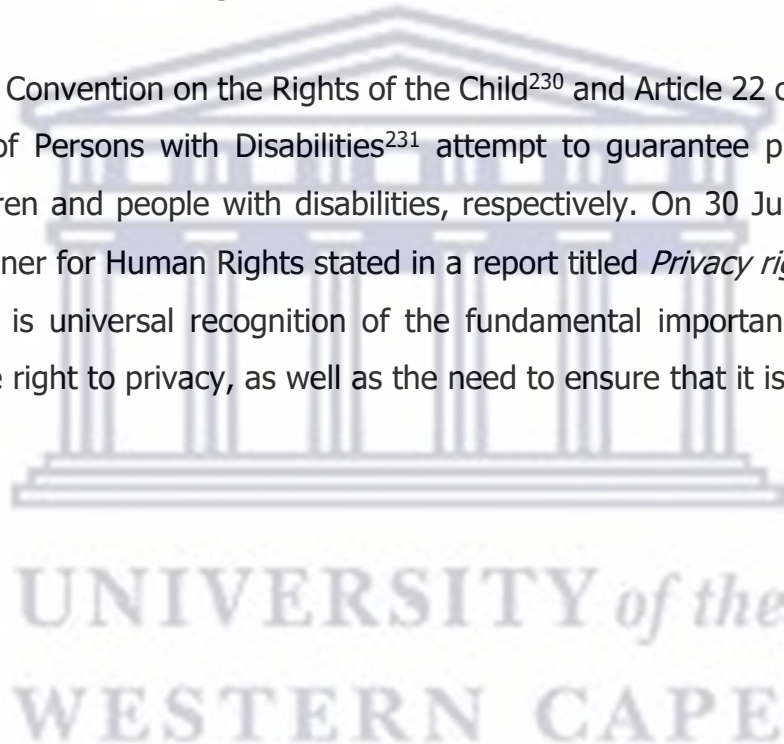
²²⁶ Privacy International 'Guide to international law and surveillance 2.0' available at <https://privacyinternational.org/sites/default/files/2019-04/Guide%20to%20International%20Law%20and%20Surveillance%202.0.pdf> 3-5 (accessed 28 June 2023).

²²⁷ Diggelmann O and MN Cleis 'How the right to privacy became a human right' (2014) 14 *Human Rights Law Review* 458.

can be said to be the main concept. Instead, it appears to reinforce the idea that the idea of privacy itself is intimately connected to a number of other ideas.²²⁸ Accordingly, the Human Rights Committee provides a detailed analysis of the ICCPR in its commentary stating that privacy under international human rights law covers all forms of communication over distance, for example in the smart city eco-system by telephone, telegram, telex, e-mail and other mechanical or electronic means of communication.²²⁹

3.3.3 The Convention on the Rights of the Child

Article 16 of the Convention on the Rights of the Child²³⁰ and Article 22 of the Convention on the Rights of Persons with Disabilities²³¹ attempt to guarantee protection for the privacy of children and people with disabilities, respectively. On 30 June 2014, the UN High Commissioner for Human Rights stated in a report titled *Privacy rights in the digital age*, that there is universal recognition of the fundamental importance and enduring relevance of the right to privacy, as well as the need to ensure that it is protected in law and practice.²³²



²²⁸ United Nations Human Rights Council 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (17 April 2013) UN Doc A/HRC/23/40.

²²⁹ Nowak M 'UN Covenant on Civil and Political Rights: CCPR commentary' (2005) 401.

²³⁰ UN Convention on the Rights of Child of 1989, UN Gen. assembly resolution 44/25 Article 16 (1) states that no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.

²³¹ UN Convention on the Rights of Persons with Disabilities of 2007 UN resolution A/RES/61/106 Article 22-Respect for privacy states:

No person with a disability, regardless of location or living situation, should be subjected to arbitrary or unlawful interference with his or her privacy, family, home, correspondence, or other forms of contact, or to unlawful attacks on his or her honor and reputation. Individuals with impairments are entitled to legal protection against such interference or attacks.

²³² Office of the United Nations High Commissioner for Human Rights 'The Right to privacy in the Digital age', (30 June 2014) available at <https://www.ohchr.org/en/privacy-in-the-digital-age> (accessed on 11 June 2022).

3.4 PRIVACY IN VARIOUS REGIONAL HUMAN RIGHTS CONVENTIONS

3.4.1 European Convention on Human Rights of 1950

Article 8 of the European Convention on Human Rights (ECHR) sets the basis for a globally improved privacy framework.²³³ In a democratic society, privacy is not regarded as an absolute right, and it is subject to certain restrictions deemed necessary. These exceptions must be implemented in conformity with the particular law that has been passed in this area. As stated in Article 8, authorities may not interfere with this right unless it is "consistent with the law and necessary in the interests of a democratic society, in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others."

Consequently, the restrictions can only be circumvented under extremely limited conditions. In addition, the European Council Directive mandates that member states enact privacy and data protection legislation in conformity with the directive's terms.²³⁴

3.4.2 American Convention on Human Rights of 1969

The core of the American Convention on Human Rights (hereafter: ACHR)²³⁵ prioritises confidentiality. "Article 11 states:

²³³ Article 8 on the right to respect Private and Family Life states:

1. Everyone is entitled to respect for his or her private and family life, residence, and correspondence.
2. No public authority shall interfere with the exercise of this right except as required by law and necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of others' rights and freedoms.

²³⁴ UN Directive 95/46/EC, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046>. (accessed on 17 June 2022).

²³⁵ The American Convention on Human Rights 'Pact of San Jose, Costa Rica', 1967.

1. Everyone has the right to have his or her honour respected and his or her dignity recognised.
2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honour or reputation.
3. Everyone has the right to the protection of the law against such interference or attacks.”

It is noteworthy to state, that the UN Charter²³⁶ (hereafter: 'the Charter') establishes the fundamental principles of equality and dignity for all people globally. Subsequently, there are numerous clauses in the Charter which discuss necessity for global recognition and protection of human rights and freedom.²³⁷ The ACHR is first and foremost a human rights instrument that is legally binding upon state member parties to protect, promote and develop the human rights and freedoms set forth in the Convention.²³⁸

Bygrave and Clarke state that the new trend in use and sharing of personal data has created concerns about individual privacy and data security, which have been exuberated by technological advancements in the processing of personal data.²³⁹ The right to privacy as stipulated in the ACHR is vital because individual privacy can be severely compromised by tracking devices in the smart city eco-system.²⁴⁰

Consequently, since March 2018, the Special Rapporteur has advanced the mandate by reviewing pertinent information, including difficulties brought on by new technologies; conducting official and 'non-official' country visits; promoting the protection of the right to privacy; advocating privacy principles; participating in international events to promote

²³⁶ Charter of the United Nations, signed 26 June 1945, 59 Stat. 1031, T.S. No. 993, 3 Bevens 1153 (entered into force 24 Oct. 1945).

²³⁷ See articles 1, 13(1), 55, 62(2), 68, 76(c) of the UN Charter.

²³⁸ See generally Article 1 of ACHR.

²³⁹ Bygrave LA *Data Privacy Law: An International Perspective* (hereafter "Data Privacy Law") (2014) Oxford University Press 9.

²⁴⁰ Bygrave *Data Privacy Law* 10.

a cogent approach to the right to privacy; raising awareness of the right to privacy and effective remedies; and reporting on all of the above.²⁴¹

3.4.3 African Charter of Human and People's Rights of 1981

In most African communities, the concept of privacy is conceptualised similarly. Despite their divergent legal systems, this is the case.²⁴² Countries governed by Common Law accord privacy the same significance as Western nations. African scholars such as Makulilo think that this feature is a result of the Western importation of the concept, hence the borrowed connotation.²⁴³ In *Griswold v. Connecticut*²⁴⁴ the Supreme Court defined privacy as "a state comprising all personal information that a person at a relevant time selects to be withheld from the knowledge of outsiders and with regard to which he demonstrates a desire for privacy".²⁴⁵ In *National Media Ltd v. Jooste*,²⁴⁶ the Constitutional Court of South Africa affirmed that its legitimacy in African culture extends beyond African literary works.

The African Region adopted the African Charter on Human and People's Rights (hereafter: ACHPR) in 1981. The Charter did not define the term 'people,' but it included all of the UDHR's rights with the exception of the right to privacy and the right against forced or compulsory labor. Regarding the right to privacy, it can only be presumed that the omission is due to the nature of the right, which, if given, may paralyze the entire concept of the Charter, namely the promotion of communal values and African cultural norms, in this case, communalism versus individualism.²⁴⁷ In fact, Ankumah EL, argues that the

²⁴¹ United Nations Human Rights Council 'Report of the Special Rapporteur on the promotion and protection of the right to Privacy' UN Doc A/HRC/40/63 (2019) (hereafter: "*Report of the Special Rapporteur on the promotion and protection of privacy rights*") available at <https://rm.coe.int/40th-hrc-session-report-of-the-special-rapporteur-on-the-right-to-priv/1680933f08> (accessed 20 June 2023).

²⁴² Makulilo AB *Protection of Personal Data in Sub-Sahara Africa* (published PhD thesis, Universität Bremen, 2012) 326 (hereafter "*Protection of Personal Data in Sub-Sahara Africa*").

²⁴³ Makulilo, AB *Protection of Personal Data in Sub-Sahara Africa* 328.

²⁴⁴ 381 U.S. 479 [1965].

²⁴⁵ Neethling J et al *Neethling's Law of Personality* 1ed (1996) 36.

²⁴⁶ [1996] 3 SA 262(A) 271.

²⁴⁷ Ankumah EL *La Commission africaine des droits de l'homme et des peuples. Pratiques et*

Charter's incomplete and vague description of protected rights is one of its most noteworthy and maybe most important flaws.²⁴⁸ Consequently, the Charter provides minimal legal protection for individuals.²⁴⁹ The ACHPR does not specify the right to privacy, but Article 18 emphasizes the State's obligation to safeguard family life.²⁵⁰

3.4.4 African Charter on the Rights and Welfare of the Child of 1990

Article 10 of the Charter ensures the right to privacy of children when it states that Article 10 of the Charter guarantees the right to privacy for children when it states that no child shall be subject to arbitrary or unlawful interference with his privacy, family, home, or correspondence, or to attacks upon his honor or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. Furthermore, the youngster is entitled to legal protection against such interference or attacks.²⁵¹

3.4.5 The African Union Framework for Human Rights and Privacy

The African Union (AU) was founded in 2002, replacing the Organization of African Unity (OAU), following the adoption of the Constitutive Act of the AU by African heads of state

²⁴⁸ procédures, Londres SADIC' (1995) 189 (hereafter "*La Commission africaine*").

²⁴⁹ Ankumah EL *La Commission africaine* 190.

²⁴⁹ Ankumah EL *La Commission africaine* 193.

²⁵⁰ Article 18 states:

1. The family is the natural and fundamental unit of society. It will be safeguarded by the state, which will ensure its physical and moral health.
2. The State shall be obligated to help the family which is the guardian of community recognised morals and traditional values.
3. The State shall ensure the eradication of all forms of discrimination against women, as well as the protection of the rights of women and children, in accordance with international declarations and conventions.
4. The elderly and the disabled have the right to protection measures tailored to their physical or moral requirements.

²⁵¹ African Charter on the Rights and Welfare of the Child, available at https://au.int/sites/default/files/treaties/36804-treaty-african_charter_on_rights_welfare_of_the_child.pdf. (accessed 17 June 2022).

in Lome, Togo.²⁵² The AU commits to advancing democratic principles and institutions, such as participatory democracy and good governance.²⁵³ As part of its efforts to promote human rights, the AU commits to defending the human and people's rights enshrined in the African Charter and other human rights treaties.²⁵⁴

Africa became the second region, after the EU, to approve a data protection instrument on June 27, 2014, with the adoption of the Convention on cyber security and protection of personal data protection also known as the Malabo Convention.²⁵⁵ Unlike the EU-DPD, however, the Convention has established not only a data protection framework, but also a cyber-security system and a data protection regime.²⁵⁶ The Convention addresses three primary issues influencing online activities: e-commerce, cybercrime, and data protection. The Convention's data protection policy is outlined in Chapter II: Personal Data Protection.²⁵⁷ In terms of the preamble, the purpose of the Chapter is to preserve privacy and encourage the free flow of information. The objective is to encourage harmonisation of current data protection legal regimes and reforms in Member States without or with weaker data protection legal regimes.²⁵⁸

The African continental free trade area (hereafter "AfCFTA") has been ratified by about 81% of African nations.²⁵⁹ Moreover, the AfCFTA's goals include establishing a single continental market for goods and services, doing away with trade barriers, increasing productivity, and promoting socioeconomic development.²⁶⁰ Consequently, Okunade and Ogunnubi are of the view that natural resources found in African nations, such as

²⁵² The 36th session of the Assembly of Heads of State and Government's ordinary session. The Act was enforced on May 26, 2001(hereafter AU Constitutive Act 2000).

²⁵³ Article 3 (g) the AU Constitutive Act 2000.

²⁵⁴ Article 3 (h) of the AU Constitutive Act.

²⁵⁵ Articles 16 – 23 of the Malabo Convention 2014.

²⁵⁶ Articles 16 – 23 of Malabo Convention.

²⁵⁷ Articles 16 – 23 of Malabo Convention.

²⁵⁸ Articles 16 – 23 of Malabo Convention.

²⁵⁹ Tralac 'Status of AfCFTA Ratification' (hereafter: "AfCFTA Ratification") available at <https://www.tralac.org/resources/infographic/13795-status-of-afcfta-ratification.htm/> (accessed 20 June 2023).

²⁶⁰ Tralac *AfCFTA Ratification*.

minerals, crude oil, gas, timber, animal products, and raw agricultural produce can be traded and utilised in numerous global economic sectors.²⁶¹ Despite the enormous amounts of resources, several African nations continue to live in poverty without receiving any benefits from the trade in natural resources.²⁶²

In addition, investments in ICT infrastructure have increased to support commerce and other economic activities.²⁶³ In comparison to industrialised nations, the continent is anticipated to have higher domestic growth product value (GDP).²⁶⁴ The development of e-commerce in Africa is still lagging in comparison to that of developed nations, and it is necessary to understand AfCFTA's potential to foster this growth.²⁶⁵ Technology is required to assist in cross-border trade with e-commerce and entrepreneurship within the context of the AfCFTA in order to promote products and services, process transactions, and manage after-sales services.²⁶⁶

The existing framework is structured similarly to international mechanisms such as the OECD recommendations, Convention 108, and the EU-DPD. The Convention specifies seven data protection principles for the processing of personal data, identical to those found in international regulations with a few minor modifications.²⁶⁷ The Convention precludes the regulation of personal data included in temporary files created by technical intermediaries, such as ISSP providers, for automatic, intermediary, and temporary data storage.²⁶⁸ Other exemptions include the processing of personal data for purely domestic purposes and in a personal context, so long as such data is not intended to be shared

²⁶¹ Okunade S and Ogunnubi O 'A "Schengen" agreement in Africa? African agency and the ECOWAS protocol on free movement' (2021) 36(1) *Journal of Borderlands Studies* 119-137 (hereafter *Schengen agreement in Africa*).

²⁶² Okunade S and Ogunnubi O *Schengen agreement in Africa* 121.

²⁶³ Asongu S and Odhiambo N *Information and communication technology APJ* 647-648.

²⁶⁴ Ajambo E and Emebinah C 'The African continental free trade area: Maximizing benefits for the Continent' (2021) *APJ* 15-27.

²⁶⁵ Ismail Y 'Mobilising e-commerce for development in Africa through AfCFTA' (2020) *CUTS International*, Geneva, Switzerland.

²⁶⁶ Kshetri N 'Barriers to e-commerce and competitive business models in developing countries: A case study' (2007) 6 *Electronic Commerce Research and Applications Journal* 443-452.

²⁶⁷ Articles 16 – 23 of Malabo Convention.

²⁶⁸ Article 9 (2) (a) of Malabo Convention.

with or sold to third parties;²⁶⁹ and the processing of personal data for journalistic and research purposes, so long as it is carried out in accordance with the professional codes. In addition to processing for artistic and literary expression, the exempted activities also include processing for artistic and literary expression.²⁷⁰ Personal data processing using data matching is restricted with DPA approval.²⁷¹ However, the Convention provides no notification provisions for data breaches.²⁷²

The framework for cross-border data transfer established by the Convention forbids the transfer of personal data outside of the AU to jurisdictions that do not provide an acceptable degree of protection.²⁷³ Sadly, the Convention leaves the AU Member States at a crossroads because it fails to define what constitutes an adequate level of protection; and while it does not encourage the free flow of data between parties to the Convention, it does not impose an adequate requirement on AU Member States, regardless of whether they have ratified the Convention. Moreover, DPAs may flow pursuant to Articles 12 (2)(k) and 14 (6)(b). There are no laws addressing Binding Corporate Rules or Model Contracts for the transfer of personal information to third nations. Permit the international transfer of personal information regardless of the level of protection provided by the receiver. Unlike other data protection laws, such as OECD, CoE, and DPD, the Convention lacks a derogation rule for trans-border data.²⁷⁴

3.5 PRIVACY AND DATA PROTECTION IN SUB-REGIONAL FRAMEWORKS IN SUB-SAHARAN AFRICA

A sub regional privacy regulation mechanism for SADC Data Protection Modal Law.²⁷⁵ The SADC passed the Data Protection Model Law draft in 2012. This Modal Law's architecture

²⁶⁹ Article 9 (2) (b) of Malabo Convention.

²⁷⁰ Article 14 (3) of Malabo Convention.

²⁷¹ Article 15 of Malabo Convention.

²⁷² Article 15 of Malabo Convention.

²⁷³ Article 14 (6) (a) of Malabo Convention.

²⁷⁴ Articles 12 (2)(k) and 14 (6)(b) of Malabo Convention.

²⁷⁵ The Southern African Development Community (SADC) is a sub-regional grouping of fifteen countries:

for data protection is similar to the international data protection codes. As a result, the proposed regime is comparable to those established by ECOWAS and the Malabo Convention, albeit with substantial differences in their scopes of applicability.²⁷⁶ As is typical for model laws, the SADC Model Law lacks a preamble with an orthodox meaning and context. Therefore, it complicates the interpretation of the law's goals and context. It also fails to state its objectives; nonetheless, from the "preamble" it is possible to infer the protection of an individual's right to privacy and the harmonisation of data protection policies and laws.²⁷⁷

In 2012, following a controversial judgement given by the Tribunal against the President of the Republic of Zimbabwe for violation of human rights and fundamental freedoms, the Tribunal lost its authority to rule on human rights matters.²⁷⁸ In order to accomplish this, the heads of state and government enacted a Protocol limiting the Tribunal's powers to the interpretation of the SADC Treaty and other ratified instruments pertaining to disputes between Member States.²⁷⁹

3.6 SOFT LAW: INTERNATIONAL IMPERATIVES

The Smart Cities Framework should be evaluated in light of a variety of South African acts, policies, frameworks, and initiatives affecting human settlements. Efforts to improve South African human settlements are guided by international objectives and agendas. There are two essential agendas listed below.²⁸⁰

Angola, Botswana, Democratic Republic of the Congo (DRC), Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Zambia and Zimbabwe.

²⁷⁶ Makulilo, AB *Protection of Personal Data in Sub-Saharan Africa* 364.

²⁷⁷ Makulilo AB *Protection of Personal Data in Sub-Saharan Africa* 367.

²⁷⁸ *Mike Campbell (Pvt) LTD & others v. Republic of Zimbabwe*; SADC (T) 2/07 2007. (hereafter "*Mike Campbell (Pvt) LTD & others v Republic of Zimbabwe*")

²⁷⁹ *Mike Campbell (Pvt) LTD & others v Republic of Zimbabwe 2*.

²⁸⁰ UN 'Transforming our World: the 2030 Agenda for Sustainable Development' (hereafter "*2030 Agenda for Sustainable Development*") 24 available at <https://sustainabledevelopment.un.org/content/documents/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf>. (accessed 21 July 2022).

3.6.1 The Agenda 2030 For Sustainable Development

In accordance with Transforming our World: the 2030 Agenda for Sustainable Development, member states of the United Nations have been required to formulate their agendas and political programs for the next 15 years.²⁸¹ The 17 Sustainable Development Goals (hereafter: SDG) provide a "plan of action for people, planet, and prosperity". SDG 11 especially addresses sustainable cities and communities: "Make cities and human settlements inclusive, safe, resilient, and sustainable."²⁸²

In October 2016, during the United Nations Conference on Housing and Sustainable Urban Development (Habitat III) in Quito, Ecuador, the New Urban Agenda was endorsed.²⁸³ This agenda is intended to influence national and municipal policies on the growth and development of cities through the year 2036.²⁸⁴ It shares a vision of cities for all, referring to the equal use and enjoyment of cities and human settlements, that seeks to promote inclusion and ensure that all inhabitants, of present and future generations, are able to inhabit and produce just, safe, healthy, accessible, affordable, resilient, and sustainable cities and human settlements to promote prosperity and quality of life for all.²⁸⁵

3.6.2. The Agenda 2063-The Africa We Want

The African Union Commission created a strategy framework for the socio-economic transformation of the continent from an African perspective.²⁸⁶ Agenda 2063 - The Africa We Want specifies several goals.²⁸⁷ It includes an Africa in which cities and other

²⁸¹ 2030 Agenda for Sustainable Development 5.

²⁸² 2030 Agenda for Sustainable Development 24.

²⁸³ UN 'The New Urban Agenda' (hereafter "The New Urban Agenda") 3, available at <https://habitat3.org/wp-content/uploads/NUA-English.pdf> (accessed 21 July 2022).

²⁸⁴ The New Urban Agenda 3-5.

²⁸⁵ The New Urban Agenda 6.

²⁸⁶ African Union Commission: 'Agenda 2063' (hereafter "African Union Commission Agenda 2063") (2015) available at https://au.int/sites/default/files/documents/33126-doc-03_popular_version.pdf (accessed 23 July 2022).

²⁸⁷ African Union Commission Agenda 2063 11.

settlements are centers of cultural and economic activity, with updated infrastructure, and people have access to inexpensive and good housing, including housing financing, as well as all the essentials of life, such as water, sanitation, energy, public transportation, and ICT.²⁸⁸

3.7 CONCLUSION

In Africa, data protection laws and institutions are still in their formative stages. Privacy is safeguarded by both human rights instruments and data privacy laws. This chapter discussed the various International, regional and sub-regional instruments pertaining to data protection and specifically to the right of privacy. The vast majority of human rights instruments and data privacy laws or instruments are soft law, and therefore do not provide compelling force for the enactment of data protection legislation at national levels. Although both laws are similar in that they all contain fundamental data protection principles and mandate the establishment of supervisory authorities, their respective scopes are distinct.

The domestic enforcement under the constitutional right to privacy has a dismal track record. Africa, as a region, disregarded or refused to acknowledge the right to privacy under the Regional Instrument. The enforcement of other infractions of human rights has also been stalling. In fact, Sub-Regions such as the SADC opted expressly to withdraw the Tribunal's authority to investigate and prosecute human rights violations. This demonstrates a lack of political will to enforce individual rights in Africa, notwithstanding the promises and assurances contained in the preambles of regional and sub-regional human rights instruments.

The Agenda 2030 for SDG, member states of the United Nations have been required to formulate their agendas and political programs for the next 15 years. The 17 SDGs

²⁸⁸ African Union Commission Agenda 2063 4.

provide a 'plan of action for people, planet, and prosperity'. SDG 11 especially addresses sustainable cities and communities: "Make cities and human settlements inclusive, safe, resilient, and sustainable. The Agenda 2063 includes an Africa in which cities and other settlements are centers of cultural and economic activity, with updated infrastructure, and people have access to inexpensive and good housing, including housing financing, as well as all the essentials of life, such as water, sanitation, energy, public transportation, and ICT. This section of the study will now briefly discuss South Africa's legal framework on data protection. The following chapter will now examine South Africa's legal framework governing Data Protection.



CHAPTER 4

SOUTH AFRICA'S LEGAL FRAMEWORK GOVERNING DATA PROTECTION

4.1 INTRODUCTION

The previous chapter provided a cross-jurisdictional assessment on the development of regulatory instrument of data protection and the right to privacy. Furthermore, while there has been a steady adoption of smart cities in the global South, with nations like Brazil, India, Rwanda, and South Korea initiating national roll out plans, the literature and research on smart cities has been dominated by examples and initiatives from the Global North.²⁸⁹ The topic of smart cities has just lately been the focus of research in the Global South.²⁹⁰ This chapter analyses the efficacy of South Africa's current legal framework for data protection. In order to contextualise the level of protection that is granted to data privacy in South Africa, a critical analysis is performed on the common law of the country, as well as the Constitution, the POPIA and subordinate regulations.

4.2 THE NATIONAL GROWTH STRATEGY

The relationship between public international law and municipal law in South Africa is governed by the 1996 Constitution of the Republic of South Africa.²⁹¹ Dugard²⁹² suggests that the nature of South Africa's approach can be characterised as one of harmonisation, as its primary objective is to harmonise public international law and South African domestic law. Ginsberg, Chernykh, and Elkins²⁹³ argue that the functions of public

²⁸⁹ Backhouse J 'The digital turn in postcolonial urbanism: Smart citizenship in the making of India's 100 smart cities.' *Transactions of the Institute of British Geographers* 43 405-419 (hereafter "*Smart citizenship*").

²⁹⁰ Backhouse J *Smart citizenship* 417.

²⁹¹ Sections 231 and 232 of the Constitution.

²⁹² Dugard *Privacy and Compliance* 42-43.

²⁹³ Ginsberg, Chernykh and Elkins 2008 U Ill L Rev 237.

international law should be evaluated from both an interstate and intrastate perspective. The authors demonstrate that the interaction between domestic law and international law, as reflected by the dichotomy between monism and dualism, differs significantly between states. Furthermore, we understand from this that South Africa follows a dualist approach with regard to international agreements, and that the binding nature of public international law, and in particular treaty law, is based on the consent of the parties to the agreement.²⁹⁴

In developing nations such as South Africa, challenges to Smart City Development (SCD) include a preference for operational management over institutional transformation and a lack of a distinct strategy.²⁹⁵ Smart City efforts in poor nations require a policy framework for evaluation and guidance.²⁹⁶ This was revealed by President Ramaphosa in his 2019 State of the Nation Address, in which he referenced the concept of a new Smart City in the 21st century within the context of a progressive state. For South Africa's cities to achieve significant progress toward the Internet of Things (IoT) and seamless connectivity, greater alliances and coordinated leadership will be required.²⁹⁷ This does not drastically contrast or juxtapose the perspective of Musakwa and Mokoena that Smart Cities in South Africa are an example of misguided priorities, as what the people truly desire is not Smart Cities but an end to poverty, inequality, and poor living conditions.²⁹⁸

The National Planning Commission (2010) in its Development Plan 2030 (hereafter: NDP) provides a long-term vision for the country and identifies a desired objective, namely the eradication of poverty and the reduction of inequality by 2030.²⁹⁹ It also anticipates

²⁹⁴ Ginsberg, Chernykh and Elkins 2008 U Ill L Rev 204-205.

²⁹⁵ Vu K and Hartley K 'Promoting smart cities in developing countries: Policy insights from Vietnam. *Telecommunications Policy*, (2018) 42(10) *Elsevier* 845–859.

²⁹⁶ Vu and Hartley K 2018 42(10) 850.

²⁹⁷ Hubbard J *et al* 'Why SA is lagging behind global smart city developments' *Finweek* available: <https://www.fin24.com/Finweek/Featured/why-sa-is-lagging-behind-global-smart-city-developments-20170829>. (accessed 9 September 2022).

²⁹⁸ Musakwa, W and Mokoena B 'Smart cities in South Africa! A case of misplaced priorities? In *Computers in Urban Planning and Urban Management* (2017) Adelaide, Australia: Computers in Urban Planning and Urban Management Conference.

²⁹⁹ National Planning Commission 'National Development Plan 2030: Our future - make it work.'

significant and quantifiable progress towards constructing functionally connected, balanced, and lively urban communities by 2030.³⁰⁰ Despite the fact that the NDP does not promote the concept of smart cities, the plan acknowledges ICT as a crucial enabler of economic activity and envisions a greater role for ICT.³⁰¹

4.3 SOUTH AFRICA'S DATA PRIVACY PRIOR TO THE ENACTMENT OF THE POPI ACT

4.3.1 Constitutional protection of privacy

South Africa's Constitution is the supreme law, and any conduct or law that conflicts with it is invalid.³⁰² The Bill of Rights, which is detailed in Chapter 2 of the Constitution, provides the enshrined rights that apply to the executive, legislature, state organs, and natural and juristic persons.³⁰³

The Constitutional enshrinement of fundamental rights strengthens their protection and elevates their stature by requiring them to apply to all laws.³⁰⁴ As a result, any law or action taken by the state, or an individual may be evaluated in light of an enshrined basic right. A limitation of a fundamental right is permissible only if it meets with the provisions of section 36 of the Constitution's limitation of rights clause.³⁰⁵

The Presidency available at <http://www.poa.gov.za/news/Documents/NPC%20National%20Development%20Plan%20Visio%202030%20-lo-res.pdf> (accessed on 25 July 2022) (hereafter "*NDP 2012'*").

³⁰⁰ NDP 2012.

³⁰¹ NDP 2012.

³⁰² Section 2 of the Constitution.

³⁰³ Sections 8(1) and 8(4) of the Constitution.

³⁰⁴ *SALRC PDP Report 20*.

³⁰⁵ Section 36 of the Constitution states: "(1) The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including -

(a) the nature of the right;

(b) the importance of the purpose of the limitation; and

(c) the nature and extent of the limitation.

(2) Except as provided in subsection (1) or in any other provision of the Constitution, no law

Currie and De Waal focused on the *Mistry v. Interim Medical and Dental Council of South Africa* case and stated that the Constitutional Court broadened the privacy rights established by the Constitution to cover "informational self-determination."³⁰⁶ The Constitutional Court has not substantially addressed ³⁰⁷ cases alleging the infringement of personal data privacy. In *Mistry v. Interim Medical and Dental Council of South Africa*,³⁰⁸ the Constitutional Court attempted to establish criteria for determining whether a violation of data privacy has occurred.

Nevertheless, the Constitution only establishes a broad framework for data privacy. A comprehensive framework of data protection principles cannot be left to the Constitutional Court because it is the responsibility of the government to implement a statutory data protection regime in South Africa. Section 14 of the Bill of Rights establishes the fundamental right to privacy, however identity is not explicitly acknowledged.³⁰⁹ Neethling, on the other hand, contends that many of the unnamed personality rights (such as identity, feelings, etc.) fit under the right to human dignity, implying that these unspecified rights are likewise recognised as constitutionally enshrined human rights.³¹⁰ As a result, the right to identify might be regarded protected within the right to human dignity, which is expressly mentioned in Section 10 of the Constitution.³¹¹

may limit any right entrenched in the Bill of Rights."

³⁰⁶ In *Mistry v. Interim Medical and Dental Council of South Africa*, 1998 (4) SA 1127 (CC), it was determined that although not directly stated in then-section 13 of the Interim Constitution, the right to informational privacy is encompassed by section 13's comprehensive protection of privacy.

³⁰⁷ Currie I et al *The Bill of Rights Handbook* 6ed (2013) 302-303. The authors clarify that informational self-determination is an interest in restricting the acquisition, use, and dissemination of personal information.

³⁰⁸ See *Mistry v Interim Medical and Dental Council of South Africa* (note 304 above) at 51.

³⁰⁹ Section 14 of the Constitution states: "Everyone has a 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."

³¹⁰ Neethling 2005 *SALJ* 18.

³¹¹ Roos 2007 *SALJ* 422.

As a result of our Constitution's recognition of the right to privacy, the legislature and executive are prohibited from enacting legislation or doing actions that violate or unjustly limit the right to privacy. Additionally, Roos argues that the government is required to enact laws to ensure an adequate level of data privacy protection where common law is insufficient.³¹²

In *Bernstein v Bester*,³¹³ the Constitutional Court imposed a stringent definition of privacy, limiting it to a person's "inner sanctum" (for instance family life, sexual preference and home environment). Ackermann J. remarked the following:

"Privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly".³¹⁴

Neethling claims that this definition is restricted to personal space of the data subject.³¹⁵

Ackerman J cautioned that caution must be exercised when interpreting fundamental rights and their limitations where he distinguished between the two-stage constitutional inquiry into whether a right (such as privacy) has been violated and then whether the violation is justified when determining the validity of a bill or conduct.³¹⁶ However, in common law, there is a single inquiry into whether an infringement was unlawful or wrongful.³¹⁷

³¹² Roos 2007 *SALJ* 423.

³¹³ *Bernstein & Others v Bester & Others NNO* 1996 (2) *SA* 751 at 788 [C].

³¹⁴ *Bernstein & Others v Bester & Others NNO* 1996 (2) *SA* 751 at 789 par [A].

³¹⁵ Neethling et al 2005 *SALJ* 20.

³¹⁶ *Bernstein & Others v Bester & Others NNO* 1996 (2) *SA* 751 at 790 par [D] – [E]; Burchell *Personality Rights and Freedom of Expression: The Modern Actio Injuriarum* (1998) 388; SALRC PDP Report 21.

³¹⁷ *SALRC PDP Report* 34.

4.3.2 Protection of Privacy Under Common Law

4.3.2.1 Privacy and Identity

In general, the law of delict protects privacy as an independent right of personality.³¹⁸ Roos is of the view that data processing of an individual's personal information constitutes a threat to the individual's right to privacy.³¹⁹ Neethling is of the view that privacy relates to an individual condition of life characterised by seclusion from the public and publicity.³²⁰ This condition embraces all those personal facts which the person concerned has himself determined to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private.³²¹

The Supreme Court of Appeal in *National Media Ltd v Jooste* confirmed this notion of privacy.³²² Common law therefore holds a third party accountable for breaching the privacy of another if the information violated is secret, private, or confidential. According to Neethling, the right to privacy embodied as a person's right is not absolute but is restricted by the legal interests of others and the public interest.³²³

Throughout history, privacy has frequently been interwoven with the right to dignity. The common law, on the other hand, has evolved to recognize an autonomous right to privacy.³²⁴ The precedent for this position is found in the case of *O'Keeffe v Argus Printing and Publishing Co Ltd*,³²⁵ in which the Plaintiff alleged that her photograph and name had

³¹⁸ Roos 'Personal data protection in New Zealand: lessons for South Africa?' (2008) 4 *Potchefstroom Electronic Law Journal* 90.

³¹⁹ Roos 2007 *SALJ* 421.

³²⁰ Neethling *et al* (2005) *SALJ* 32.

³²¹ Neethling *et al* (2005) *SALJ* 37.

³²² 1996 (3) SA 262 (A) 271 - 272. Cf Neethling, 'The concept of privacy in South African Law' (2005) *SALJ* 18, 20.

³²³ Neethling J *et al* *Neethling's Law of Personality* (note 230 above) 281.

³²⁴ Neethling *et al* 'Law of Personality' (2005) 217.

³²⁵ 1954 3 SA 244 (C).

been used for advertising purposes without her authorisation. The court determined that the following question arose:

"... [W]hether the publication of the plaintiff's photograph and name is capable of constituting a violation of the plaintiff's' real personality rights,' and in particular, of her dignity rights."³²⁶

As a result, both the right to privacy and the right to identity are now included into South African common law through the law of person.³²⁷ Individual identity implies to the right of an individual to have control over the accuracy of his or her personal data.³²⁸ To ensure the protection of the abovementioned rights, the law of delict provides the legal framework to that effect.³²⁹

4.3.3 Limitations to the protection of data privacy under the common law and the Constitution

Traditional delictual principles do not vest the individual with active control, and thus do not address situations in which the data subject is unaware:

- (a) that third parties are collecting or processing his or her personal information;
- (b) that he or she has access to his or her personal information; or
- (c) that he or she may correct inaccurate personal information.³³⁰

According to Neethling, in order for an individual to exert active control over his or her personal information, the individual must be:

³²⁶ 1954 3 SA 244 (C) 247 F.

³²⁷ Neethling et al (2005) 219 and 273. Neethling et al *Law of Delict* (1993) 332 - 335.

³²⁸ Roos 2007 *SALJ* 422.

³²⁹ Neethling et al (1993) 5 *SALJ* 250-251.

³³⁰ Roos 2007 *SALJ* 423.

- (a) aware that a data record containing personal information about him or her is being held by the data controller;
- (b) is legally entitled to know who has accessed his data records; and
- (c) is legally entitled to obtain the rectification or deletion of specific data.³³¹

The traditional common law concepts stated above becomes more important only when an individual exercises active control over his or her own personal data.³³² Another restriction of common law is the absence of regulation of transborder data flows (hence referred to as "TBDFs").³³³

4.4 SUBORDINATE DATA PROTECTION LEGISLATION

In South Africa, sectoral regulations implemented in the form of the Promotion of Access to Information Act No. 2 of 2000 (PAIA),³³⁴ the Electronic Communications and Transactions Act No. 25 of 2002 (ECTA),³³⁵ and the National Credit Act (NCA)³³⁶ give little protection for data privacy.³³⁷ Other laws that protect privacy are discussed below:

4.4.1 Promotion of Access to Information Act No. 2 of 2000

The main objective of the Act is intended to give effect to an individual's constitutional right to access information³³⁸ held by the State or another person and necessary for the

³³¹ Neethling *et al* (2005) 278.

³³² Neethling *et al* (2005) 280.

³³³ Roos 2007 *SALJ* 403; *SALRC PDP Report* par 1.2.12.

³³⁴ No. 2 of 2000.

³³⁵ No. 25 of 2002.

³³⁶ No. 34 of 2005.

³³⁷ A Roos 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position' (2007) 424.

³³⁸ Section 32 of the Constitution states that: Everyone has the right of access to -

(a) any information held by the state; and

(b) any information that is held by another person and that is required for the exercise or protection of any rights.

exercise or protection of any rights.³³⁹ The PAIA³⁴⁰ protects data privacy by allowing individuals access to and correction of their personal information held in manual and electronic records, it promotes freedom of information as well lawful access to personal data.³⁴¹

4.4.2 The Electronic Communications and Transactions Act No. 25 of 2002

The Electronic Communications and Transactions Act No. 25 of 2002 (hereafter: "ECTA") was intended to regulate electronic commerce, therefore it applies only to electronic communications.³⁴² The primary purpose of the ECTA is to safeguard the public interest by streamlining electronic communications and transactions.³⁴³ This Act imposes no statutory responsibilities on data controllers; compliance with Section 51 is optional; there is no independent supervisory authority; and there are no criminal sanctions to compel compliance with the principles.³⁴⁴ The POPIA supersedes the ECTA by mandating data protection principles.

4.4.3 National Credit Act 34 of 2005

The National Credit Act (hereafter: "NCA") aims to foster a fair and nondiscriminatory marketplace for consumer credit by regulating consumer credit broadly and establishing improved consumer information standards (which inter alia includes the regulation of credit information).³⁴⁵ The NCA defines "confidential information"³⁴⁶ to include personally identifiable information. However, the NCA restricts data protection to the consumer

³³⁹ Preamble to PAIA.

³⁴⁰ One of the purposes of the PAIA, as stated in section 9(b)(1), is to give effect to the constitutional right of access to any information held by the state or by another person - subject to justifiable limitations, including, but not limited to, limitations designed to protect privacy in a reasonable manner.

³⁴¹ Section 9(b)(1) of the PAIA.

³⁴² Preamble to ECTA; Roos 2007 *SALJ* 426.

³⁴³ Section 2(1) of the ECTA.

³⁴⁴ A Roos 'Data Protection Law in South Africa' in Makulilo AB African Data Privacy Laws: Springer (2017) 428-429.

³⁴⁵ Preamble to NCA.

³⁴⁶ Section 1 of the NCA.

credit business.³⁴⁷ Similar to the ECTA, the NCA is deficient in that it lacks specific data protection responsibilities to protect data privacy in particular. The protection afforded by the above-mentioned sectoral regulation provides fairly fragmented protection for the confidentiality of personal data. To prevent over-regulation, but also to ensure that the generic protection of a data protection regulatory system is implemented in tandem with sector-specific law, the broader yet more particular protection of personal information was compared to sectoral legislation.³⁴⁸

4.5 THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

If one considers the shortcomings of data protection as provided for in the South African legal framework prior to the POPIA, it is clear that a comprehensive overhaul of the statutory framework was required to ensure that legislation provides an adequate level of data protection comparable to that provided by other international instruments.³⁴⁹ Another essential aspect of POPIA is to strike a balance between the right to the protection of personal data and other rights, particularly the right to access information. Given the rapid expansion and expanding usage of large-scale data processing (Big Data), connected devices and systems, for example smart cars, wearables, and converging technologies by both the public and private sectors, achieving this objective has never been more essential (smartphones, drones).³⁵⁰ In other words, to ensure a robust culture of human rights compliance within South Africa's Smart Cities, it will be essential to ensure the adequate protection and implementation of data protection and access to information rights, as the latter may serve to advance the protection of personal data, as well as the transparency, oversight, and accountability of the public and private sectors.³⁵¹

³⁴⁷ Section 3 of the NCA.

³⁴⁸ South African Law Reform Commission Discussion Paper 109 (Project 124) 'Privacy and Data protection' (2005) iv at 396 available at <https://www.justice.gov.za/salrc/dpapers/dp109.pdf>, (accessed on 05 July 2022).

³⁴⁹ *SALRC PDP Report* ix.

³⁵⁰ See *SALRC PDP Report* ix.

³⁵¹ See note 269.

The provisions of the POPIA are discussed in detail below. Following that, the POPIA will be compared to other international instruments in terms of data subject rights and fundamental data privacy principles.

4.5.1 Specific Data Protection: A summary of the POPIA

In chapter 1, a brief background of the POPIA is provided.³⁵² The focus of this discussion is on the particular provisions of this Act that seek to protect the constitutionally guaranteed right to data privacy.³⁵³ Appropriately, higher regulatory protection is required to overcome privacy vulnerabilities generated by the disturbance of the economic atmosphere brought on by global trade and smart city technological advancements.³⁵⁴ In *H v. W*,³⁵⁵ Willis J emphasised the consequences of the modern technology era on personal data and said that the common law must be created in cases where social networking sites violate privacy.³⁵⁶

The development to the POPIA commenced when the SALRC initiated a protracted and time-consuming investigation into legislative change.³⁵⁷ Focusing on the technological hazards that effect personal data protection, the SALRC emphasised that the accessibility of electronic communication through technology and the internet led to an increase in privacy violations and necessitated that governments either develop or update data protection legislation.³⁵⁸ The SALRC's inquiry included a comprehensive examination of the data protection laws of well-established international governments.³⁵⁹ Nonetheless, it

³⁵² See Chapter 1, paragraph 1. above.

³⁵³ The SALRC Final Report at 3.3.43 explains that "the aim of privacy legislation is not to stem the flow of information, but to regulate it."

³⁵⁴ Burns Y and Burger A *A Commentary on the Protection of Personal Information Act* 4-5.

³⁵⁵ *H v W* (2013) 2 All SA 218 (GSJ).

³⁵⁶ *H v W* (2013) 2 All SA 218 (GSJ) at 21.

³⁵⁷ The SALRC Final Report at 1.3.1.

³⁵⁸ The SALRC Final Report 4.1.1-4.1.3.

³⁵⁹ The researched comparative legal jurisdictions included: Australia, Canada, Chile, Ireland, the United Kingdom, the United States of America, the Netherlands, and New Zealand.

is generally acknowledged that the POPIA is based on the EU's legal framework for data protection.³⁶⁰

4.5.2. POPIA Purpose and Application

Section 2 of the POPIA summarises its key goals. The restriction envisioned in this section will need striking a balance between the right to privacy, the right to access information, and the interests of the free movement of information within and without South Africa's boundaries.³⁶¹ Luck argues that the right to privacy, despite being essential, may be limited and balanced, given that data privacy is not limited to domestic policy but is part of the global community and economic and trade issues are therefore relevant.³⁶²

As indicated in the commencement of this discussion, the POPIA was designed in accordance with the European data protection regulatory regime; consequently, it is also vital to guarantee that its requirements for legitimate processing are in line or harmony with international standards.³⁶³ The Information Regulator's mandate under section 40(e) of the POPIA is tied to the achievement of this objective.³⁶⁴

The POPIA applies to the processing of personal information submitted into a record³⁶⁵ by or for a responsible party³⁶⁶ using automated or non-automated means. The Act also applies when the responsible person resides in South Africa, indicating that it has no extraterritorial reach.³⁶⁷ The POPIA applies to a responsible party who is not domiciled in

³⁶⁰ The SALRC Final Report 4.1.1-4.1.3 addressed the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data, and Directive No. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on Free Movement in depth.

³⁶¹ Section 2 (a) (i) and (ii) of the POPIA.

³⁶² Luck R 'POPI - is South Africa keeping up with international trends?' (2014) 44 *De Rebus* 84.

³⁶³ Section 2(b) of the POPIA.

³⁶⁴ This function of the Information Regulator will be discussed in chapter 5.

³⁶⁵ Section 1 of the POPIA defines a 'record' in broad terms.

³⁶⁶ A 'responsible party' is defined by Section 1 of the POPIA as "a public or private body or any other person that, alone or in combination with others, determines the purpose and means of processing personal information."

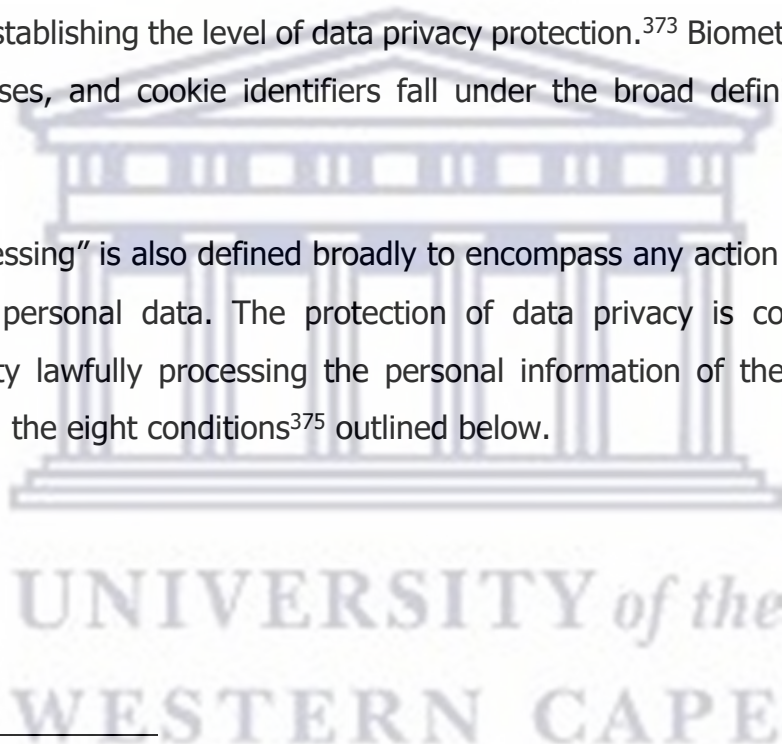
³⁶⁷ Section 3(1) of the POPIA. The term 'non-automated means' is not defined in the POPIA.

South Africa, but who uses automated or non-automated means in South Africa, unless those means are only used to transmit personal information through South Africa.³⁶⁸

4.5.3. Key terms Employed in the POPIA

Key terms such as personal information,³⁶⁹ processing,³⁷⁰ data subject,³⁷¹ and responsible party³⁷² are among the primary terminology used in the POPIA. Without getting into specifics, for the purposes of this study, the terms 'personal information' and 'processing' are crucial for establishing the level of data privacy protection.³⁷³ Biometric data, Internet protocol addresses, and cookie identifiers fall under the broad definition of personal information.³⁷⁴

The term "processing" is also defined broadly to encompass any action undertaken by a third party on personal data. The protection of data privacy is contingent on the responsible party lawfully processing the personal information of the data subject in accordance with the eight conditions³⁷⁵ outlined below.



³⁶⁸ In contrast to the territorial scope of the POPIA, the GDPR extends to non-EU organisations that target EU individuals. Refer to the debate in Chapter 5 below.

³⁶⁹ Section 3(1) (b) (ii) of the POPIA. See Burns Y and Burger-Smidt A A *Commentary on the Protection of Personal Information Act* at 6. The POPIA's Section 3(1)(b)(ii). The authors are of the opinion that in this regard, "the responsible party will not be considered to have processed the personal information: he, she, or it is acting as a mere conduit for the forwarding of personal information; this occurs when the responsible party forwards personal information from one country to another using automated or non-automated means via the Republic."

³⁷⁰ Section 1 of the POPIA defines the term 'processing'.

³⁷¹ Section 1 of the POPIA defines a "data subject" as "a person to whom the personal information Relates."

³⁷² Section 1 of the POPIA defines a 'responsible party' as "a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information."

³⁷³ Section 1 of the POPIA.

³⁷⁴ Roos A 'Data Protection Law in South Africa' at 204.

³⁷⁵ Burns Y and Burger A *Commentary on the Protection of Personal Information Act* at 29.

4.5.4. Conditions for the legitimate Processing of Personal Data

The POPIA stipulates eight conditions³⁷⁶ for lawful processing of personal data by the responsible party:

a) Condition 1: Accountability

The responsible party must ensure that the conditions outlined in Chapter 3 of the Act are met when determining the purpose, acquiring personal information, and carrying out the processing. The POPIA is woven with a thread of accountability, and the responsible party must stay accountable at every stage of processing.³⁷⁷

b) Condition 2: Processing Limitations

Condition 2 limits the reasons for processing, which include legality, minimality, consent, justification, and objection, as well as direct collection from the data subject.

(i) Legitimacy of processing³⁷⁸

The processing of personal information must be conducted properly and appropriately, without violating privacy rights. This responsibility extends beyond the POPIA to include ensuring conformity with other laws, such as the Constitution, other legislation, and international instruments to which South Africa is a signatory.³⁷⁹

(ii) Minimality³⁸⁰

To be eligible for processing, personal data must be appropriate, pertinent, and not excessive given its intended use. It has been suggested that the literal reading of section 10 requires that all three conditions (sufficient, relevant, and not excessive) be met in order for the processing to be considered legitimate. To prevent ambiguity and

³⁷⁶ Chapter 3 of the POPIA.

³⁷⁷ Burns Y and Burger A *Commentary on the Protection of Personal Information Act* 45.

³⁷⁸ Section 9 of the POPIA.

³⁷⁹ Burns Y and Burger A *Commentary on the Protection of Personal Information Act* 48.

³⁸⁰ Section 10 of the POPIA.

interpretation concerns, the minimality criterion should be limited to the specified reason for which the collection of personal information is required.³⁸¹

(iii) Consent, justification, and objection

The POPIA defines "consent" as "any voluntary, precise, and informed expression of will in terms of which permission is given for the processing of personal information."³⁸² The argument has been made that technology provides a barrier to free and informed consent. Big Data in smart cities, for instance, enables data to be utilised beyond the purpose limitation for which consent was obtained, so threatening the function and importance of consent as a legal basis.³⁸³ A holistic approach must be taken to privacy standards in order to strengthen the consent requirement by incorporating privacy by default or privacy by design standards,³⁸⁴ which are not mandated by the POPIA.

(iv) Collection of data directly from the data subject³⁸⁵

In order to ensure that the data subject is in control of the processing, the final criteria of the processing limitation is that the personal information must be collected directly from the data subject. To ensure active control, the POPIA offers a higher level of protection than common law. However, there are exceptions to this rule that diminish its force.³⁸⁶

(c) Condition 3: Purpose specification

The collection of personal information must be clearly defined and lawfully related to an activity or function of the party responsible.³⁸⁷ This requirement encompasses the whole processing lifespan of the personal information obtained for a particular purpose. The

³⁸¹ Burns Y and Burger A *Commentary on the Protection of Personal Information Act* at 51.

³⁸² Section 1 of the POPIA.

³⁸³ Mitrou L 'The General Data Protection Regulation: A Law for the Digital Age?' in Tatiana-Eleni Synodinou et al (ed) (2017) *EU Internet Law*: Springer 39-40.

³⁸⁴ Mitrou L 'The General Data Protection Regulation: A Law for the Digital Age?' in Tatiana-Eleni Synodinou et al (ed) (2017) *EU Internet Law*: Springer at 42.

³⁸⁵ Section 12(1) of the POPIA.

³⁸⁶ The exceptions are set out in section 12(1)(2) of the POPIA.

³⁸⁷ Section 13(1) of the POPIA.

responsible party will be obligated to inform the data subject of the intended use from the time personal information is collected until its destruction.

Nevertheless, given the provisions of section 14(3) of the POPIA, personal information may be kept for a number of years.³⁸⁸ The responsible party is required to destroy, delete, or de-identify a record as soon as it is reasonable to do so once the retention of the record is no longer permitted pursuant to the retention period that has expired as stipulated in section 14 (1) and (2).³⁸⁹

d) Condition 4: further limitations on processing

Section 13 requires that any further processing of personal information must be in conformity with or compatible with the original purpose for which it was gathered.³⁹⁰ Compatibility is evaluated by considering the factors outlined in section 15(2) of the POPIA.³⁹¹ If any of the elements listed in section 15(3)(a) to (f) are met, further processing is not deemed incompatible with the initial intended purpose of collection.

e) Condition 5: Quality of Information

A responsible party is obligated by section 16 of the POPIA to take reasonable steps to ensure that personal information is complete, accurate, not misleading, and current.³⁹² In this regard, the responsible party must consider the purpose for which personal information is acquired or further processed.³⁹³

³⁸⁸ The POPIA permits the responsible party, in the absence of a law or code of conduct, to retain the record for a time period that affords the data subject a reasonable opportunity to request access. Personal information records may be kept for longer periods for historical, statistical, or research purposes, subject to the implementation of sufficient measures against their use for any other purpose.

³⁸⁹ Section 14(4) of the POPIA.

³⁹⁰ Section 15(1) of the POPIA.

³⁹¹ Section 15(2) of the POPIA.

³⁹² Section 16(1) of the POPIA.

³⁹³ Section 15(2) of the POPIA.

(f) Condition 6: Openness

Sections 14 and 51 of the PAIA require a responsible party to keep documentation pertaining to all processing operations under its authority.³⁹⁴ Similar to section 13(1), section 18(1) requires the responsible party to take reasonable steps to inform the data subject of the specifics of the gathered personal information.³⁹⁵

(g) Condition 7: Security Measures

In accordance with this condition, in order to protect the integrity and confidentiality of personal data, the responsible party must take appropriate, reasonable technical and organisational measures to prevent loss, damage, or destruction of such data, as well as unauthorised access to or processing of such data.³⁹⁶ Technical and implementation of risk identification prior to the implementation of security measures are necessary.³⁹⁷ The proposed POPIA Regulations suggest that the Information Regulator is leaning toward a risk-based approach to POPIA compliance.³⁹⁸

This condition assumes self-regulation may not be adequate to counteract the effects of modern digital technologies, which have the potential to circumvent the responsible party's security measures. In addition to being unique, it is not recognised under established common law rules. However, the POPIA does not include the need (design and default) to ensure that privacy safeguards are 'built in' to the technology from the design stage; ideally, such a provision should be included in the POPIA's accountability condition.³⁹⁹

³⁹⁴ Section 17 of the POPIA.

³⁹⁵ Section 18(1)(a) through to (h) of the POPIA has a list of the details. See also J Neethling 'Features of the Protection of Personal Information Bill' (2013) 75 *Journal of Contemporary Roman-Dutch Law* 241-255.

³⁹⁶ Section 19(1)(a) and (b) of the POPIA.

³⁹⁷ Section 19(2) of the POPIA.

³⁹⁸ Regulation 4 of the draft POPIA Regulations.

³⁹⁹ See Condition 1 above p67. See Chapter 2 para 2.4.

(h) Condition 8: Participation of data subject

This condition is derived from the openness principle and offers the data subject two specific rights to actively control their personal information: the right of access and the right to edit or erase it. The Common law does not grant such a right to the data subject.

4.6 SOFT LAW

4.6.1 *The Integrated Framework for Urban Development*

The Integrated Urban Development Framework (IUDF) is the policy framework of the South African government that directs the growth and administration of urban regions in the future. Its objective is to steer urban growth toward a sustainable growth model of compact, integrated, and coordinated cities and towns in order to accomplish the desired spatial transformation outcome.⁴⁰⁰ Given the particular conditions and problems facing South Africa's urban areas, the IUDF seeks to foster a shared understanding between government and society about the development of inclusive, resilient, resource-efficient, and livable urban settlements. It is essential that not only are all smart city efforts aligned with the mission and objectives of the IUDF, but that they are also incorporated into the integrated urban planning of all municipalities.⁴⁰¹ Essential principles of the IUDF will be further analysed in Chapter 6.

4.6.2 *The District Development Model*

The government adopted the District Development Model (DDM)⁴⁰² in 2019 as an operational model for enhancing the coherence and effectiveness of government service

⁴⁰⁰ Cooperative Governance and Traditional Affairs (CoGTA). 2016. *Integrated Urban Development Framework* (hereafter: IUDF) available at http://www.sacities.net/wp-content/uploads/2017/10/IUDF%202016_WEB-min.pdf (accessed on 23 July 2022).

⁴⁰¹ IUDF 2016.

⁴⁰² District Development Model (hereafter DDM), available at <https://businesstech.co.za/news/government/440169/dlamini-zuma-outlines-new-municipal-regulations-for-south-africa/>. (accessed 25 July 2022).

delivery and economic development. The concept, which is aligned with the NDP and the IUDF, intends to encourage collaborative planning among the three domains of government and state agencies so that they can operate in concert and with an eye toward impact.⁴⁰³ According to Dr. Nkosazana Dlamini-Zuma, Minister of Cooperative Government and Traditional Affairs, the DDM aims to promote local governance by eliminating silo planning, budgeting, and execution.⁴⁰⁴ The 44 districts and eight metropolitan municipal spaces have been recognized as combined planning, budgeting, and implementation impact areas.⁴⁰⁵

The Smart Cities Framework aligns with the DDM's principles. Partnerships are important for the effective implementation of any smart city effort.⁴⁰⁶ Partnerships are also central to the DDM: The "one plan", "one budget", and "one space" for each district or metropolitan area will serve as a magnet to attract contributions from all government agencies, the corporate sector, and civil society organizations for the implementation of developmental programmes.⁴⁰⁷ In addition, the DDM seeks to be a realistic instrument for improving cooperative governance.⁴⁰⁸ This pragmatic approach compliments the SCF's view that any smart city program should be begun by first gaining an awareness of what is already accessible and occurring in a municipality, prior to taking action.⁴⁰⁹ Therefore, any smart city intervention must be consistent with the content of the One Plan prepared for the relevant district or metropolitan municipality.⁴¹⁰

⁴⁰³ DDM, available at <https://businesstech.co.za/news/government/440169/dlamini-zuma-outlines-new-municipal-regulations-for-south-africa/>. (accessed 25 July 2022).

⁴⁰⁴ DDM, available at <https://businesstech.co.za/news/government/440169/dlamini-zuma-outlines-new-municipal-regulations-for-south-africa/>. (accessed on 25 July 2022).

⁴⁰⁵ DDM, available at <https://businesstech.co.za/news/government/440169/dlamini-zuma-outlines-new-municipal-regulations-for-south-africa/>. (accessed on 25 July 2022).

⁴⁰⁶ DDM, available on <https://iudf.co.za/news/what-is-the-district-development-model-and-has-it-replaced-the-iudf/> (accessed 25 July 2022).

DDM 2020 available at <https://iudf.co.za/news/what-is-the-district-development-model-and-has-it-replaced-the-iudf/> (accessed 25 July 2022).

⁴⁰⁸ MISA strategic plan, available at http://www.misa.gov.za/wp-content/uploads/2020/03/MISA_STRATEGIC-PLAN_2020-2025.pdf (accessed 27 July 2022) (hereafter MISA).

⁴⁰⁹ MISA 2020.

⁴¹⁰ MISA 2020.

4.6.3 Smart-specific policies, initiative and guidelines

Following a worldwide surge in smart city activities, the International Organisation for Standardisation (ISO) recognised the need for standardisation. After five years of research and consultation with city leaders worldwide, ISO 37106:2018, Sustainable cities and communities – Guidance on building smart city operating models for sustainable communities, was issued in August 2018.⁴¹¹ The finalisation of the standard occurred in the first quarter of 2020. This standard provides guidelines on enabling processes for integrating technology and data in conjunction with organisational change to establish an open, collaborative, citizen-centric, and digitally enabled operating model" for a sustainable future city.⁴¹²

In addition to the ISO, the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC), the British Standards Institute (BSI), the European Telecommunications Standards Institute (ETSI), the United Nations specialised agency for information and communication technologies (ITU), and the International Electrotechnical Commission (IEC) all contribute to or formulate smart city standards.⁴¹³

4.7 CONCLUSION

It has been argued that the principles of the law of delict provide limited protection of data privacy because active control of the processing of personal data by the data subject is not acknowledged. Specific protection of data privacy has not been acknowledged by courts employing traditional delictual principles in circumstances involving privacy violations.⁴¹⁴ The examination of this issue is ongoing and demonstrates that data privacy

⁴¹¹ OECD, ISO, available at https://www.oecd.org/gov/regulatory-policy/ISO_Full-Report.pdf (accessed 29 July 2022).

⁴¹² OECD, ISO, available at https://www.oecd.org/gov/regulatory-policy/ISO_Full-Report.pdf (accessed 29 July 2022).

⁴¹³ Smart city technology, available at <https://rodger.global-linguist.com/smart-city-technology-trends-part-3/> (accessed 29 July 2022).

⁴¹⁴ Roos A 'Data Protection: Explaining the International Backdrop and Evaluating the Current South

is not expressly provided for in section 14; however, case law demonstrates that the Constitutional Court has extended privacy protection to informational (data) privacy. The sentiment of Neethling must be reflected in that the Constitution requires the legislature to pass data protection legislation.⁴¹⁵

As discussed in chapter 2, the collection and processing of personal data in smart city eco-system is not a problem in and of itself; however, it raises data vulnerability, threatens its security, may infringe on the right to privacy, and undermines the confidence of the data subject, particularly in online transactions. The POPIA's active control principles are unique to a data protection regulatory regime. It was proven that the POPIA exceeds the protection of privacy afforded by common law by protecting the data subject's rights that are inherent to the requirements for legitimate processing.⁴¹⁶ The authors of a recent article analysing the case *Black Sash Trust v. Minister of Social Development*⁴¹⁷ explain the misuse and unlawful processing of social security personal information and call for the POPIA to come into full force and effect so that the Information Regulator can become fully operational and exercise its enforcement powers to protect against privacy violations.⁴¹⁸ Moreover, given the challenges faced by South Africa's urban areas, guidelines such as the IUDF and DDM seek to foster a shared understanding between government and society about the development of inclusive, resilient, resource-efficient, and livable urban settlements in preparation for smart cities. The next chapter expounds on a comparative analysis on data protection laws in various jurisdictions.

African Position' 422.

⁴¹⁵ Neethling *Neethling's Law of Personality* 17.

⁴¹⁶ Neethling *Features of the Protection of Personal Information Bill* 14.

⁴¹⁷ *Black Sash Trust v Minister of Social Development and Others (Freedom Under Law NPC Intervening)* (CCT48/17) [2017] ZACC 8; 2017 (5) BCLR 543 (CC); 2017 (3) SA 335 (CC).

⁴¹⁸ Batchelor B and T Wazvaremhaka 'Balancing financial inclusion and data protection in South Africa: *Black Sash Trust v Minister of Social Development*' (2019) 136(1) *SALJ* 112.

CHAPTER 5

COMPARATIVE ANALYSIS OF DATA PROTECTION LAWS IN VARIOUS JURISDICTIONS

5.1. INTRODUCTION

It is evident that ongoing technology advances in smart cities have increased the likelihood of privacy violations.⁴¹⁹ As noted in Chapter 4, DPAs have a legislative obligation to monitor the impact of technologies and to recommend revisions to their data protection regulatory regimes to ensure that such laws keep pace with the rapid advancement of technology.

While not all aspects of international data protection legislative reform may be applicable to South Africa, the POPIA must continue to be appropriate to meet the goal of preserving the individual's right to privacy in a technological era that is constantly evolving. This chapter examines the characteristics of legal reform in the data protection regimes of the U.S. and the EU to determine the extent to which such legal reform may promote data privacy protection in the South African context by enhancing the protection afforded to data subjects to counter the negative impact of new or emerging technologies on data privacy.

5.2. DATA PROTECTION IN THE U.S.

The U.S. applies a sectoral approach to data protection laws. There is no comprehensive federal data protection law. Instead, the federal legislation safeguards data in sector-specific scenarios. These laws only apply to certain industries, such as "healthcare, education, communication, and financial services in the event of data collecting on

⁴¹⁹ Refer to Chapter 1, paragraph 1.2 above for a discussion on new and emerging communications and information technologies which pose data protection challenges.

children"⁴²⁰ In other words, most U.S. privacy regulations restrict data processing based on the context in which data are used (e.g., healthcare, banking, education).⁴²¹ Ultimately, privacy regulation in the United States is highly contextual, sectoral, based on common law, federal and state laws, and largely dependent on private law or explicit agreements that are afterwards enforced by federal legislation.⁴²²

The Federal law enforcement is the responsibility of the Federal Trade Commission (hereafter: FTC), but state attorneys general are also involved in consumer privacy protection.⁴²³ The Fair Information Practice Principles, which provide a standard set of principles that have served as the basis for many privacy and data protection laws around the world, including those in the United States, the European Union, and elsewhere, were first outlined in 1973 by an advisory committee of the United States Department of Health, Education, and Welfare⁴²⁴ and subsequently incorporated into the United States Privacy Act of 1974.⁴²⁵

5.2.1. *The U.S. Constitution's Fourth Amendment*

The Fourth Amendment to the United States Constitution outlines the limits of privacy rights in the U.S. It protects citizens from the government's "unreasonable searches and seizures." In *Katz v. United States*,⁴²⁶ the Supreme Court found that the government's warrantless eavesdropping of a person making a phone conversation from a phone booth exceeded the defendant's subjective expectation of privacy, which might be justified by the need to prevent social norms.⁴²⁷ A privacy claim under the Fourth Amendment invokes

⁴²⁰ Terry N 'Existential challenges for health care data protection in the United States' (2017) 3 *Ethics Med Public Health* 19.

⁴²¹ Schwartz P and Solove D 'Reconciling personal information in the United States and European Union' (2014) 102 *Calif L Rev* 877–916).

⁴²² DeVries W 'Protecting privacy in the digital age' (2003) 18 *Berkeley Tech LJ* 283–311.

⁴²³ Cortez EK' *Data protection around the world-privacy laws in action* 1ed (2021) 232.

⁴²⁴ Sec'y Advisory Comm. On Automated Personal Data Sys., U.S. Dept. of Health, Educ. and Welfare, Records, Computers, and the Rights of Citizens (1973), available at <https://aspe.hhs.gov/report/records-computers-and-rights-citizens>. (accessed on 13 July 2022).

⁴²⁵ *Privacy Act of 1974*, 5 U.S.C. § 552a, as amended.

⁴²⁶ 389 U.S. 347 (1967).

⁴²⁷ 389 U.S. 347, 361 (1967).

the reasonableness requirement and the expectation of privacy test. Consequently, privacy concerns in the U.S. are evaluated based on the requirements of an “objective third party” or a person with “reasonable sensibility”.

As a penumbra of rights derived or implied by the Constitution, the U.S. Supreme Court has also affirmed the privacy rights of persons in connection to birth control⁴²⁸, same-sex relationships,⁴²⁹ and abortion.⁴³⁰ These rights to privacy have sometimes been referred to as unenumerated rights.⁴³¹

The majority of states have enacted privacy torts, which guarantee fundamental privacy rights in the U.S, either by common law, legislation, or by interpreting their state constitutions.⁴³² Therefore, Included in privacy torts are invasion of seclusion,⁴³³ public exposure of private facts,⁴³⁴ appropriation,⁴³⁵ and false light.⁴³⁶ These torts protect four distinct individual rights, all of which revolve around the "right to be left alone," as famously stated by Warren and Brandeis in an 1890 law review article.⁴³⁷ Both the reasonableness standard established by US common law and the First Amendment have limited the scope of privacy torts.⁴³⁸

5.2.2. Sectoral laws

The most distinguishing feature of U.S. privacy and data protection law is its regulatory scope. U.S. privacy laws/ regulations are generally of sectoral orientation. For instance,

⁴²⁸ *Griswold v Connecticut*, 381 U.S. 479 (1965).

⁴²⁹ *Lawrence v Texas*, 539 U.S. 558 (2003).

⁴³⁰ *Roe v Wade*, 410 U.S. 113 (1973).

⁴³¹ Helscher D 'Griswold v. Connecticut and the unenumerated right of privacy' (1994). 15 N Ill U L Rev 33–61.

⁴³² Cortez, *Data protection around the world-privacy laws in action*, 235.

⁴³³ American Law Institute: 'Restatement (Second) of Torts' § 652B (1977) (hereafter "Restatement (Second) of Torts").

⁴³⁴ Restatement (Second) of Torts § 652D (1977).

⁴³⁵ Restatement (Second) of Torts § 652C (1977).

⁴³⁶ Restatement (Second) of Torts § 652E (1977).

⁴³⁷ Warren and Brandeis 'The Right to Privacy' (1890) 5 HLR 193.

⁴³⁸ Cortez, *Data protection around the world-privacy laws in action*, 235.

distinct regulations are employed to the data processing undertakings of government agencies and private companies.⁴³⁹ Further, businesses that operate in multiple sectors of the economy or process different types of data are governed by different rules.⁴⁴⁰ Therefore, sectoral laws define the appropriate level of protections for discrete/diverse data processing functions, such as consumer transactions, law enforcement, and health record maintenance.⁴⁴¹ In a nutshell, sectoral regulations consider dangers to privacy and data protection to be unique to particular data processing businesses or technologies.⁴⁴²The numerous sector-specific data protection regulations are outlined below.

5.2.2.i The Fair Credit Reporting Act⁴⁴³ (and the Fair and Accurate Credit Transactions Act (Pub. L. No. 108–159) which amended the Fair Credit Reporting Act).

Consumer reporting agencies, those who use consumer reports (such as lenders), and providers of consumer reporting information are all covered (such as a credit card company). The term "consumer reports" refers to any message issued by a consumer reporting agency (CRA) about a consumer's creditworthiness, credit history, credit capacity, character, and general reputation that is used to determine a consumer's eligibility for credit or insurance.⁴⁴⁴ A CRA is required to take reasonable measures to ensure the correctness of information.⁴⁴⁵ Where data is "inaccurate, incomplete, or unverifiable," a CRA must immediately rectify it.⁴⁴⁶

⁴³⁹ Schwartz P 'The EU-US privacy collision: A turn to institutions and procedures' (2013) 126 *Harv L Rev* 1966– 2009.

⁴⁴⁰ Schwartz, *The EU-US privacy collision: A turn to institutions and procedures*, 126.

⁴⁴¹ See general discussion in Swire P and Ahmad K, *Foundations of Information Privacy and Data Protection: A survey of global concepts, Laws and practices*. (International Association of Privacy Professionals, Portsmouth, 2012).

⁴⁴² Reidenberg J, 'Resolving conflicting international data privacy rules in cyberspace' (2000) 52 *Stan L Rev* 1315–1371).

⁴⁴³ 15 U.S.C. §1681.

⁴⁴⁴ 15 U.S.C. § 1681(d)(1).

⁴⁴⁵ 15 U.S.C. § 1681e (2013).

⁴⁴⁶ 15 U.S.C. § 1681i (a)(5)(A) (2013).

5.2.2.ii Electronic Communications Privacy Act (Electronic Communications Privacy Act,1986)⁴⁴⁷

This Act Prohibits wiretapping of others' conversations without judicial sanction or previous consent.⁴⁴⁸ Moreover, it prohibits the disclosure or use of information obtained through illicit wiretapping or electronic eavesdropping.⁴⁴⁹

5.2.2.iii The Computer Fraud and Abuse Act, 1986⁴⁵⁰

The purpose of the Computer Fraud and Abuse Act of 1986 seeks to prevent and penalise hacking-related actions, which the Act defines as "unauthorised access" to protected computers.⁴⁵¹ Moreover, the Act prohibits people and organisations from exceeding their "authorised access"⁴⁵² Included in the definition of "protected computers" are those used by financial institutions, the U.S. government, and computers used in or influencing interstate or foreign commerce or communication.⁴⁵³ The term "Damage" in the Act is defined as any degradation to the integrity or availability of data, a program, a system, or information, as defined by the Act.⁴⁵⁴

5.2.2.iv The Children's Online Privacy Protection Act, 1998⁴⁵⁵

The COPAA was created to protect children under the age of thirteen when they use the Internet by regulating how websites collect, use, and disclose their personal

⁴⁴⁷ 18 U.S.C. §2510.

⁴⁴⁸ Doyle C (2012) *Privacy: an overview of the Electronic Communications Privacy Act*. Congressional Research Service, available at <https://www.hsdl.org/?view&did¼725508> (accessed on 15 July 2022).

⁴⁴⁹ Doyle C (2012) *Privacy: an overview of the Electronic Communications Privacy Act*. Congressional Research Service, available at <https://www.hsdl.org/?view&did¼725508> (accessed on 15 July 2022).

⁴⁵⁰ 18 U.S.C. §1030.

⁴⁵¹ 18 U.S.C. §1030.

⁴⁵² 18 U.S.C. § 1030(e)(6).

⁴⁵³ 18 U.S.C. § 1030(e)(2).

⁴⁵⁴ 18 U.S.C. §1030(a)(5).

⁴⁵⁵ 15 U.S.C. §§ 6501, et seq.

information.⁴⁵⁶ Under the COPPA, a website's "operator"⁴⁵⁷ is required to notify a child's parent or guardian of any information collected from the child.⁴⁵⁸ Hence, the COPPA applies to both children's websites and "general audience" websites if the operator has actual knowledge that the site is collecting personal information from minors.⁴⁵⁹

5.2.2.v The Gramm-Leach- Bliley Act, 1999⁴⁶⁰

The Gramm-Leach- Bliley Act mandates that financial institutions respect the privacy of their customers and maintain the security and confidentiality of their non-public personal information.⁴⁶¹ Hence this is essential for the provision of financial services, financial institutions may share personal information with other businesses.⁴⁶² Information may be shared with credit bureaus or financial regulators.⁴⁶³

5.2.2.vi. The Federal Trade Commission

The Federal Trade Commission (FTC) governs the processing of personal information in the United States and plays a crucial role in protecting the privacy of American consumers.⁴⁶⁴ It achieves so primarily through Section 5 of the Federal Trade Commission Act, which grants it the ability to maintain independent oversight over unfair and deceptive commercial practices and to take enforcement action against them.⁴⁶⁵ The FTC has the authority to issue injunctions and civil fines against firms that violate the privacy

⁴⁵⁶ Robert Hasty Et.al 'Data Protection Law In USA, Advocates for International Development,' available at https://www.neighborhoodindicators.org/sites/default/files/course-materials/A4ID_DataProtectionLaw%20.pdf (accessed on 17 June 2022).

⁴⁵⁷ 16 C.F.R. pt 312.2.

⁴⁵⁸ 16 C.F.R at pts. 312.4(c), 312.5.

⁴⁵⁹ 16 C.F.R at pts. 312.3.

⁴⁶⁰ 16 C.F.R. pt 312.2. at § 6801.

⁴⁶¹ 16 C.F.R at § 6801(a).

⁴⁶² Vincete DM and De Vasconsels S, *Data Protection in the Internet*, (2020) 412.

⁴⁶³ Vincete DM and De Vasconsels S, *Data Protection in the Internet*, 412.

⁴⁶⁴ Solove D Hartzog W *The FTC and the new common law of privacy*, 114 Colum L Rev 583–676 (2014).

⁴⁶⁵ 15 U.S.C § 45.

rights of their customers, and it therefore dominates the enforcement of privacy standards.⁴⁶⁶

The FTC has been lauded for its ability to influence the behavior of large corporations, additionally, it has also been criticised for neglecting to act on highly criticised practices that have generated privacy concerns, such as Facebook's online tracking methods.⁴⁶⁷ The FTC is the primary agency charged with enforcing federal privacy laws such as the GLBA,⁴⁶⁸ FCRA,⁴⁶⁹ and COPPA.⁴⁷⁰ In recent years, the government has taken a more active role in preserving consumer privacy by issuing consent decrees in settlements with companies accused of violating privacy rules.⁴⁷¹

5.2.2.vii California Consumer Privacy Act ⁴⁷²

The enactment of the California Consumer Privacy Act (CCPA), a comprehensive privacy law that detractors have called 'California's GDPR,' is by far the most significant privacy development in the United States in recent years.⁴⁷³ The CCPA has a significant impact, to California's size and Silicon Valley's location, wherefore, businesses around the United States and the world are evaluating its implications.⁴⁷⁴

The CCPA took effect on January 1, 2020. It does not repeal CalOPPA, but it does provide consumers with enhanced data protection when dealing with covered businesses.⁴⁷⁵ In

⁴⁶⁶ Solove D and Hartzog W 'The FTC and the new common law of privacy,' (2014)114 *Colum L Rev* 583–676.

⁴⁶⁷ Cortez E.K, Data Protection around the world-Privacy laws in action, 235.

⁴⁶⁸ 15 U.S.C. §§ 6801-6809 (2012).

⁴⁶⁹ 15 U.S.C. § 1681 (2012).

⁴⁷⁰ 15 U.S.C. §§ 6501-6506 (2012).

⁴⁷¹ 20 USC § 1232g.

⁴⁷² *The California Consumer Privacy Act (CCPA)*, A.B. 375, 2017 General Assembly, Reg., Session, (Cal.2018).

⁴⁷³ Raul et al 'The Privacy, Data Protection and Cyber Security' (2019) *Law review*, 416).

⁴⁷⁴ RAUL et al, *The Privacy, Data Protection and Cyber Security Law, Review*, 416.

⁴⁷⁵ CCPA Tipping the Scales: Balancing Individual Privacy with Corporate Innovation for a Comprehensive Federal Data Protection Law Notes Williams, Sahara Page 217.

terms of the Act, a covered business is required to disclose to a 'consumer'⁴⁷⁶ all 'personal information,' which includes the following:

Information that identifies, refers to, characterizes, is reasonably capable of being associated with, or may reasonably be related to, a particular consumer or household, directly or indirectly. Personal information includes, but is not limited to, a non-exhaustive list of ten information categories and inferences drawn from them, if it identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be associated with, a particular consumer or household.⁴⁷⁷

Smart apps in smart city eco-systems commonly gather a variety of persistent and semi-persistent identifiers, both for internal operations and to earn advertising revenue. All of these, including resettable advertising identifiers, are explicitly covered by the CCPA and must be disclosed.⁴⁷⁸ A privacy policy must describe the types of data gathered, including 'biometric information'⁴⁷⁹, health insurance information, education information, and financial information. Before drafting a privacy policy for a mobile application, developers must carefully assess whether the information collected would infer any of the above or any other personal information (including sensitive information like location or sexual, religious, or political preferences).⁴⁸⁰

The CCPA resolves a number of CalOPPA's shortcomings, to begin with, it addresses the content of a privacy disclosure in a more comprehensive manner which prior to or at the time of collection, a business must identify the kinds of personal information it will collect

⁴⁷⁶ §1798.140(g) of CCPA

⁴⁷⁷ §1798.140(o)(1) of CCPA.

⁴⁷⁸ Cf Sec1 of POPIA, which includes the word 'online identifier' or 'other particular attributed to an individual' in the definition of 'personal information' but does not define the term further to make it apparent that it includes a device identification. It is nevertheless possible to argue persuasively that a device identification constitutes personal information under POPIA because it can be linked to an identifiable individual.

⁴⁷⁹ CCPA §1798.140(b). 'Biometric information' comprises of personal features, such as deoxyribonucleic acid (DNA), can be used to determine an individual's identity. A biometric identification template, such as a faceprint, a minutiae template or a voiceprint, can be retrieved from images of the iris, retina, fingerprints, face, hand, palm, vein patterns and voice recordings.

⁴⁸⁰ §1798.140(m) of CCPA.

and the purposes for which it will be used.⁴⁸¹ If it has not sold or shared personally identifiable information for commercial reasons, it must report this fact.⁴⁸² Additionally, a consumer must be informed of his or her right to request information about the personal information gathered about him or her, as well as the right to have that information deleted, as well as the procedures for exercising those rights.⁴⁸³ While a corporation is not forbidden from incentivising voluntary sharing of extra information through reasonable and fair means,⁴⁸⁴ it must refrain from discriminating against consumers and get opt-in consent for any financial incentive plan.⁴⁸⁵

While the CCPA does not address data minimisation directly, it may indirectly encourage businesses to delete information immediately when it is no longer required for one-time use and to anonymise information as soon as possible, as businesses are not required to respond to consumer requests regarding such data.⁴⁸⁶ Furthermore, if a business has “actual information” that a consumer is under the age of 16, the business must first obtain the consumer's affirmative authorisation to sell (i.e. opt-in consent) (or a parent or guardian of a child under 13).⁴⁸⁷ Beyond the constraints of legitimate research and compliance with regulatory requirements, the lawful use and retention of personal information is limited to 'internal purposes' that a customer would reasonably anticipate in the context of his or her relationship with the business.⁴⁸⁸ The California Attorney General is authorised to enforce the CCPA's requirements with statutory fines of up to \$7,500 per infringement.⁴⁸⁹

⁴⁸¹ §1798.100(b) of CCPA.

⁴⁸² §1798.115(c)(1) & (2) of CCPA.

⁴⁸³ §1798.130(a)(5)(B) of CCPA.

⁴⁸⁴ §1798.125(a) of CCPA.

⁴⁸⁵ §1798.125(b) of CCPA.

⁴⁸⁶ §1798.100(e) of CCPA.

⁴⁸⁷ §1798.120(c) of CCPA.

⁴⁸⁸ §1798.105(d) of CCPA.

⁴⁸⁹ §1798.140(c)(1) of CCPA.

5.3 DATA PROTECTION IN THE EU

5.3.1 INTRODUCTION

Globally, the EU has been at the forefront of data protection law and policy formulation, and the POPIA was primarily based on earlier EU data protection legal instruments and guidelines.⁴⁹⁰ It has been noted that, under the Bill of Rights, the courts are required to consider international law;⁴⁹¹ therefore, the Information Regulator should consider any defining aspect of legal developments with specific regard to legislative reform influenced by technological changes adopted by foreign jurisdictions in order to improve data privacy protection.

The EU recognises data protection as a distinct right from privacy.⁴⁹² The EU Directive⁴⁹³ was implemented as a comprehensive data protection regime in response to a proposal by the European Commission (EC) to address inconsistencies in member state data protection regime.⁴⁹⁴ The courts interpret EU legislation in conjunction with the European Data Protection Board, whose interpretations have persuasive but non-binding force.⁴⁹⁵ If national justices have difficulty interpreting EU regulations, they may refer the matter to the Court of Justice of the European Union in certain circumstances (hereafter CJEU).⁴⁹⁶

⁴⁹⁰ The South African Law Reform Commission Project 124 'Privacy and Data Protection Report' 163-4 dated 2009 available at https://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf, accessed on 15 June 2021.

⁴⁹¹ Burns Y and A Burger-Smidt A Commentary on the Protection of Personal Information Act (2018) 2.

⁴⁹² Article 7 of the Charter of Fundamental Rights of the European Union.

⁴⁹³ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

⁴⁹⁴ Hoofnagle CJ et al 'The European Union general data protection regulation: what it is and what it means?' (2019) 28(1) *Information & Communications Technology Law* 65-98 available at <https://www.tandfonline.com/doi/citedby/10.1080/13600834.2019.1573501?scroll=top&needAccess=true>. (accessed on 29 September 2019).

⁴⁹⁵ Article 19(3)(b) of the Treaty on European Union.

⁴⁹⁶ Article 19(3)(b) of the Treaty on European Union.

EU data protection regulations are interpreted by the CJEU, the highest court in the EU.⁴⁹⁷ For example, it granted data subjects the 'right to be forgotten'⁴⁹⁸ and ruled recently that active consent is required for the storage of cookies used to track online browsing behaviour.⁴⁹⁹ The EU data protection regime witnessed a regulatory paradigm shift in May 2018 when the GDPR⁵⁰⁰ and the Law Enforcement Directive were enacted as part of a legal reform package.⁵⁰¹ The GDPR completely repealed the 1995 EU Directive.⁵⁰²

Globally, the GDPR harmonises data protection law across the EU in order to maintain uniformity in the legal systems of member states and to prevent unnecessary administrative burdens.⁵⁰³ Importantly, it takes into account the rapid technological advancements that rendered the EU Directive of 1995 insufficient for providing a high level of data privacy protection.⁵⁰⁴ The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Privacy and Electronic Communications) (EC Directive) (Amendments) (Regulations 2011) (PECR) governs direct marketing, as

⁴⁹⁷ *Maximillian Schrems v Data Protection Commissioner* [2015] Case C-362/14 ECLI:EU:C:2015:650.

⁴⁹⁸ Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos* (May 13, 2014) available at <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN> (accessed 01 October 2022).

⁴⁹⁹ Mitrou L 'Data Protection, Artificial Intelligence and Cognitive Services: Is The General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof?'" December 2013 available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914, accessed 7 October 2022.

⁵⁰⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> (accessed on 30 July 2021). The GDPR entered into force on 24 May 2016 and was effective as of 25 May 2018.

⁵⁰¹ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC accessed on 30 July 2021. The Enforcement Directive was passed on 5 May 2016 and came into effect on 6 May 2018.

⁵⁰² See Article 94(1) of the GDPR.

⁵⁰³ Recital 9 of the preamble of the GDPR.

⁵⁰⁴ Recital 6 of the preamble of the GDPR.

well as the processing of location and traffic data and the use of cookies and comparable technologies such as smart cities.⁵⁰⁵ Hence, A draft of the proposed Regulation on Privacy and Electronic Communications (e-Privacy Regulation) to replace the existing e-Privacy Directive was released by the European Commission.⁵⁰⁶

The proposed modifications to the e-Privacy Regulation will:

- a) Make it more difficult to gain consent for cookies;
- b) Attempt to place the onus of getting consent for the usage of cookies on the browsers of website visitors; and
- c) Make it more difficult to gain consent for direct marketing and require it to satisfy the GDPR standard; existing exclusions are likely to be kept.⁵⁰⁷

5.3.2. Changes to the EU Data Protection Framework

The General Data Protection Regulation is technologically neutral in that it protects data subjects⁵⁰⁸ regardless of the form or type of technology used to process personal data.⁵⁰⁹ It has been characterised as technology-independent legislation whose provisions exhibit a technological neutrality approach despite the absence of technology-specific terminology.⁵¹⁰ The discussion that follows below does not provide a comprehensive analysis of all changes to the EU data protection regime, but rather focuses on the novelty provisions of the GDPR, which include enhanced rights for data subjects and obligations imposed on data controllers⁵¹¹ to prevent data privacy breaches caused by the use of technology. The POPIA does not address these provisions directly. The novelty provisions

⁵⁰⁵ Alen *et al*'The privacy, Data protection and Cyber security' (2019) *law review* 374 (hereafter "*Data protection*").

⁵⁰⁶ Alen *Data protection* 375.

⁵⁰⁷ Alen *Data protection* 376.

⁵⁰⁸ Article 4(1) of the states that the GDPR does not contain a separate definition of a 'data subject' but encompasses the description of a data subject in the definition of 'personal data'. Unlike the POPIA, the GDPR does not recognise a juristic person as a data a subject.

⁵⁰⁹ Recital 15 of the preamble of the GDPR.

⁵¹⁰ Recital 15 of the preamble of the GDPR.

⁵¹¹ See Article 4(7) of the GDPR.

discussed in the following section prescribe how personal data can be processed by new or emerging technologies.

5.3.3 Definitions

The GDPR pertains to any data that directly or indirectly identifies or could identify an individual, including public and non-sensitive information.⁵¹² The widespread application of the GDPR in a smart city has created the perception that the GDPR requirements will apply to all forms of data in the future, thereby becoming “the law of everything”.⁵¹³ The definition of “personal data” includes “online identifiers” and “location data,”⁵¹⁴ which is consistent with the online environment. For instance, the GDPR obligations will apply when a device is linked to an IP address, since an IP address can be indirectly linked to an internet user's identity.⁵¹⁵

With reference to Recital 26 of the GDPR, Mitrou asserts that despite being ambiguous, identifiability is a dynamic criterion that takes into consideration both the technology in use at the time of processing and technological advancements.⁵¹⁶ Thus, identifiability is triggered, regardless of the technology employed, when the identity of the data subject is isolated, either directly or indirectly.⁵¹⁷ Examples of personal data include the name, email address, biometric information, facial recognition, location, preferences, and search history.⁵¹⁸ Furthermore, the GDPR expands the definition of ‘processing’.⁵¹⁹ Technologies

⁵¹² Hoofnagle CJ et al ‘The European Union general data protection regulation: what it is and what it means?’ *Information & Communications Technology Law* (note 517 above).

⁵¹³ N Purto ‘The law of everything. Broad concept of personal data and future of EU data protection law’ (2018) *Law, Innovation and Technology* 40 available at <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176>, accessed on 30 September 2022.

⁵¹⁴ Recital 30 of the GDPR. See further L Mitrou ‘The General Data Protection Regulation: A Law for the Digital Age?’ in Tatiana-Eleni Synodinou et al (ed) *EU Internet Law*: Springer (2017) 24.

⁵¹⁵ Recital 30 of the GDPR. See further L Mitrou ‘The General Data Protection Regulation: A Law for the Digital Age?’ in Tatiana-Eleni Synodinou et al (ed) *EU Internet Law*: Springer (2017) 24.

⁵¹⁶ Mitrou L “Data Protection, Artificial Intelligence and Cognitive Services: Is The General Data Protection Regulation (GDPR) ‘Artificial Intelligence-Proof?’” (note 522 above) 30.

⁵¹⁷ Recital 26 of the GDPR.

⁵¹⁸ Recital 26 of the GDPR.

⁵¹⁹ Article 4(2) of the GDPR.

such as Blockchain and Artificial Intelligence or machine learning, which are automated means that perform operations on personal data, their continued storage, and/or further processing, lie squarely within the scope of Article 4(2) of the GDPR.

5.3.4 Extraterritorial Application

The GDPR has extraterritorial application,⁵²⁰ so it is applicable apply even if a company has no physical presence in the EU.⁵²¹ The European Court of Justice (ECJ) established the criteria for determining the territorial scope of EU data protection law.⁵²² The GDPR will apply extraterritorially if two conditions are met, namely, when processing activities relate to the offering of goods or services, regardless of whether a payment of the data subject is required to such data subjects in the Union.⁵²³ and when processing activities relate to the monitoring of behaviour within the Union.⁵²⁴ This implies that South African businesses must comply with the GDPR if they engage in the activities listed in GDPR Article 3(2)(a) and (b).

5.3.5. Data Subject's Rights

Similar to the GDPR, data subjects have a set of rights governing how their personal data is processed.⁵²⁵ By default, controllers are obligated to disclose information on activities

⁵²⁰ Article 3(1) of the GDPR.

⁵²¹ See for example Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, in which the Court determined that Google Spain is an establishment of Google Inc. and that the selling of advertising activities was carried out in the context of the activities of the Spanish establishment, so the search engine had to comply with EU law.

⁵²² See for example C-230/14, *Weltimmo S.R.O. V. Nemzeti A Datvedelmi Es Informacioszabadsagh Atosag (Hungarian DPA)*, 1.10.15. The ECJ determined that factors such as the degree of stability of the arrangements and the effective exercise of activities must be interpreted in light of the specific nature of the economic activities and service provision concerned.

⁵²³ Article 3(2)(a) of the GDPR.

⁵²⁴ Article 3(2)(b) of the GDPR.

⁵²⁵ Article 15 of GDPR.

taken in response to requests within one calendar month, with limited option to extend this period by two months if the request is burdensome.⁵²⁶

Amongst the rights afforded to data subjects are the following:

1. Right of access⁵²⁷

A data subject has the right to request access to and a copy of his or her personal data, as well as the required information regarding how the data controller has used the data.

2. Right to rectify⁵²⁸

Subjects have the right to have inaccurate or outdated personal data repaired or updated without delay.

3. Right to be forgotten⁵²⁹ ('right to be erased')

Individuals have the right to have their personal information removed. The right is not absolute; it only applies under certain conditions, such as when the controller no longer requires the data for the purposes for which they were collected or otherwise lawfully processed, or as a result of the controller's successful exercise of the right to object or withdrawal of consent.

4. Right to processing restriction⁵³⁰

Data subjects have the right to restrict the processing of their personal data in specific circumstances. These include instances in which the correctness of the data is

⁵²⁶ Article 15 of GDPR.

⁵²⁷ Article 15 of GDPR.

⁵²⁸ Article 16 of GDPR.

⁵²⁹ Article 17 of GDPR.

⁵³⁰ Article 18 of GDPR.

contested, the processing is unlawful, the data are no longer required except for the data subject's legal rights, or the controller's legitimate grounds for processing are contested.

5. Right to object⁵³¹

Data subjects have the right to object when processing is done on the basis of the data controller's legitimate interests or in the public interest. Controllers will be forced to suspend data processing until they can demonstrate "compelling legitimate reasons" that outweigh the rights of the data subject. In addition, data subjects have an unfettered right to object to the processing of their personal data for direct marketing purposes at any time.

6. The right to be exempt from automated decision-making, including profiling⁵³²

Automated decision-making (including profiling) that has a substantial impact on the data subject is only permitted if necessary for entering into or performing a contract, authorised by UK law, or the data subject has given explicit, for example, opt-in consent.

5.4 IS THERE A LACK OF ACCOUNTABILITY?

The responsible party must ensure that the conditions outlined in Chapter 3 of the Act are met when determining the purpose, acquiring personal information, and carrying out the processing. The POPIA is woven with a thread of accountability, and the responsible party must stay accountable at every stage of processing.⁵³³

However, certain instruments require notification prior to engaging in any subsequent processing that is permissible on the basis that it is compatible with the original

⁵³¹ Article 21 of DPA.

⁵³² Article 22 of EU GDPR and Art 49 of DPA, 2018.

⁵³³ See condition 1 on page 62.

purpose.⁵³⁴ A broader discussion on the PbD concept can be found in chapter 2 paragraph 2.4.

5.5 CONCLUSION

Greenleaf argues that data protection laws outside of Europe have already converged on more than half of the higher standards required in Europe since the 1990s.⁵³⁵ 120 countries have enacted EU data privacy laws, making the GDPR a “gold standard” for data protection reform in a number of countries.

It is clear that the GDPR establishes stringent requirements to strengthen data privacy protection reform in the ever-changing digital environment. Although the UK left the EU, it cannot depart from the protections afforded by the GDPR and has taken legislative measures to ensure that its domestic data protection regime is aligned with the GDPR.

In contrast to the European Union's data protection policy, which in many ways represents the gold standard of privacy laws, the predominant approach in the U.S. is rooted in consumer protection regulations.⁵³⁶ However, sectoral legislation in the U.S. have the advantage of covering nearly everything in a more efficient manner, despite being complex and expensive. The following chapter will now discuss principles for an ideal smart city regulatory framework for SA and can potentially be an export model for other countries too.

⁵³⁴ Art 13(3) & art 14(4) of GDPR.

⁵³⁵ Greenleaf G 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108' (2011) 2 *International Data Privacy Law* 77.

⁵³⁶ McGeeveran W 'Friending the privacy regulators' (2016) 58 *Arizona Law Review* 959-961.

CHAPTER 6

SMART CITY FRAMEWORK

6.1 INTRODUCTION

Smart cities have the potential to improve the delivery of public services and address a variety of societal issues, such as controlling traffic congestion,⁵³⁷ lowering carbon emissions,⁵³⁸ promoting effective waste management,⁵³⁹ improving public health outcomes, building affordable housing, and making it easier for citizens to access public services.⁵⁴⁰ The previous chapter examined the characteristics of legal reform in the data protection regimes of the U.S. and the EU to determine the extent to which such legal reform may promote data privacy protection in the South African context. Privacy concerns play a significant role in the development and outcome of prior proposed smart cities initiatives.⁵⁴¹ This chapter now discusses an ideal framework as well as privacy principles for smart cities. It further discusses what lessons SA can learned from local and international initiatives.

UNIVERSITY of the
WESTERN CAPE

-
- ⁵³⁷ See Press Release N.Y.C. Dep't of Transp., 'NYC DOT Announces Expansion of Midtown Congestion Management System, Receives National Transportation Award' available at https://www1.nyc.gov/html/dot/html/pr2012/pr12_25.shtml. (accessed 23 June 2023).
- ⁵³⁸ Copenhagen 'World Smart Cities Forum' available at <https://worldsmartcities.org/copenhagen/?msckid=c1451bbbd15911eca302d0f6add159e9> (accessed 23 June 2023).
- ⁵³⁹ See Levi Sumagaysay 'San Francisco's Trash Bins Get Smart' *The Mercury News* available at <https://www.mercurynews.com/2019/02/27/san-franciscos-trash-bins-get-smart/> (accessed 19 June 2023).
- ⁵⁴⁰ Life SG 'Smart Nation Singapore' available at <https://www.smartnation.gov.sg/initiatives/strategic-national-projects/lifesg> (accessed 27 June 2023).
- ⁵⁴¹ David GC and Eliot Brown 'Google Parent Nears Deal to Build Its Vision of a City in Toronto' *Wall STJ* available at <https://www.wsj.com/articles/alphabets-city-building-unit-nears-development-deal-in-toronto-1507142561> (accessed 23 June 2023).

6.2 IDEAL FRAMEWORK FOR SMART CITIES

6.2.1 *The Integrated Framework for Urban Development*

The SCF complements the IUDF, so smart city projects directed by the SCF contribute directly to the achievement of the IUDF objectives of spatial integration, inclusion, access, growth, and governance.⁵⁴²

The urban growth and management model⁵⁴³ of the IUDF focuses on creating compact urban expansion, providing interconnected infrastructure, and coordinating urban government and investments. It asserts that innovative urban infrastructure and technology can enable the capture of the economic benefits of denser urban forms. While all nine IUDF policy levers could be assisted by smart city projects, at least three levers identify ICT as a supporting technology:

Policy Leverage 4: Integrated Urban Infrastructure identifies an intervention to invest in ICT infrastructure and literacy:⁵⁴⁴ Successful ICT investments should lead to effective governance structures, the availability of infrastructure and technological platforms, and the closing of digital divides.⁵⁴⁵ As a means of enhancing rural-urban connections, the IUDF promotes improved access to ICT infrastructure (e.g., via high-speed internet and cell coverage).⁵⁴⁶ Policy Leverage 8: Effective Urban Governance necessitates the improvement of communication and the application of technology. "Government, and local government in particular, must use technology more to inform, empower, and include individuals in its activities."⁵⁴⁷

Locally, various national sector departments and other organisations have engaged the theme of smart cities.⁵⁴⁸ The year 2020 witnessed the release of a National Smart

⁵⁴² IUDF 2016.

⁵⁴³ IUDF 2016.

⁵⁴⁴ IUDF 2016, p73.

⁵⁴⁵ IUDF 2016, p73.

⁵⁴⁶ IUDF 2016, p104.

⁵⁴⁷ IUDF 2016, p104.

⁵⁴⁸ Department Telecommunications and Postal Services (DTPS). 2020. National Smart Commun

Communities Framework by the Department of Telecommunications and Postal Services (DTPS).⁵⁴⁹ The purpose of the DTPS framework is to prepare municipalities for data-driven, efficient service delivery.⁵⁵⁰ The framework expounds on data as the guiding principle and essential component of smart city development,⁵⁵¹ meaning that having an overview of the data value chain in cities can assist a deeper understanding of the digital environment in ways that enable us to modify the physical area.

6.3 EXAMPLES OF SMART INITIATIVES IN SOUTH AFRICA

Despite the fact that smart city thinking has not been mainstreamed in South Africa, there are examples of the concept being adopted:

In a summary of the City of Johannesburg's smart city plan, Backhouse⁵⁵² described the city's approach as having "modest objectives, beginning with connectivity." The City of Johannesburg lays significant emphasis on connecting its smart city initiatives with its IDP procedure. Officially announcing its desire to become a smart city in 2013, the city adopted a Smart City Strategy and Implementation Roadmap in 2014. Within the municipality, a Smart City Unit was formed. Lawrence Boya, director of the Smart City Unit for the City of Johannesburg, explains the objective of the smart city initiative.

A smart city programme must be fully integrated into the Integrated Development Plan (IDP) of the city, becoming one with the IDP. A holistic strategy is essential when executing a smart city initiative. The goal of creating a smart city should be a social objective, not merely a city-led approach. All stakeholders and communities must be

Framework. [https://nationalgovernment.co.za/department_annual/344/2020-department:telecommunications-and-postal-services-\(dtps\)-annual-report.pdf](https://nationalgovernment.co.za/department_annual/344/2020-department:telecommunications-and-postal-services-(dtps)-annual-report.pdf). Also Refer to Chapter 4, paragraph 4.7.3 above for a discussion on smart-specific policies and initiatives locally and international initiatives.

⁵⁴⁹ National Smart Communities Framework, 2020.

⁵⁵⁰ National Smart Communities Framework, 2020.

⁵⁵¹ National Smart Communities Framework, 2020.

⁵⁵² Backhouse J *et al* 'Smart, Sustainable Cities and Settlements' (2015) Johannesburg: South African Cities Network.

involved, and a smart city must be citizen-centric, reflecting the preferences of inhabitants and meeting their needs.⁵⁵³

Current smart city initiatives in the City of Johannesburg consist of integrated transport systems, last-mile connectivity via optical fibre and Wi-Fi, and automated and integrated police enforcement management systems. An example of a smart intervention resulted from a research undertaken by Johannesburg Water in an effort to increase the efficiency of its workforce.⁵⁵⁴ Ntshavheni Mukwevho⁵⁵⁵, Managing Director of Johannesburg Water, one of the findings of this study suggested that teams spend too much time at the depots in the morning in addition to going to work sites.⁵⁵⁶

Several private sector projects to establish precincts or satellite cities as smart cities have also taken place in Johannesburg.⁵⁵⁷ The most notable is the Modderfontein development, which claimed to create a new urban region characterised by narratives of intelligent and sustainable urbanisation.⁵⁵⁸ The initial plans were not implemented, and Brill and Reboredo⁵⁵⁹ contend that the project posed a risk of reinforcing Johannesburg's existing patterns of inequality and causing environmental damage in the region. The City of Johannesburg opposed the proposed development because several of the concepts were in conflict with the city's overall objectives.⁵⁶⁰

⁵⁵³ Civictech: 'How Africa can implement smart cities) available at <https://civictech.africa/how-africa-can-implement-smart-cities/> (accessed on 1 September 2022).

⁵⁵⁴ Civictech: 'How Africa can implement smart cities) available at <https://civictech.africa/how-africa-can-implement-smart-cities/> (accessed on 1 September 2022).

⁵⁵⁵ Mukwevho N 'Johannesburg Water Smart Service Delivery' Unpublished presentation at the Third Water Resilient Cities event held on 5 November 2019, Nelson Mandela Bay Municipality.

⁵⁵⁶ Mukwevho N 'Johannesburg Water Smart Service Delivery' Unpublished presentation at the Third Water Resilient Cities event held on 5 November 2019, Nelson Mandela Bay Municipality.

⁵⁵⁷ Brill F and Reboredo R 'Failed Fantasies in a South African Context: The Case of Modderfontein, Johannesburg' (2018) 30 *Urban Forum* 171-189 (hereafter "*the case of Modderfontein*").

⁵⁵⁸ Brill F and Reboredo R *the case of Modderfontein* 172.

⁵⁵⁹ Brill F and Reboredo R *the case of Modderfontein* 173.

⁵⁶⁰ Brill F and Reboredo R *the case of Modderfontein* 175.

In 2000, the City of Cape Town unveiled the first edition of its Smart City Strategy (the most recent review took place in 2016). The objective of the plan was to achieve existing city goals such as job development, economic growth, and increasing resident participation, as well as to construct a system of high-quality public services that could be made available to a wide variety of individuals. The approach established the groundwork for substantial investments in business process integration and Automation to improve city system and service delivery efficiencies⁵⁶¹ led to the deployment of an Enterprise Resource Planning (ERP) system, which continues to act as the municipality's digital backbone.⁵⁶²

The Smart City Playbook⁵⁶³ recognised Cape Town as one of the smart cities in Africa in 2016. The newspaper praised the City of Cape Town for adopting an approach appropriate to its local environment. Instead of pursuing huge initiatives that its residents cannot profit from, it is focusing on what it deems to be their needs.⁵⁶⁴ There are also a number of smart city developments started by the private sector in the greater Cape Town area. The City of Cape Town authorised the Harbour Arch mixed-use precinct at the end of 2019.⁵⁶⁵ Moreover, upscale residential communities in the greater metropolitan area have invested in smart city technologies such as biometric access control and license plate recognition.⁵⁶⁶

6.4 PRIVACY CONSIDERATIONS FOR SMART CITIES

In the U.S. with regards to governmental surveillance, some commentators have expressed concerns that the adoption of smart city technologies run the risk of stifling First Amendment expression, as residents may be less willing to participate in free speech

⁵⁶¹ City of Cape Town, 2016 in Boyle, 2019.

⁵⁶² Boyle, 2019.

⁵⁶³ The Smart City Playbook is a publication by Machina Research that documents the best practices of cities throughout the world. Nokia sponsored the 2016 competition.

⁵⁶⁴ Green J 'The Smart City Playbook: smart, safe, sustainable. Machina Research Strategy Report' (2016).

⁵⁶⁵ Boyle, 2019.

⁵⁶⁶ Boyle, 2019.

and public assembly if they believe the city is recording them.⁵⁶⁷ For instance, the Office of Science and Technology Policy found in the White House's recently released Blueprint for an AI Bill of Rights that people and communities "should be free from unchecked surveillance" and that technologies like AI should not restrict the exercise of civil rights and civil liberties, such as with regard to voting, peaceful assembly, speech, or association.⁵⁶⁸ On the other hand, city governments at large have been affected by cybersecurity attacks, for example, in 2018 a ransomware attack on the city of Atlanta forced the local government to shut down its computer systems.⁵⁶⁹

6.5 SAFEGUARDING PRIVACY IN SMART CITIES

The Fair Information Practices, is a government report from the 1970s that serves as the cornerstone for contemporary U.S. privacy regulation of the criteria for transparent government information processing.⁵⁷⁰ For example, in cases where the collection of personal information differs from what consumers might anticipate, the FTC has advised that entities make disclosures to consumers "at a relevant time and in a prominent manner" and provide choice to individuals.⁵⁷¹ Global privacy frameworks are not uniform when it comes to the content that is required in such notices.⁵⁷²

⁵⁶⁷ Muggah R and Walton G 'Smart Cities Are Surveilled Cities' *Foreign Policy* available at <https://foreignpolicy.com/2021/04/17/smart-cities-surveillance-privacy-digital-threats-internet-of-things-5g/> 9 (accessed 25 June 2023).

⁵⁶⁸ Office of Science and Technology Policy 'The White House, Blueprint for an AI Bill of Rights, Privacy 6, 30, 34 available at <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf> (accessed 27 June 2023).

⁵⁶⁹ Blinder A and Perloth N 'A Cyberattack Hobbles Atlanta, and Security Experts Shudder' *N.Y. Times* available at <https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html> (accessed 27 June 2023).

⁵⁷⁰ Federal Privacy Council, Fair Information Practice Principles available at <https://www.fpc.gov/resources/fipps/> (accessed 28 June 2023).

⁵⁷¹ FTC 'Protecting Consumer Privacy in an Era of Rapid Change' available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> (accessed 29 June 2023).

⁵⁷² Fussell S 'The City of the Future Is a Data-Collection Machine' *The Atlantic* available at <https://www.theatlantic.com/technology/archive/2018/11/google-sidewalk-labs/575551/> (accessed 29 June 2023).

Privacy by Design (PbD) can allay privacy risks in smart cities and this concept is globally recognised in privacy frameworks, such as the GDPR, FTC guidelines, and most recently the proposed legislative text for the American Data Privacy and Protection Act, the pre-eminent federal legislative framework on privacy in the United States.⁵⁷³ For example, Seattle has implemented a programmatic privacy review procedure to assist government officials gather and utilize data.⁵⁷⁴ This Privacy program is designed to provide structure and guidance for city agencies to increase confidence in how residents' personal information is used.⁵⁷⁵ A privacy assessments, like the one implemented in Seattle, can serve as a component of privacy by design program.⁵⁷⁶ Moreover, In considering cybersecurity safeguards smart cities can learn from other governmental entities, such as those at the federal and state levels, identifying support and resources from grant programs, such as the \$1 billion cybersecurity grant program for state and governments allocated in the Bipartisan Infrastructure Law.⁵⁷⁷

6.6 LESSONS THAT CAN BE LEARNED FROM LOCAL AND INTERNATIONAL INITIATIVES

Smart city efforts should be developed from the outset so that they can be monitored and assessed.⁵⁷⁸ This will facilitate the sharing of learning with peers. While projects or interventions should not be replicated without being adapted to the local context (what works in one place may not work in another), lessons can be learned from both local and international initiatives. Below are few lessons learned:⁵⁷⁹

⁵⁷³ See Art. 25 of GDPR and American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

⁵⁷⁴ City of Seattle 'About the Privacy Program' available at <https://www.seattle.gov/tech/initiatives/privacy/privacy-program> (accessed 27 June 2023).

⁵⁷⁵ City of Seattle 'Privacy Reviews of City Technology' (hereafter: "Privacy Program", available at <https://www.seattle.gov/tech/initiatives/privacy/privacy-reviews> (accessed on 29 June 2023).

⁵⁷⁶ City of Seattle *Privacy Program*.

⁵⁷⁷ Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, § 70612(a), 135 Stat. 429, 1272, 1285) (2021) available at <https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf> (accessed 30 June 2023).

⁵⁷⁸ Boyle, 2019.

⁵⁷⁹ Boyle, 2019.

Smart city retrofitting is a time-consuming process. For example, Cape Town released the initial edition of their Smart City Strategy in 2000 (the most recent assessment was in 2016).⁵⁸⁰ The city's digital plan is based on the ERP system from the early 21st century.⁵⁸¹ Smart technologies and initiatives are not obligated to exclude particular elements of society.⁵⁸² For instance, Rwanda's Irembo platform can be accessible via unstructured supplementary service data (USSD), which does not require an internet connection, allowing users with basic mobile phones to access it.⁵⁸³

Ethical ramifications should be carefully considered when using some smart city technology.⁵⁸⁴ For instance, Gaffney and Robertson⁵⁸⁵ stated that certain smart technologies used to collect data for Rio's City Operations Centre are only implemented in certain geographic locations (in this case some of the wealthiest areas of Rio de Janeiro). They contend that when there are more cameras and surveillance, municipal officials intervene more, and that the system exacerbates the digital and socioeconomic divides that define the city.⁵⁸⁶

Smart city projects should not be driven by technology; rather, they should be in response to challenges.⁵⁸⁷ For instance, Johannesburg Water initially found issues with respect to the productivity of their personnel. As a subsequent stage, they investigated the causes of the problem, and only then did they consider whether an ICT solution would solve some of the obstacles.⁵⁸⁸ It may be conceivable to adapt and copy certain smart

⁵⁸⁰ Boyle, 2019.

⁵⁸¹ Backhouse 2020.

⁵⁸² Irembo available at: <https://irembo.gov.rw/rolportal/en/eservice-by-category?cat=LGV&menu-highlight=CAT> (accessed on 1 September 2022).

⁵⁸³ Irembo available at: <https://irembo.gov.rw/rolportal/en/eservice-by-category?cat=LGV&menu-highlight=CAT> (accessed on 1 September 2022).

⁵⁸⁴ Gaffney C and Robertson C Smarter than Smart: Rio de Janeiro's Flawed Emergence as a Smart City (2018) 25(3) *Journal of Urban Technology* 47-64. (hereafter "Gaffney C and Robertson C").

⁵⁸⁵ Gaffney C and Robertson C 2018.

⁵⁸⁶ Gaffney C and Robertson C 2018.

⁵⁸⁷ Mukwevho, 2019.

⁵⁸⁸ Mukwevho, 2019.

technologies and efforts for usage in multiple areas under certain conditions.⁵⁸⁹ For instance, Kenya, Cameroon, and Nepal have replicated India's Safe city platform.⁵⁹⁰

The implementation of smart city technologies frequently depends on an array of governance regulations.⁵⁹¹ For instance, Quayside in Toronto, Canada encountered difficulties due to the lack of a national data governance plan prior to the start of project.⁵⁹²

6.7 CONCLUSION

The SCF needs to be implemented into practice in order to have an impact. In order to execute the smart city framework, municipalities would need assistance from the DCoG, the provinces, SALGA, and other National Departments. This could entail aid with conducting various assessments to determine a municipality's readiness for smart cities, the creation of a regional smart city strategy, and the design and implementation of smart cities.

Indeed, all-inclusive smart cities have a crucial role to play in adopting a privacy framework such as through the adoption of principles like those described in this chapter to address privacy concerns and foster public trust and confidence in smart cities projects. The following chapter will provide conclusions and recommendations.

⁵⁸⁹ Nesta "Five bottom up smart city initiatives" available at: <https://www.nesta.org.uk/blog/five-bottom-up-smart-city-initiatives-from-india/> (accessed on 3 September 2022).

⁵⁹⁰ Nesta "Five bottom up smart city initiatives" available at: <https://www.nesta.org.uk/blog/five-bottom-up-smart-city-initiatives-from-india/> (accessed on 3 September 2022).

⁵⁹¹ Waterfront Toronto 'Waterfront home' available at: <https://waterfrontoronto.ca/nbe/portal/waterfront/Home> (accessed 7 September 2022).

⁵⁹² Waterfront Toronto 'Waterfront home' available at: <https://waterfrontoronto.ca/nbe/portal/waterfront/Home> (accessed 7 September 2022).

CHAPTER 7

CONCLUSION AND RECOMMENDATIONS

7.1 OVERVIEW

Analysts predict that with smart city initiatives being implemented, the smart cities market will reach \$7 billion in revenue by 2030.⁵⁹³ In fact, since 2019, 379 completely built smart cities exist in 61 different countries.⁵⁹⁴ With all the advantages that the 4IR and smart cities have brought, disadvantages such as data privacy issues are to the forefront on a national and international scale. In light of these challenges, this study examined the the protection of personal Information in Smart Cities and lessons to be learned for South Africa from the European Union and the United States.

Moreover, due to the borderless nature of the technologies used to collect, store, and transmit personal data on a global scale, data privacy issues resulting from technological advances are a global concern. Thus, the research considered the technological foresight activities of well-established foreign DPAs as well as the reform of data protection legislation in the EU and the USA. In order for the POPIA to remain pertinent, adequate, and effective in the digital age, this chapter provides the Legislature and Information Regulator with recommendations to strengthen the protection of personal information in South Africa. This chapter is divided in two different parts. The first part concludes this research and challenges faced with regards to protection of personal information in the

⁵⁹³ Precedence Research 'Smart Cities Market Size to Surpass US\$7,162.5 BN by 2030' *Global Newsire* available at <https://www.globenewswire.com/en/news-release/2022/05/10/2439944/0/en/Smart-Cities-Market-Size-to-Surpass-US-7-162-5-BN-by-2030.html>. (accessed 23 June 2023).

⁵⁹⁴ Mathis S and Kanik A 'Why You'll be Hearing a lot Less About 'Smart Cities,' *City Monitor* <https://citymonitor.ai/government/why-youll-be-hearing-a-lot-less-about-smart-cities> (accessed on 23 June 2023).

smart city eco-system. The second and the last part of this research highlight certain perspectives and recommendations to those issues.

7.2 CONCLUSION

The Information Regulator can plan or structure its technological foresight activities using these foreign DPAs' activities as solid guidelines. The lesson learnt from the EU and US Data Protection Acts have taught us that the Information Regulator must amass expertise in the ICT field in order to remain abreast of the impact of smart technologies on data privacy. In Africa, data protection laws and institutions are still in their formative stages. Privacy is safeguarded by both human rights instruments and data privacy laws.⁵⁹⁵

The SALRC initiated its investigation into the preservation of data privacy since 2009, the global digital landscape has shifted significantly, with significant implications for data privacy protection. South Africa will be required to keep up with international best practices. Foreign jurisdictions, including the EU and the US have begun reforming their data protection regulatory regimes in response to technological impacts.

The analysis of the EU data protection regime revealed that the EU Directive was repealed in its entirety by the GDPR in large part because it lacked the substance necessary to safeguard data privacy in the digital age. This study focused on the novelty provisions of the GDPR, including enhanced rights for data subjects and the obligations imposed on data processors to prevent data privacy breaches resulting from the use of technology.⁵⁹⁶ These novelty provisions are not specifically addressed by the POPIA. Unlike the U.S., the EU also regulates online privacy through the ePrivacy Directive. Moreover, South African enterprises are affected by the GDPR's extraterritorial application.⁵⁹⁷ Scholars refer to the GDPR as a "gold standard" for countries reforming their data protection because it is recognised as international best practice. In contrast to the European Union's data

⁵⁹⁵ See discussion in Chapter 3.

⁵⁹⁶ See discussion in chapter 5, paragraph 5.3.1.

⁵⁹⁷ See discussion in Chapter 5, paragraph 5.3.4.

protection policy, which in many ways represents the gold standard of privacy laws, the predominant approach in the U.S. is rooted in consumer protection regulations. However, sectoral legislation in the U.S. have the advantage of covering nearly everything in a more efficient manner, despite being complex and expensive.

Given the fact that the POPIA was primarily based on the EU Directive, it is essential that it be reformed in accordance with the provisions discussed in Chapter 5, section 5.3. The additional reforms adopted by the EU and the US that afford data subjects enhanced protection for their personal information must also be considered. Data protection is no longer limited to domestic protection, despite the fact that there is no one-size-fits-all approach to regulatory reform. This is due to the fact that the risks associated with technological advances transcend territorial borders.

7.3 RECOMMENDATIONS

7.3.1 Recommendations on Technological Foresight

Section 47(7) of the POPIA only mandates that the Information Regulator appoint a person with specialised knowledge temporarily or for a specific matter. Long-term, the Information Regulator may decide to establish a council of experts in accordance with its independence so that it can swiftly respond to the ever-changing privacy and technological landscape.

To remain at the vanguard of technological advancements, it is also recommended that the Information Regulator participate as an active member in international forums that address data privacy issues impacted by technology.⁵⁹⁸ The Regulator should also prioritise a smart technology strategy, similar to those adopted by the DPAs in the EU

⁵⁹⁸ Such as the International Working Group on Data Protection in Telecommunications.

and the US by establishing specific technology objectives to address new technologies or disruptive business models and how these could be regulated in certain industries.

7.3.2 Recommendations for Reform

The concept of PbD⁵⁹⁹ is a valuable, innovative requirement in the GDPR that is a preventative measure to enhance data privacy protection by ensuring that technologies used to process personal data are designed to include controls to mitigate the risks of unlawful processing. Technology hinders free and informed consent, and the use of technologies such as Big Data enables the utilisation of personal data outside the scope of the purpose for which consent was granted. The concept of consent's function and significance as a legal ground is therefore diminished. The POPIA does not include the design and default obligation to assure that privacy protections are 'built in' to technology from the outset. Focusing on data protection by design and default requirements, the Information Regulator's research strategy must incorporate preventative measures to mitigate the effects of technology. To encourage the use of PETs, the POPIA will need to be amended to include privacy by design and default as a standard requirement, as is presently mandated by the GDPR.⁶⁰⁰

In order to mitigate the negative effects of technology from the inception, it is recommended that the POPIA's accountability condition include design and default provisions. Alternately, it is recommended that the Information Regulator consider issuing a binding code of conduct that targets the manufacturers of technologies to ensure that privacy controls are embedded from the design stage (data protection by design and default) of the technologies.⁶⁰¹

The regulation of the online environment, especially as it pertains to electronic communications services in public communication networks, necessitates a higher level

⁵⁹⁹ See discussion in Chapter 2, paragraph 2.4.

⁶⁰⁰ See discussion in Chapter 5, paragraph 5.3.4.

⁶⁰¹ See Chapter 5, paragraph 5.3.4, page 66.

of data privacy protection. It is recommended that the Information Regulator evaluate the requirements of the ePrivacy Directive and the proposed ePrivacy Regulation and recommend to Parliament the enactment of specific legislation or the amendment of the POPIA in order to regulate online privacy comprehensively.

Given that the POPIA was based on the 1995 EU Directive, it would be irresponsible for the Information Regulator not to consider the provisions of the GDPR when reforming data protection law in South Africa to counteract the negative effects of rapid technological advancement. It is strongly recommended that South Africa adopt a holistic approach to data protection law reform and amend the POPIA to include the following key GDPR provisions to provide a higher level of data privacy protection:

- (a) The POPIA should incorporate the GDPR identifiability criterion, extending the POPIA's applicability to all forms of data identifying a data subject, whether directly or indirectly and regardless of the technology employed;⁶⁰²
- (b) The term "processing" in the POPIA should be expanded in accordance with Article 4 of the GDPR so that operations on personal data, continued storage thereof, and/or further processing by automated technologies such as Blockchain, cloud computing, Artificial Intelligence, or machine learning fall squarely within the definition of "processing" and are therefore subject to the conditions for the lawful processing of personal information;
- (c) To provide equivalent protection to data subjects and in light of the fact that some technologies process personal data outside of South Africa, the POPIA should also establish an extraterritorial scope of application, subject to the same restrictions imposed by the GDPR.
- (d) The POPIA should incorporate the GDPR consent requirements and compel the responsible party to demonstrate that the data subject consented to the processing of his or her personal data.
- (e) The specific rights provided by the right to be forgotten give internet users greater control over the use and veracity of their personal information. As a result, it is

⁶⁰² See discussion in Chapter 5, paragraph 5.3.1.

proposed that section 24 of the POPIA be made more explicit in order to provide data subjects with the right to request the erasure or further processing of their personal information held by responsible parties, as stipulated in Article 17 of the GDPR.

Due to the technologically sensitive nature of data protection law, it is recommended that the POPIA include a periodic review mechanism similar to that of the Privacy Act, which is a crucial provision for ensuring that the POPIA remains adequate and effective in a rapidly evolving technological smart city ecosystem.

7.3.3 Governance and implementation Foresight

Despite significant academic and media concern about privacy issues, we only have a 'rudimentary' understanding of how personal information is acquired and handled. It is critical to consider both the positive and negative implications of each technology used in a smart city in order to ensure transparency and trust striking a balance between the smart city and its residents. The Minister of Electricity in South Africa⁶⁰³ must attend to ensure that there is accessibility of continuous uninterrupted electricity for smart cities to exist. It is recommended that the government allocate and dispense a budget in order to cater for solar powered lighting, generators and invertors.

The Smart City Framework needs to be implemented into practice and in order to be execute the Smart City Framework, municipalities would need assistance from the DCoG, the provinces, SALGA, and other National Departments. This could entail aid with conducting various assessments to determine a municipality's readiness for smart cities, the creation of a regional smart city strategy, and the design and implementation of smart cities. ⁶⁰⁴ It is recommended that the South African government implements the Agenda 2030 and Agenda 2063 goals to make Smart cities a reality in South Africa.

⁶⁰³ See discussion in Chapter 2, paragraph 2.2.1 on loadshedding, page 23.

⁶⁰⁴ See overall discussion in chapter 6.

BIBLIOGRAPHY

1. PRIMARY SOURCES

1.1 South Africa

Statutes

- Constitution of the Republic of South Africa Act No. 108 of 1996.
- Consumer Protection Act No. 68 of 2008.
- Electronic Communications and Transactions Act No. 25 of 2002.
- Electronic Communications Act 36 of 2005.
- Freedom of Information Act of 2018.
- National Credit Act No. 34 of 2005.
- Protection of Personal Information Act No. 4 of 2013
- Promotion of Access to Information Act No. 2 of 2000.

Case law

- *Bernstein v Bester NO 1996 (2) SA 751 (CC).*
- *H v W(2013) 2 All SA 218 (GSJ).*
- *Jooste v National Media Ltd 1994 (2) SA 634 (C).*
- *NM and Others v Smith and Others (Freedom of Expression Institute as Amicus Curiae) 2007 (7) BCLR 751 (CC) 32.*

- *Minister of Justice and Constitutional Development and Others v Prince (Clarke and Others Intervening)*.
- *Mistry v Interim Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC)*.
- *O'Keeffe v Argus Printing and Publishing Co Ltd 1954 (3) SA 244(C)*.
- *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk 1977 (4) SA 376 (T)*.

1.3 International Law

Statutes and International Conventions

Conventions

- African Charter of Human and People's Rights of 1981.
- African Charter on the Rights and Welfare of the Child of 1990.
- African Union Convention on cyber security and protection of personal data protection of 2014.
- American Convention on Human Rights of 1967.
- American Convention on Human Rights of 1969.

- American Declaration of the Rights and Duties of Man O.A.S. Resolution XXX of 1948.
- Convention on the Rights of Child of 1989.
- Convention on the Rights of Persons with Disabilities of 2007.
- European Convention on Human Rights (ECHR) of 1950.
- International Covenant on Civil and Political Rights (ICCPR) of 1966.

Statutes

- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

- Organisation for Economic Cooperation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data, 23 September 1980.
- California Consumer Privacy Act of 2018.
- Constitutive Act of the African Union 2000.
- Charter of Fundamental Rights of The European Union.
- Fair Credit Reporting Act.
- Federal Trade Commission Act of 1914.
- Gramm-Leach- Bliley Act of 1999.
- The General Data Protection Regulation 2016/679.
- The Online Privacy Protection Act of 2004.

Case law

- *Breyer v Bundesrepublik Deutschland* Case C-582/14 ECLI:EU:C:2016:779
- *Google v. CNIL* and *C-136/17, G.C. and Others v. CNIL* C-507/17.
- *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos*

(AEPD), *Mario Costeja González* [2014] Case C-131/12 ECLI:EU:C:2014:317.

- *Griswold v. Connecticut* [1965] 381 U.S. 479.
- *Lawrence v Texas* [2003] 539 U.S. 558.
- *Maximillian Schrems v Data Protection Commissioner* [2015] Case C-362/14 ECLI:EU:C:2015:650.
- *Mike Campbell (Pvt) LTD & others v. Republic of Zimbabwe*, [2007]. SADC (T) 2/07.
- *Roe v Wade* [1973] 410 U.S. 113.

2. SECONDARY SOURCES

Books

- Burdon M, *Digital data collection and information privacy law* 1 ed (2020) Cape Town: Cambridge University Press.
- Chertoff M *Exploding Data: Reclaiming Our Cyber Security in the Digital Age* 1 ed (2018) New York: Atlantic Monthly Press.
- Cortez EK *Data protection around the world-privacy laws in action* 1 ed (2021) New York: Springer.
- Currie I & De Waal JD *The Bill of Rights handbook* 6 ed (2013) Cape Town: Juta.
- Davey R & Jansen LD *Social Media in the Workplace* 1 ed (2017) South Africa: Lexis Nexis

- Duncan J *Stopping the Spies: Constructing and resisting the surveillance state in South Africa* 1 ed (2018) Johannesburg: Wits University Press.
- Edwards L and Waelde C eds *Law and the Internet* 3 ed (2009) chs14, 15 and 16 Oxford: Hart Publishing.
- Gutwirth S et al *Reinventing Data Protection?* 9 ed (2009) Dordrecht: Springerlink.
- Jeffrey L et al *international law: Norms, Actors and Process* 2d ed (2006) 95 USA: Aspen Publishing.
- Neethling J et al *Law of Personality* 2 ed (2005): Durban: Lexis Nexis
- Schönberger MV & Cukier K *Big Data: A Revolution that Will Transform how We Live, Work, and Think* 6 ed (2013) London: Houghton Mifflin Harcourt.
- Townsend AM *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia* 1 ed (2013) New York: WW Norton & Company.
- Trubek D et al *Law and New Governance in the EU and the US* 1 ed (2006) 65-67 Oxford: Hart Publishing.
- Van der Merwe D et al *Information Communications Technology Law* 3ed (2016) Johannesburg: LexisNexis Butterworths

Dissertations

- Makulilo, AB *Protection of Personal Data in Sub-Sahara Africa* (published PhD thesis, Universität Bremen, 2012) 326.

Internet References

- Article 29 Data Protection Working Party "Guidelines on consent under Regulation 2016/679" WP259rev. Adopted on 01, 10 April 2018 18 available at https://webcache.googleusercontent.com/search?q=cache:l-b4dUk35iAJ:https://ec.europa.eu/newsroom/article29/document.cfm%3Faction%3Ddisplay%26doc_id%3D51030+&cd=1&hl=en&ct=clnk&gl=za (accessed 3 September 2021).
- Ars technica 'What Google can really do with Nest, or really, Nest's data' available at <http://arstechnica.com/business/2014/01/what-google-can-really-do-with-nest-or-really-nests-data/> (accessed 5 September 2022).
- BBC 'Heathrow plane in near miss with drone' available at <http://www.bbc.com/news/uk-30369701> (accessed 5 November 2021).
- Blinder A and Perloth N 'A Cyberattack Hobbles Atlanta, and Security Experts Shudder' *N.Y. Times* available at <https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html> (accessed 27 June 2023).
- Businesstech news '3 smart cities planned for South Africa', available at <https://businesstech.co.za/news/technology/477240/3-smart-cities-planned-for-south-africa/> (accessed 7 October 2021).

- California Department of Justice 'Privacy Laws' available at <https://oag.ca.gov/privacy/privacy-laws> (accessed 6 October 2021).
- Cooperative Governance and Traditional Affairs (CoGTA). 2016. *Integrated Urban Development Framework* (IUDF) available at [http://www.sacities.net/wp-content/uploads/2017/10/IUDF%202016 WEB-min.pdf](http://www.sacities.net/wp-content/uploads/2017/10/IUDF%202016%20WEB-min.pdf) (accessed on 23 July 2022).
- Copenhagen 'World Smart Cities Forum' available at <https://worldsmartcities.org/copenhagen/?msclkid=c1451bbbd15911eca302d0f6add159e9> (accessed 23 June 2023).
- Daily Maverick news 'Cybersecurity: South African companies are ripe for hackers', available at <https://www.dailymaverick.co.za/article/2021-08-01-cybersecurity-south-african-companies-are-ripe-for-hackers/> (accessed on 7 October 2021).
- David GC and Eliot Brown 'Google Parent Nears Deal to Build Its Vision of a City in Toronto' *Wall STJ* available at <https://www.wsj.com/articles/alphabets-city-building-unit-nears-development-deal-in-toronto-1507142561> (accessed 23 June 2023).
- Energy Capital Power 'Ramaphosa names his electricity minister, Paul Mashatile becomes new deputy president' 7 March 2023 available at <https://energycapitalpower.com/south-africa-minister-electricity-appointed/> (accessed 17 March 2023).

- eNews Channel Africa 'Budget shows Treasury is short of ideas to fix SA's economic woes' available at <https://www.enca.com/analysis/budget-shows-treasury-short-ideas-fix-sas-economic-woes> (accessed 7 October 2021).
- eNews Channel Africa 'SA Information Regulator battling to cope', available at <https://www.enca.com/news/sa-information-regulator-battling-cope> (accessed 7 October 2021).
- European Council Directive 95/46/EC, available at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046>. (accessed on 17 June 2022).
- Federal Privacy Council, Fair Information Practice Principles available at <https://www.fpc.gov/resources/fipps/> (accessed 28 June 2023).
- FTC 'Protecting Consumer Privacy in an Era of Rapid Change' available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> (accessed 29 June 2023).
- Fussell S 'The City of the Future Is a Data-Collection Machine' *The Atlantic* available at <https://www.theatlantic.com/technology/archive/2018/11/google-sidewalk-labs/575551/> (accessed 29 June 2023).
- Gonschorek A 'How Luno Uses Data to Make Product Decisions' available at <https://www.offerzen.com/blog/how-luno-uses-data-to-make-product-decisions>. (accessed 7 October 2021).

- Greenleaf G 'Global Data Privacy Laws 2013: 99 Countries and counting' (2013) Privacy Laws and Business International Report 10' available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305882. (accessed 7 October 2021).
- Hieroglyph 'Interview: Jonathan Sadowski on the Future of Cities' available at <https://hieroglyph.asu.edu/2014/10/interview-jathan-sadowski-on-the-future-of-cities/> (accessed 7 October 2021).
- International Business Machines Corporation 'Analyzing the future of cities' available at https://www.ibm.com/smarterplanet/us/en/smarter_cities/overview/index.html. (accessed 6 October 2021).
- Isaac M and Frenkel S, NY Times 'Facebook Security Breach Exposes Accounts of 50 Million Users' 28 September 2018 available at <https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html> (accessed 3 November 2021).
- Life SG 'Smart Nation Singapore' available at <https://www.smartnation.gov.sg/initiatives/strategic-national-projects/lifesp> (accessed 27 June 2023).
- Levi Sumagaysay 'San Francisco's Trash Bins Get Smart' *The Mercury News* available at <https://www.mercurynews.com/2019/02/27/san-franciscos-trash-bins-get-smart/> (accessed 19 June 2023).
- Neves J 'Dark History: The real reasons behind load shedding in South Africa' *Biznews* 21 July 2021 <https://www.biznews.com/energy/2021/07/05/load-shedding-sa-history>. (accessed 21 May 2022).

- Mathis S and Kanik A 'Why You'll be Hearing a lot Less About 'Smart Cities,' *City Monitor* <https://citymonitor.ai/government/why-youll-be-hearing-a-lot-less-about-smart-cities> (accessed on 23 June 2023).
- Muggah R and Walton G 'Smart Cities Are Surveilled Cities' *Foreign Policy* available at <https://foreignpolicy.com/2021/04/17/smart-cities-surveillance-privacy-digital-threats-internet-of-things-5g/> 9 (accessed 25 June 2023).
- OECD, ISO, available at <https://www.oecd.org/gov/regulatory-policy/ISO-Full-Report.pdf> (accessed on 29 July 2022).
- Technologymagazine – 'Top 10 smart cities in the world [Online],' available at: <https://www.gigabitmagazine.com/big-data/top-10-smart-cities-world> (accessed 19 September 2022).
- Tralac 'Status of AfCFTA Ratification' available at <https://www.tralac.org/resources/infographic/13795-status-of-afcfta-ratification.html> (accessed 20 June 2023).
- United Nations Department of Economic and Social Affairs 'World Urbanization Prospects: The 2014 Revision, Highlights, United Nations, Department of Economic and Social Affairs, Population Division' available at <http://esa.un.org/unpd/wup/Highlights/WUP2014-Highlights.pdf>. (accessed 5 October 2021).
- Office of Science and Technology Policy 'The White House, Blueprint for an AI Bill of Rights, Privacy 6, 30, 34 available at <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf> (accessed 27 June 2023).

- Precedence Research 'Smart Cities Market Size to Surpass US\$7,162.5 BN by 2030' *Global Newsire* available at <https://www.globenewswire.com/en/news-release/2022/05/10/2439944/0/en/Smart-Cities-Market-Size-to-Surpass-US-7-162-5-BN-by-2030.html>.(accessed 23 June 2023).
- Press Release N.Y.C. Dep't of Transp., 'NYC DOT Announces Expansion of Midtown Congestion Management System, Receives National Transportation Award' available at https://www1.nyc.gov/html/dot/html/pr2012/pr12_25.shtml. (accessed 23 June 2023).
- United Nations General Assembly 'Universal Declaration of Human Rights' available at <http://www.refworld.org/docid/3ae6b3712c.html> (accessed on 7 October 2021).
- United Nations General Assembly 'Peace, Dignity and Equality on a Healthy Planet,' available at <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (accessed on 3 June 2022).
- United Nations 'Transforming our World: the 2030 Agenda for Sustainable Development' available at <https://sustainabledevelopment.un.org/content/documents/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf>. (accessed on 21 July 2022).
- United Nations Human Rights Council 'Report of the Special Rapporteur on the promotion and protection of the right to Privacy' UN Doc A/HRC/40/63 (2019) available at <https://rm.coe.int/40th-hrc-session-report-of-the-special-rapporteur-on-the-right-to-priv/1680933f08> (accessed 20 June 2023).

- United Nations Office of the United Nations High Commissioner for Human Rights 'The Right to privacy in the Digital age', (30 June 2014) available at <https://www.ohchr.org/en/privacy-in-the-digital-age> (accessed on 11 June 2022).
- United States Department of Commerce 'EU-U.S. Privacy Shield Framework Principles' available at <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg>. (accessed 3 September 2021).
- United States Department of Commerce 'Swiss-US Privacy Shield Framework' <https://www.trade.gov/td/services/odsi/swiss-us-privacyshield-framework.pdf>. (accessed 3 September 2021).

Journal Articles

- Ajambo E and Emebinah C 'The African continental free trade area: Maximizing benefits for the Continent' (2021) *APJ* 15-27.
- Bratman B et al 'The Right to Privacy and the Birth of the Right to Privacy' (2002) 69 *Tennessee Law Review* 344
- Clarke, R 'Information Technology and Datavveillance,' (1988) 31(5) *Communications of ACM* 505-508
- Clavell GG '(Not So) Smart Cities - The societal drivers and impact of smart environments, Privacy and Emerging Sciences and Technologies' (2012) 40(6) *Oxford University Press* 27-28.

- Cocchia A 'Smart and Digital City: How to Create Public and Economic Value with High Technology in Urban Space' (2014) 7(3) *Springer International Publishing* 13-43.
- De Santis R 'Smart city: fact and fiction' (2014) Paper No. 54536 *Munich Personal RePEc Archive* 3-6.
- Gandomi A & Haider M 'Beyond the Hype: Big Data Concepts, Methods, and Analytics' (2015) 35(2) *International Journal of Information Management* 137-144.
- George W & Michael A 'Reputation, Compliance, and International Law' (2002) 31 (1) *JSTOR* 108–109
- Hancke G & de Carvalho de Silva B 'The Role of Advanced Sensing in Smart Cities' (2013) 13(1) *Sensors* 393-425.
- Helscher D 'Griswold v. Connecticut and the unenumerated right of privacy' (1994). 15 N Ill U L Rev 33–61.
- Hiller J and Blanke J 'Smart Cities, Big Data, and the Resilience of Privacy' (2017) 68 (2) *HLJ* 1-49.
- Hoofnagle CJ et al 'The European Union general data protection regulation: what it is and what it means?' (2019) 28(1) *Information & Communications Technology Law* 65-98
- Kitchin R 'The Real-Time City? Big Data and Smart Urbanism' (2014) 79(1) *GEOJ* 1-14

- Klabbers J, 'The Redundancy of Soft Law' (1996)65. *NORDIC J INT'L L.* 167- 168.
- Klabbers J, 'The Undesirability of Soft Law' (1998) 67 *NORDIC J. INT'L L.* 381-391.
- Koops B 'The trouble with European data protection law' (2014) 4(4) *IDPL* 250-261.
- Kshetri N 'Barriers to e-commerce and competitive business models in developing countries: A case study' (2007) 6 *Electronic Commerce Research and Applications Journal* 443-452.
- Lee DJ et al 'Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection' (2011) 35(2) *MIS Quarterly* 423-424.
- Michael C and James A 'Comparative Analysis of the Right to Privacy in the United States, Canada and Europe' (2014) 29(2) *Connecticut Journal of International Law* 261.
- Minkler L and Sweeney S 'On the invisibility and interdependence of basic rights in developing countries' (2011) 33 *HRQ* 351-396.
- Neethling J 'The concept of privacy in South African Law' (2005) 122(1) *SALJ* 18 - 28.
- Odendaal N 'Splintering Urbanism or Split Agendas? Examining the Spatial Distribution of Technology Access in Relation to ICT Policy in Durban, South Africa. *Urban Studies*' (2011) 48 (11) *Sage J.* 2375-2397.
- Okunade S and Ogunnubi O 'A "Schengen" agreement in Africa? African agency and the ECOWAS protocol on free movement' (2021) 36(1) *Journal of Borderlands Studies* 119-137.

- Townsend B and Thaldar D 'Navigating Uncharted Waters: Biobanks and Informational Privacy in South Africa' (2019) 35(4) *SAJHR on* 329–350.
- Prosser W 'Privacy' (1960) 48(3) *California Law Review* 384.
- Quane HA 'Further dimension to the interdependence and indivisibility of human rights? Recent developments concerning the rights of indigenous peoples.' (2012) 25 *HHLJ* 49–83.
- Reidenberg J, 'Resolving conflicting international data privacy rules in cyberspace' (2000) 52 *Stan L Rev* 1315–1371.
- Roos A 'Core principles of data protection law' (2006) 39(1) *CILSA* 102-130.
- Roos A 'Data Protection: explaining the international backdrop and evaluating the current South African position' (2007) 124 *SALJ* 400-433.
- Schwartz P 'The EU-US privacy collision: A turn to institutions and procedures' (2009) (2013) 126 *Harv L Rev* 1966.–
- Solove D and Hartzog W 'The FTC and the new common law of privacy,' (2014) 114 *Colum L Rev* 583–676.
- Van Brakel R and De Hert P 'Surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies,' (2011) 3 *VUB* 163-192.

- Vu K and Hartley K 'Promoting smart cities in developing countries: Policy insights from Vietnam. *Telecommunications Policy*,' (2018) 42(10) *Elsevier* 845–859.
- Warren S and Brandeis L 'The Right to Privacy' (1890) 4 *Harvard LR* 193–220.
- Ziegeldorf JH Morchon OG and Wehrle K 'Privacy in the Internet of Things: threats and challenges, *Security and Communications Networks*' (2014) 7(12) *Wiley Online Library* 2728-2742.

Law Commission Papers

- South African Law Reform Commission Discussion Paper 109 (Project 124) *Privacy and data protection* (2005).

White Papers

- The *White paper on National Integrated ICT Policy* (GN 1212 in GG 40325 of 3 October 2016).