



Cape Peninsula
University of Technology

**DATA PRIVACY GOVERNANCE FRAMEWORK FOR THE INTERNET OF THINGS
IN SOUTH AFRICAN ORGANISATIONS**

by

LEONA ANNELESE MCARDLE

Thesis submitted in fulfilment of the requirements for the degree

Master of Technology: Information Technology

in the Faculty of Informatics and Design

at the Cape Peninsula University of Technology

Supervisor: Mr Ayodeji Olanrewaju Afolayan

Co-supervisor: Dr Errol Francke

Cape Town

December 2021

CPUT copyright information

The dissertation/thesis may not be published either in part (in scholarly, scientific or technical journals) or as a whole (as a monograph), unless permission has been obtained from the University.

DECLARATION

I, Leona Annelise McArdle, declare that the contents of this thesis represent my own unaided work and that the thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.



Signed

08/12/2021

Date

ABSTRACT

In today's world, lived experiences and other social aspects of society have been influenced exponentially by digitalisation and technological advances such as the Internet of Things (IoT). The benefits of IoT have been widely documented and are evident in various application domains such as manufacturing, smart homes and healthcare (particularly during the COVID-19 pandemic). The adoption of connected devices has given rise to the collection and processing of sensitive personal data of users. Consumers of smart devices are enticed to acquire more products and services that provide convenient, automated and immersive experiences.

Despite the plethora of benefits and the growing global interest in the application of IoT, the susceptibility of connected devices to malicious attacks amplifies the risks to data privacy. Predictions have been made of the number of IoT devices reaching 50 billion by the year 2030. A direct correlation has been made between the increased number of devices and the upsurge in cyber-attacks and data breaches worldwide. In South Africa well-known organisations and state owned enterprises (SOEs) have fallen prey to the nefarious actions of threat actors. Noteworthy breaches include Liberty Holdings in 2018, Experian in 2020, and more recently Transnet, South African National Space Agency (SANSa) and the Department of Justice and Constitutional Development (DOJ&CD) in 2021. The Protection of Personal Information (POPI) Act came into effect in July 2021, following an eight-year delay. The continuous postponement of the Act has hampered the protection of South Africans data privacy as demonstrated by more regular occurrences of data breaches in recent years.

Several countries have attempted to address privacy concerns through the enactment of data privacy laws necessitated by the proliferation of technological advances that aid the aggressive collection and indiscriminate use of personal data. Despite these regulatory updates, the intricacies of data management and the dynamic nature of the governance of data privacy in IoT environments has prompted scholars to indicate the need for a holistic data privacy governance framework.

Therefore, this study aimed to explore the factors affecting the governance of data privacy regulation and compliance in connected environments, with a view to develop a framework of guidelines and best practices for governing data privacy in IoT environments in South Africa.

This research employed a qualitative multiple-case study of IoT-based organisations in South Africa. This study used non-probability, purposive sampling of a homogeneous dimension to select organisations and participants. In addition, semi-structured interviews of IoT-based organisations in South Africa and a document review of various countries with recently updated data protection regulation were incorporated. The responses were analysed using thematic analysis for the identification of categories and emergent themes.

The findings indicate that there are several factors that influence data privacy governance. The upsurge in data breaches is a cause of concern for many organisations. There was consensus that the human factor (individuals and their actions) posed the biggest challenge in terms of the protection of data privacy. Additionally, unsecured devices and networks leave organisations vulnerable to possible attacks. Thus, securing smart devices and educating people on security measures can be seen as integral to curbing security violations, ensuring network integrity and ultimately protecting data privacy.

Furthermore, this study identified and explored four key areas of consideration for data privacy governance in IoT environments in South Africa, namely data privacy, data security, data governance and compliance. This study's exposition on data privacy pertained to the establishment of guidelines on data management in regard to compliance, people and technology in relation to IoT environments. Data security explored the ways to mitigate and manage data security risks through the adaptation and implementation of standards, protocols and measures designed specifically for IoT environments. The aspect of data governance expounded on the implementation of relevant strategies and policies to govern facets of data privacy in IoT-based organisations. Finally, the concept of compliance provided deep insights in relation to the role of legislation, organisational processes and practices in the industry sector and the effects on data privacy governance in IoT-environments in South Africa.

Based on the identified key areas of the study, a proposed framework for data privacy governance in IoT environments in South Africa was developed. Thus, IoT-based organisations in South Africa can draw on the guidelines in the proposed framework to inform and assist in the management of data privacy governance in accordance with regulatory compliance.

Keywords: Internet of Things (IoT), data privacy, data security, data governance, compliance, POPI Act, privacy regulation, multiple-case study

ACKNOWLEDGEMENTS

I wish to thank:

- My supervisor, Mr Ayodeji Olanrewaju Afolayan for your guidance and support which played a crucial role in my completion of this study. Your dedication to excellence and due diligence is a testament to your character. Thank you for bringing me this far and not letting me give up!
- My co-supervisor, Dr Errol Francke, thank you for help and words of guidance and encouragement.
- My parents, thank you for your understanding and encouragement. I appreciate everything that you do for me.
- Everyone who partook and availed themselves on my journey – each part was equally important and highly valued.

GLOSSARY

Acronyms	Definition
4G-LTE	Fourth Generation Long-Term Evolution
AES	Advanced Encryption Standard
API	Application Programming Interface
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
BBN	Bolt, Beranek and Newman Corporation
BLE	Bluetooth Low Energy
CCPA	California Consumer Privacy Act
CCTV	Close Circuit Television
CERN	Conseil Européen pour la Recherche Nucléaire or European Organisation for Nuclear Research
CHAT	Cultural Historical Activity Theory
DARPA	Defense Advanced Research Projects Agency
DNS	Domain Name System
DOJ&CD	Department of Justice and Constitutional Development
DoS	Denial of Service
EU	European Union
FID	Faculty of Informatics and Design
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HTML	Hyper Text Mark-up Language
HTTP	Hypertext Transport Protocol
IaaS	Infrastructure as a Service
IBM	International Business Machines Corporation
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IMP	Interface Message Processor
IoT	Internet of Things
IPC	Information and Privacy Commission
ISP	Internet Service Provider
NCSA	National Center of Supercomputer Applications
NFC	Near Field Communication

NSF	National Science Foundation
OAIC	The Office of the Australian Information Commissioner
OECD	Organization for Economic Co-operation and Development
OIPC	The Office of the Privacy Commissioner of Canada
PaaS	Platform as a Service
POPI Act / POPIA	Protection of Personal Information Act
RFID	Radio Frequency Identification
RSS	Really Simple Syndication
SaaS	Software as a Service
SANSA	South African National Space Agency
TCP/IP	Transmission Control Protocol/Internet Protocol
USA	United States of America
WSN	Wireless Sensor Network
WWW	World Wide Web

TABLE OF CONTENTS

DECLARATION	iii
ABSTRACT	iv
ACKNOWLEDGEMENTS.....	vi
GLOSSARY	vii
TABLE OF CONTENTS.....	ix
LIST OF TABLES	xvi
LIST OF FIGURES.....	xviii
CHAPTER ONE: INTRODUCTION.....	1
1.1 Introduction	1
1.2 Research background	4
1.2.1 A brief overview of IoT architectures and application domains	5
1.2.2 Background to the research problem	6
1.3 Research problem.....	8
1.4 Research aim	8
1.5 Research objectives	8
1.6 Research question and sub-questions	8
1.7 Research methodology	9
1.7.1 Research philosophy	9
1.7.2 Research approach.....	10
1.7.3 Research design.....	10
1.7.4 Data collection	12
1.7.5 Data analysis	12
1.8 Ethics	13

1.9	Delineation	13
1.10	Contribution.....	13
1.11	Summary.....	14
1.12	Thesis outline	14
CHAPTER TWO: LITERATURE REVIEW.....		17
2.1	Introduction	17
2.2	Privacy: a concept in disarray.....	18
2.2.1	A categorisation of privacy	19
2.2.2	A taxonomy of privacy harms.....	20
2.2.3	Seven types of privacy.....	24
2.3	A nomenclature for the protection of personal information.....	25
2.3.1	Applied terminology for privacy regulation.....	25
2.3.2	Industry-specific definitions from Google search	25
2.3.3	Definitions from academic literature	27
2.4	Technological advances that impacted on data privacy	28
2.4.1	A brief history of the internet	28
2.4.2	Social media	31
2.4.3	Big data	32
2.4.4	Mobile devices.....	32
2.4.5	Cloud computing	33
2.4.6	The Internet of Things (IoT)	33
2.5	An overview of IoT	34
2.5.1	Security in IoT environments.....	34
2.5.2	Architectures for IoT.....	34
2.5.3	Five layer architecture, technologies and security threats	35
2.5.4	Application domains for IoT.....	39
2.5.5	Data privacy and governance in IoT	41
2.6	Protection of personal information regulation and policies	42
2.7	Related work	44

2.8	Activity Theory.....	47
2.8.1	Overview of activity theory	48
2.8.2	The activity system	49
2.9	Summary.....	50
CHAPTER THREE: RESEARCH METHODOLOGY		52
3.1	Introduction	52
3.2	Research Philosophy	53
3.2.1	Ontological considerations	54
3.2.2	Epistemological considerations.....	55
3.2.3	Axiology	60
3.3	Research approach.....	60
3.3.1	Deductive approach	61
3.3.2	Abductive approach	62
3.3.3	Inductive approach.....	63
3.4	Research design	64
3.4.1	Descriptive research	64
3.4.2	Explanatory research	65
3.4.3	Exploratory research.....	65
3.5	Research strategy	66
3.5.1	Experimental research	66
3.5.2	Surveys.....	68
3.5.3	Action research.....	69
3.5.4	Participatory research	70
3.5.5	Grounded theory	70
3.5.6	Ethnography	71
3.5.7	Archival research	72
3.5.8	Narrative inquiry.....	73
3.5.9	Case study.....	73
3.5.10	Research methods.....	76

3.5.10.1	Quantitative research	77
3.5.10.2	Qualitative research	77
3.6	Sampling	77
3.6.1	Probability sampling.....	78
3.6.2	Non-probability sampling.....	80
3.7	Unit of analysis.....	83
3.8	Data collection.....	83
3.8.1	Secondary data.....	84
3.8.2	Document analysis.....	84
3.8.3	Primary data	85
3.9	Data analysis	89
3.9.1	Thematic analysis	89
3.10	Ethics	90
3.11	Summary.....	91
CHAPTER FOUR: ANALYSIS AND FINDINGS.....		93
4.1	Introduction	93
4.1.1	Problem statement.....	94
4.1.2	Research questions	94
4.1.3	Research objectives.....	94
4.1.4	Research aim.....	94
4.2	The context of study.....	94
4.3	Data collection.....	95
4.3.1	Data collection process for interviews	95
4.3.2	Data collection process for policy document review	100
4.4	Data analysis	104
4.4.1	Analysis of interview data.....	105
4.4.2	Analysis of policy document review.....	129
4.5	Summary.....	152

CHAPTER FIVE: INTERPRETATION OF FINDINGS	153
5.1 Introduction	153
5.2 Subject.....	155
5.3 Tools.....	157
5.4 Rules.....	159
5.5 Community.....	161
5.6 Division of labour.....	163
5.7 Object	165
5.8 Outcome	168
5.9 Summary.....	171
CHAPTER SIX: DISCUSSION.....	173
6.1 Introduction	173
6.2 Theme 1: Factors affecting data privacy regulation in IoT organisations in South Africa 174	
6.2.1 Data privacy.....	174
6.3 Theme 2: Knowledge of existing local and international data privacy legislations in relation to IoT environments.....	178
6.3.1 Regulation	178
6.4 Theme 3: Best practices for the governance of data privacy in IoT environments 192	
6.4.1 Data security.....	192
6.5 Theme 4: Data privacy governance framework for IoT organisations in South Africa 197	
6.5.1 Internet of Things (IoT)	197
6.6 Summary.....	199
CHAPTER SEVEN: RECOMMENDATIONS, REFLECTION AND CONTRIBUTIONS	201
7.1 Introduction	201
7.2 Summary of the study	202

7.2.1	SQ1.1: What are the factors affecting data privacy regulation in IoT organisations in South Africa?	202
7.2.2	SQ1.2: How knowledgeable are South African organisations about existing local and international data privacy legislations in relation to IoT environments?	203
7.2.3	SQ1.3: What are the best practices for the governance of data privacy in IoT environments?	204
7.2.4	SQ1.4: How can a data privacy governance framework for IoT organisations in South Africa be developed?	205
7.3	Best practices, guidelines and framework	206
7.3.1	Data privacy	206
7.3.2	Data security	207
7.3.3	Data governance	208
7.3.4	Compliance	208
7.4	Contributions	209
7.5	Recommendations	210
7.6	Limitation	211
7.7	Future research	212
7.8	Reflection	213
7.9	Conclusion	213
REFERENCES		215
APPENDICES		239
APPENDIX A: ETHICAL CLEARANCE FROM FACULTY OF INFORMATICS AND DESIGN, CPUT		239
APPENDIX B: RESEARCH PARTICIPATION EMAIL REQUEST		240
APPENDIX C: RESEARCH BRIEF		241
APPENDIX D: PARTICIPANT CONSENT FORM		243
APPENDIX E: INTERVIEW SCHEDULE		245
APPENDIX F: SAMPLE INTERVIEW TRANSCRIPT		249
APPENDIX G: SAMPLE OF ATLAS.TI TRANSCRIPTS AND CODES FOR INTERVIEW ANALYSIS		253

APPENDIX H: SAMPLE OF ATLAS.TI TRANSCRIPTS AND CODES FOR DOCUMENT ANALYSIS	257
APPENDIX I: SAMPLE OF FULL CODING TABLE IN MS EXCEL	261
APPENDIX J: PROOFREADING CERTIFICATE	264
APPENDIX K: TURNITIN REPORT	265

LIST OF TABLES

Table 2.1: Industry-specific definitions on Google	25
Table 2.2: Academic literature definitions.....	27
Table 2.3: Security requirements and challenges for IoT	34
Table 2.4: Common technologies and security vulnerabilities at perception layer	36
Table 2.5: Common technologies and security vulnerabilities at transport layer.....	37
Table 2.6: Common technologies and security vulnerabilities at processing layer.....	38
Table 2.7: Common security vulnerabilities at application layer	38
Table 2.8: Common security vulnerabilities at business layer	39
Table 2.9: Summary of related work	46
Table 2.10: Components of an activity system, description and context.....	50
Table 3.1: Types of case study	75
Table 3.2: Rationale for single-case designs.....	76
Table 3.3: The phases of thematic analysis	90
Table 4.1: Brief overview of each organisation.....	97
Table 4.2: Participant classification	98
Table 4.3: List of countries with updated data protection legislation 2018–2021	101
Table 4.4: The phases of thematic analysis	104
Table 4.5: Summary of generated codes, categories and themes.....	107
Table 4.6: Summary of generated codes, categories and themes for participants' profile	108
Table 4.7: Summary of findings for SQ1.1	113
Table 4. 8: Summary of findings for SQ1.2	119
Table 4.9: Summary of findings for SQ1.3	124
Table 4.10: Summary of findings for SQ1.4	126
Table 4.11: Findings, categories and themes.....	127
Table 4.12: Categories and themes generated from codes.....	131
Table 4.13: Definitions for Personal Data or Personal Information	133

Table 4.14: Principles related to the processing of personal information	136
Table 4.15: Lawful processing of personal information.....	137
Table 4.16: Countries with definitions for consent	140
Table 4.17: Right of the data subject in relation to the processing of personal information	143
Table 4.18 Definitions for the responsible parties and operators	146
Table 4.19: Responsibilities of Information Regulator and information officers in South Africa	147
Table 4.20: Findings, sub-themes and themes.....	151
Table 5.1: Components of an activity system, description and context.....	154
Table 5.2: Findings related to Subject.....	156
Table 5.3: Findings related to Tools	158
Table 5.4: Findings related to Rules.....	160
Table 5.5: Findings related to Community.....	162
Table 5.6: Findings related to Division of Labour	164
Table 5.7: Findings related to Object	167
Table 5.8: Findings related to Outcome	170

LIST OF FIGURES

Figure 1.1: Chapter One outline	1
Figure 1.2: Thesis organisation and chapter clarification.....	15
Figure 2.1: Chapter Two outline	17
Figure 2.2: Global number of internet users 2005–2019	28
Figure 2.3: Popular social media networks worldwide	31
Figure 2.4: IoT architectures	35
Figure 2.5: Five-layer architecture with security and privacy issues	36
Figure 2.6: Application domains of IoT	40
Figure 2.7: Countries with updated privacy regulations (2018–2021)	43
Figure 2.8: Biggest data breach fines and settlements worldwide	44
Figure 2.9: The activity system	49
Figure 3.1: Chapter Three outline	52
Figure 3.2: Influence of researcher's beliefs and assumptions on research design	53
Figure 3.3: Critical realist stratified ontology.....	57
Figure 3.4: Deductive and inductive approaches to the relationship between theory and research.....	61
Figure 3.5: Example of a simple deductive argument or syllogism	62
Figure 3.6: Example of inductive reasoning	63
Figure 3.7: Example of a true experimental design	67
Figure 3.8: Kurt Lewin's original plan for action research	69
Figure 3.9: The process of theoretical sampling.....	71
Figure 3.10: Basic types of designs for case studies.....	74
Figure 3.11: Techniques for sampling	78
Figure 4.1: Chapter Four outline	93
Figure 4.2: Distribution of IoT-based organisations across South Africa	96
Figure 4.3: Example of initial codes generated.....	105
Figure 4.4: Example of generating categories and potential themes	106
Figure 4.5: Example of themes generated	106

Figure 4.6: Representation of word frequency in policy documents.....	130
Figure 4.7: Example of generating initial codes.....	131
Figure 4.8: Proposed principles	137
Figure 5.1: Chapter Five outline	153
Figure 5.2: Mapping of study's finding to activity system	154
Figure 6.1: Chapter Six outline.....	173
Figure 7.1: Chapter Seven outline.....	201
Figure 7.2: Proposed data privacy governance framework	207

CHAPTER ONE: INTRODUCTION

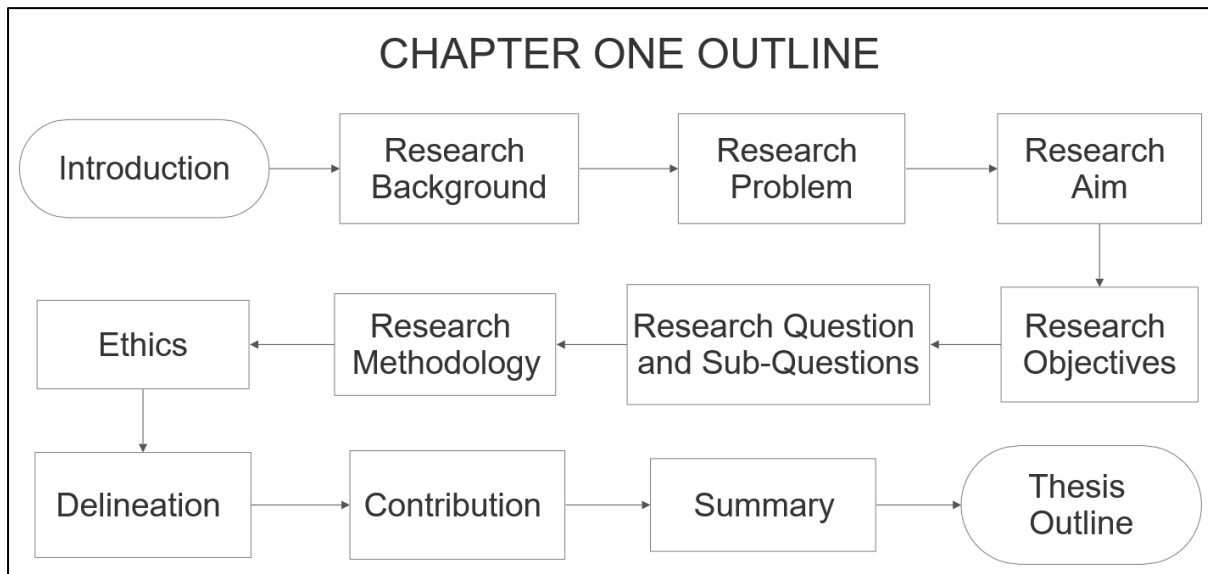


Figure 1.1: Chapter One outline

1.1 Introduction

The protection of personal information has become a keenly debated topic since the European Union's (EU's) General Data Protection Regulation (GDPR) took effect in May 2018 (Marcus, 2018; Reinwarth, 2019). Privacy has been a phenomenon of interest for a long time, with academics and law makers endeavouring to define privacy in numerous ways (Barendt, 2017; Peters, 2020). The right of a person's privacy has been a source of concern that dates back to the 1890s (Warren & Brandeis, 1890). Nevertheless, there is no consensus on the definition for privacy. Solove (2002) contends the definitions are either too comprehensive or too limited. Even though there is a continuance in the lack of a generally accepted definition for privacy, the evolution of computers and emerging technologies has brought more focus on a facet of privacy, namely the right of the protection of private data, i.e. data protection (Lukacs, 2017; Peters, 2020). In this study, an encapsulating data privacy definition is explored and adopted.

In 2011 already the Organization for Economic Co-operation and Development (OECD) defined that the preservation of data privacy requires the user's informed consent, relevance to the purpose of use, specification of purpose, usage limitations, transparency, notification and correction or deletion of data, and accountability. Similarly, the regulation of the collection, storage, usage and transferring of an individual's data can be termed as data protection which is paramount to the concept of data privacy (Bennett & Raab, 2003; Peters, 2020). The accessibility and magnitude of information available in today's information society have

escalated privacy concerns due to the proliferation of data use by organisations which has given rise to more focused research on data privacy practices (Doig et al., 2018). An information society was defined by Martin (1988:306) as:

a society in which the quality of life, as well as prospects for social change and economic development, depend increasingly upon information and its exploitation. In such a society, living standards, patterns of work and leisure, the education system and the marketplace are all influenced markedly by advances in information and knowledge. This is evidenced by an increasing array of information-intensive products and services, communicated through a wide range of media, many of them electronic in nature.

Technological evolution in the last decade has given rise to advances such as the Internet of Things (IoT) which enables interconnection and communication between objects over the internet through sensors (Matos et al., 2017; van den Hoven et al., 2020). Everyday items and gadgets embedded with sensors enable the collection and collation of huge volumes of data (Hussain, 2017; Wu et al., 2020). An estimated 22 billion IoT connected devices were in use by the end of 2018, according to a report by Statista Research Department, with a further 50 billion predicted by 2030 (Vailshery, 2021). The integration of these connected devices into people's everyday existence, exponentially multiplies the opportunities for cyber-attacks and data breaches (Shin & Park, 2017; Wu et al., 2020). Thus, accessing information through IoT devices and associated platforms such as "social media, mobile applications, big data analytics and cloud computing" impacted on the users' privacy and made organisations and people more susceptible to data breaches (van den Hoven et al., 2020). These breaches include hacking, mishandling of sensitive data, selling data to third parties and vulnerabilities in security systems that expose users' information to manipulations (Leskin, 2018; Irwin, 2020).

These adverse effects and occurrence of data breaches have been on an alarming increase which has raised many questions on the capability of effective data privacy regulation. Leskin (2018) questions the competence of existing laws to deal with an ever growing technology driven society and the consequence of the rising number and variation of these incidents. IBM Security (2021) reports that on average a data breach's total cost is in the region of \$4.24 million, a rise of 10% from the preceding year and the highest in seven years. Malinga (2019) established that more than one billion individuals' data were compromised in 2018; notable breaches included Facebook users (50 million in March, 90 million in September, 7 million in December); Marriott (500 million users); Google+ (500,000 accounts); Twitter (330 million

users); and British Airways (380,000 transactions). In South Africa, the personal data of 934,000 drivers were leaked in May 2018 from online traffic fine website, ViewFines (Etheridge, 2018).

In a reported incident in August 2020 credit information services agency, Experian reportedly exposed the information of 24 million South Africans and nearly 800 000 organisations (Cimpanu, 2020). Recently, Transnet, South Africa's port and rail authority, suffered a ransomware attack in July 2021 which crippled the company's operations for more than a week, forcing a declaration of *force majeure* to relieve the company from contractual responsibilities (Neves, 2021). In September 2021, two months after the Transnet breach, the South African National Space Agency (SANSA) and the Department of Justice and Constitutional Development (DOJ&CD) fell victim to cyber-attacks as well (Feltham, 2021). The DOJ&CD's breach subsequently affected South Africa's Information Regulator (IR), the national information watchdog, resulting in the unavailability of the IR's website and emails for more than three days (Diphoko, 2021).

Following the leak, the IR's chairperson voiced concern over the considerable number of breaches being experienced in South Africa and stated that in August of 2021, thirty-eight security breaches were reported (Information Regulator, 2021). Thus, the revelation of the Regulator indicated the magnitude of challenges faced in terms of data breaches and the enforcement of the privacy regulation. The inadvertent breach and subsequent admission of the data protection regulating body, imply that there is a serious limitation in the capacity to deal with incidents of cyber security and data breaches (Moyo, 2021b). Consequently, that begs the question of the regulator's capability to ensure compliance of data privacy governance within IoT environments which is of a more complex nature.

Given the role information plays in today's world, enterprises seek to garner valuable insights from the vast amount of data generated by connected objects to gain competitive advantage (Doig et al., 2018). Nevertheless, identifiable information of a person is not a commodity without impact on autonomy, social connections and the lives of individuals. Thus, it is imperative to establish ways of safeguarding the ethical access and use of the data (Medhora, 2018). Strategic data management or data governance, according to Ladley (2012:11) has various definitions. However, the overarching theme maintains: "It is the organization and implementation of policies, procedures, structure, roles, and responsibilities which outline and enforce rules of engagement, decision rights, and accountabilities for the effective management of information assets" (ibid, 11).

Data privacy represents a major aspect of the governance of an individual's information as privacy policies set forth controls for the processing and use of personal information (Dennedy et al., 2014; Swartz et al., 2019). Requirements for data privacy, brought on by rapid deployment of technologies such as IoT, need to be exponentially altered periodically, due to the various methods IoT sensors and interconnected mediums collect and utilise user's private data (Naeini et al., 2017; Anand & Sharma, 2020). Privacy and data governance in heterogeneous IoT environments are particularly challenging due to information linkage from various data sources (Zheng et al., 2018; Dasgupta et al., 2019). Thus, Anand and Sharma (2020) argue that due to these complexities and vulnerabilities in the system, persons are often at risk of their data being utilised for purposes other than what was agreed upon. This is a growing concern of unethical access and utilisation of personal data in IoT environments.

Managing the security concerns for IoT applications and devices have led to various articles with proposed frameworks and guidelines. Thinakaran et al. (2017) proposed a conceptual privacy framework presenting fundamental principles for the development of health applications within IoT that are cognisant of privacy. Following a study of academic literature of numerous existing data governance frameworks, the 4I (Identify, Insulate, Inspect and Improve) Framework was developed by (Dasgupta et al., 2019). In the context of South Africa, a list of privacy compliance guidelines is proposed by Baloyi and Kotzé (2019), for the purpose of aiding organisations in complying with privacy legislation within CPS and IoT environments.

The purpose of the study thus, is to examine the compliance, governance and regulation of data privacy in IoT environments, with the aim of developing a framework of guidelines and best practices for governing data privacy in IoT environments in South Africa.

1.2 Research background

Our digital footprints are no longer the feather-light markings being washed away on the next tide, but rather resemble deep-set imprints that will follow us to the end of time (Ali et al., 2018). In recent times not only is the information that individuals communicate, but also private or meta data (GPS location, devices used, time of communication, IP address, ISP, contact numbers or email addresses) recorded (New Zealand Human Rights Commission, 2018; Chiara, 2020). It was further argued that the aggregation, mining and analysis of meta data provide detailed information on a user's preferences, relationships and behaviour. As technology rapidly develops and connectivity intensifies, so do the resources for retrieving information which directly affects privacy (van den Hoven et al., 2020). Similarly, Swartz et al. (2019) assert that the continuous progression of information security and privacy management, for individuals and corporations, should be dictated by the pervasive nature of

advancing technologies. However, the standardisation and completion of IoT technical specifications and reference architectures are yet to be agreed upon which raises concerns about the standardisation of data privacy governance in IoT environments (Nicolescu et al., 2018).

1.2.1 A brief overview of IoT architectures and application domains

Numerous IoT architectures have been proposed, including the commonly used three-, four- and five-layer architectures. However, a uniform architecture for IoT still does not exist (Ren et al., 2017; Sethi & Sarangi, 2017; Burhan et al., 2018; Park et al., 2019). A brief introduction to the afore-mentioned architectures is highlighted in this section.

Three layer architecture: It consists of the perception (includes the devices), network (connection) and application (application services) layers (Sethi & Sarangi, 2017).

Four layer architecture: It comprises of the above-mentioned three layers and a support layer for authentication of users and information between the perception and network layers (Ren et al., 2017).

Five layer architecture: It encompasses the perception, transport (data transfer), processing (storing analysis and processing of data), application and business layers (management) (Burhan et al., 2018).

For the purpose of this study, the researcher will focus on the five-layer architecture which according to Burhan et al. (2018) fulfils the security and privacy requirements for IoT environments. A more detailed discussion on the security and privacy issues can be found in Chapter Two.

Industry and user-specific applications which enable “device-to-device” and “human-to-device” interactions, are facilitated by IoT (Horn et al., 2019:101). Eleonora Borgia created a comprehensive list of IoT applications in 2014 which included 24 subareas that were grouped under the following domains: Industrial, Smart City and Health Wellbeing (Pico-Valencia et al., 2018; Hassan, 2018). In Chapter Two these domains will be explored in detail. In this section the afore-mentioned domains are briefly presented as follows.

- **Industrial domain:** Financial and commercial transactions between entities can be exploited by IoT in all aspects of industrial activities, ranging from logistics and manufacturing to banking (Borgia, 2014). According to Pico-Valencia et al. (2018) the industrial domain encompasses the automation of processes that would generally be performed by humans in product creation or the provision of a service. Ultimately, improving productivity and efficiencies are some of the main objectives of applications in

this domain (Eddine et al., 2018). Some examples of applications in this domain include inventory management, animal tracking and real-time vehicle diagnostics (Hassan, 2018).

- **Smart city domain:** The emphasis of this domain is on energy management and smart solutions for improving the quality of human life and increasing the environmental sustainability of cities (Borgia, 2014). Thus, applications are focused on enhancing the day-to-day undertakings of people, for example smart meters for water and electricity usage (Pico-Valencia et al., 2018).
- **Health wellbeing domain:** There are a number of ways in which IoT can play a considerable part in supporting individuals and improving social activities. These include independent living for people with varying needs, along with real-time health and medical care (Borgia, 2014). Eddine et al. (2018) assert that smart healthcare applications can play a significant role in the remote monitoring of patients which could alleviate the strain on medical services and staff. The capability of remote patient monitoring has been paramount in the fight against COVID-19 over the past two years (Haghi Kashani et al., 2021).

It is necessary to understand the types of IoT application areas in order to identify the dynamic nature of data acquisition for each domain and the related concerns for the governance of data privacy.

1.2.2 Background to the research problem

The IoT applications can already be seen as an integral part of everyday life and therefore attention should be given to safeguarding and protecting user information. The features and requirements for security in IoT, according to Lin et al. (2017:1132) are: “confidentiality, integrity, availability, authenticity, identification and authentication, privacy, and trust”. Security as well as privacy concerns exist at every layer of the architecture that necessitates consideration for offering secure IoT applications (Tewari & Gupta, 2020). The security challenges in IoT extend beyond traditional networking attacks and issues such as “interoperability, resource constraints, resilience to natural disasters and physical attacks, autonomic control, information volume, privacy protection and scalability” should also be addressed (Radoglou Grammatikis et al., 2019:45).

The IoT has led to the proliferation of devices and technologies that are constantly connected through the internet, regardless of it being a person, a thing, a sensor or a service (Alaba et al., 2017; Wu et al., 2020). Thus, massive volumes of personal data are collected and shared by IoT devices to provide personalisation of services through identification which constitutes a risk to privacy (Wachter, 2018). The IoT applications and devices record users' behaviour,

physical location and sensitive information such as medical records. Therefore, the importance of preserving privacy in IoT environments is paramount (Rayes & Salam, 2017). Thus, governments and organisations recognising the significance of personal information protection is a direct consequence of growing customer rights awareness and the continuing rise of data violations and information breaches (Gan et al., 2019).

The Ponemon Institute LLC, (2018) predicted a 43% probability of South African organisations suffering a data breach. In addition, IBM Security (2020) reported that 48% of attacks on South African organisations are from malevolent actors, 26% are caused by system glitches and human error accounts for the other 26%. The average expenditure involving data breaches for South African organisations totalled R55 million in 2021, increasing from R36.5 million in 2018, R32 million in 2017 and R28.6 million in 2016 (Moyo, 2018; IBM Security, 2021). Besides the SANSA, DOJ&DC, IR and Transnet breaches mentioned earlier in this chapter, other noteworthy breaches include: Liberty Holdings – 40 terabytes of data in June 2018 (Job, 2018); Facebook/Cambridge Analytica – affected about 60,000 South Africans (Hedley, 2018); Ster-Kinekor – 7 million users' details were leaked (Venktess, 2017); a repository containing the personal data of over 60 million South Africans was discovered in October 2017 (van Niekerk, 2017).

Attempts have been made to address critical issues related to the “integration of services and systems, interoperability, cyber-security, personal privacy and infrastructure development” by South Africa in the development of policies and legal frameworks (Manda, 2017:43). Following years of delay, the Protection of Personal Information (POPI) Act, 2013 (Act 4 of 2013), became fully enforceable on the 1st of July 2021 (Bhagattjee, 2021). However, the implementation of the POPI Act has not been a deterrent for malicious attacks on South African organisations and government entities, as evidenced by recent ransomware attacks on Transnet and the DOJ&CB, and subsequently the IR itself (Feltham, 2021; Malinga, 2021). Questions have been raised about the effective application of the POPI Act in complex innovation systems such as IoT environments and the capacity of the IR to ensure proper compliance to data privacy governance.

According to Morar et al. (2021) the challenges for IoT governance include aspects of “data governance”, “privacy rights” and “security breaches”. Dasgupta et al. (2019:212) contend that “currently there is no concrete IoT framework, which is available and can provide a blueprint to establish a data governance environment, particularly from a regulatory perspective”. Therefore, given the ubiquitous and dynamic nature of data in IoT environments, it is

imperative that data governance is prioritised to ensure compliance with regulations and that boundaries of data privacy are upheld at all times.

1.3 Research problem

Rapid technological advances, intensification of connectivity and society's reliance on technology have triggered a proliferation of data privacy concerns. The governance of data privacy regulation and compliance for the Internet of Things (IoT) in relation to people, data, processes and things is a cause for concern for individuals and organisations worldwide. The regulation of data privacy and compliance in South Africa remains largely invisible. Despite the advent of the POPI Act, a growing threat of data breaches within digital environments continues. Consequently, the lack of active governance tailored for IoT environments, in relation to data privacy may lead to massive violations of user data and breaches of privacy. This may result in an adverse impact, not only on users and organisations, but also the country at large. Therefore, given the global nature of IoT, the governance of data privacy in IoT-based environments in South Africa becomes imperative for the country to remain an international contender in technological advances.

Problem statement: There is no defined holistic framework of best practices and guidelines for the governance of data privacy in IoT environments in South Africa.

1.4 Research aim

The aim of this study is to explore the factors affecting the governance of data privacy regulation and compliance in connected environments, with a view to develop a framework of guidelines and best practices for governing data privacy in IoT environments in South Africa.

1.5 Research objectives

The objectives of the research are:

- i. To determine the factors affecting data privacy regulation in IoT-based organisations in South Africa.
- ii. To establish awareness of organisations' adherence to data privacy and regulatory laws in the use of data obtained through IoT environments.
- iii. To determine existing best practices for the governance of data privacy in an IoT environment.
- iv. To develop a framework of guidelines for data privacy governance in IoT environments in South Africa.

1.6 Research question and sub-questions

RQ: How can data privacy governance be implemented in IoT environments in South Africa?

SQ1.1: What are the factors affecting data privacy regulation in IoT organisations in South Africa?

SQ1.2: How aware are South African organisations of existing international or cross-border data privacy and regulatory legislations in relation to IoT environments?

SQ1.3: What are the best practices for the governance of data privacy in IoT environments?

SQ1.4: How can a data privacy governance framework for IoT organisations in South Africa be developed?

1.7 Research methodology

The methodology of research involves the systematic planning of conducting research (Mishra & Alok, 2017). It incorporates the philosophies, strategies and methods that encompass the entire process of executing research (Marczyk et al., 2005). Therefore, it can be seen as the logical approach of "planning and conducting the research study, drawing conclusions and disseminating the findings" (ibid, 2005:22). The study adopted a complementary research methodology that followed scientific steps and techniques in the investigation of the subject matter.

1.7.1 Research philosophy

The nature of knowledge in research can be viewed as the research philosophy (Saunders & Lewis, 2012). Furthermore, a researcher's vision of the world, whether it relates to facts or feelings and attitudes, will strongly influence the researcher's chosen philosophy, strategy and methods. This researcher adopted a philosophical stance and views that are in line with the research aim and objectives. There are three main philosophical positions in research, namely ontology, epistemology and axiology. This researcher positions the research in terms of the ontological views and epistemological belief.

1.7.1.1 Ontology

Ontology is a reflection based on the elucidation of the researcher on whether social actors are independent of or have influence over perceived facts (Dudovskiy, 2018). Subjectivism refers to an ontological position where "social phenomena (are) created from the perceptions and consequent actions of those social actors concerned with their existence" (Saunders et al., 2009:110). Researchers with a subjectivist persuasion, according to Holden and Lynch (2006:10) are unable to remain completely impartial and unbiased from "what is being observed, the study's subject matter or the methods of the study".

In this study, the researcher adopted a subjective ontology, since the researcher believes social actors have an influence over perceived facts.

1.7.1.2 Epistemology

Epistemology relates to what is considered as acceptable knowledge as well as the classification by the researcher as to what is regarded as knowledge (Bryman & Bell, 2014). Thus, the research sought to understand the phenomenon through the views and perceptions of subjects in the study. Epistemology can be classified into three main paradigms, namely critical realism, positivism and interpretivism. The interpretivist paradigm requires the researcher to have an understanding of the varying roles individuals play as social actors (Saunders & Lewis, 2012). Thus, the researchers are not impartial observers and have to take into account their own viewpoints as well as the social factors that influence the research subjects (Walliman, 2005).

This researcher took an interpretivist approach to investigate and comprehend privacy regulation and governance in IoT environments.

1.7.2 Research approach

Qualitative research, according to Greener (2008) is likely to encompass an inductive approach; whereas quantitative research in all likelihood comprises of a deductive approach. Emanating from “specific observations or measures”, induction or an inductive approach aims to develop a theory based on “patterns and repeated occurrences” (Saunders & Lewis, 2012:109). Research focussed on a subject’s “values, attitudes, perceptions” can be classified as qualitative research with alignment to an inductive approach (Neville, 2005:3).

The inductive approach allows the researcher to identify patterns that might emerge which informs the understanding of factors relating to the research subject. Therefore, an inductive research approach was adopted for this study based on the need to infer from the findings in order to develop a holistic framework of guidelines and best practices for data privacy governance in IoT environments in South Africa.

1.7.3 Research design

Research design involves the overall strategy or plan for the procurement of research subjects or participants and the collection of information from these subjects including the analysis of information gathered (Welman et al., 2005). Qualitative research adopts three different design types, namely descriptive, explanatory or exploratory (Kothari, 2004; Saunders et al. 2009; Bhattacharjee, 2012). This research adopted a qualitative approach with an exploratory design

with the aim to explore the factors affecting the governance of data privacy in IoT environments in South Africa.

1.7.3.1 Research strategy

Saunders and Lewis (2012:70) highlighted “experiments, surveys, case studies, action research, grounded theory, ethnography and archival research” as commonly used research strategies. A case study is described as the investigation of a case with the purpose of observing and understanding the intricacy and specific nature of the case (Stake, 1995; Bryman, 2012). A multiple-case design involves a study that includes more than one case and the purpose is to comprehend the “similarities and differences between the cases” (Baxter & Jack, 2008:550).

To explore the factors affecting the governance of data privacy in IoT environments in South Africa, this researcher adopted a case study from multiple sources which according to Saunders and Lewis (2012) incorporates the use of numerous sources of evidence to examine a specific subject matter within its real-life context. This strategy supports the need to explore the subject matter from the perspective of different subjects to inform an insightful exploration of the research phenomenon.

1.7.3.2 Sampling methods

Methods for sampling in research, Neville (2005) states can be classified as either probability or non-probability sampling, with probability methods aligned to quantitative research and non-probability methods aligned to qualitative research. In the absence of a sample frame of the population, the researcher can employ non-probability sampling which encompasses sample selection based on the subjective judgement of the researcher (Saunders & Lewis, 2012). This researcher employed purposive sampling with the aim of selecting organisations and individuals who are best suited, in the researcher's judgement, to provide information on the factors affecting the governance of data privacy in IoT environments in South Africa. The sample for the study was drawn from IoT-based organisations located in four of the provinces in South Africa. The sample size was fifteen IoT-based organisations, varying in size, with similar operational scope. Data were collected from selected representatives till the point of saturation was reached. For the document analysis, recently updated personal information protection policies from ten countries were analysed.

1.7.3.3 Units of analysis or observation

The “unit of analysis” constitutes elements or members of the population of the research and generally denotes “humans, groups, organisations or institutions, human products or outputs

and events” (Welman et al., 2005:53). To identify the factors that affect the governance of data privacy in IoT environments in South Africa, the unit of analysis involved IoT-based organisations that collect, store, aggregate and disseminate data obtained through IoT devices and applications in South Africa, and selected data protection policy documents. The unit of observation included the person(s) responsible for privacy compliance (data controllers, data processors, compliance officers) in selected IoT-based organisations and the data privacy stipulations in the policy document.

1.7.4 Data collection

Data collection methods differ. Kothari (2004), notes that the onus is on the researcher to choose the applicable method based on a variety of factors, such as nature, scope and object of enquiry. Interviews were deemed appropriate to collect rich and insightful data from the selected participants, together with a document analysis of recently updated privacy protection policy documents. Interviews and document analysis may be described as follows.

- **Interviews:** As a qualitative research technique, intensive interviews of participants can be used to explore individual views and opinions on certain ideas and situations (Dudovskiy, 2018). The typology for collecting data via interviews are determined by the degree of structure and formality required. Saunders and Lewis (2012:72) concur that interviews can be categorised as “structured, semi-structured or unstructured interviews”. This researcher employed semi-structured interviews and data were collected till the point of saturation was reached.
- **Document analysis:** Impartial and consistent analysis of policies are facilitated by applying document analysis (Wach, 2013) in order to “elicit meaning, gain understanding, and develop empirical knowledge” (Bowen, 2009:27). Policy documents pertaining to data protection from ten countries, inclusive of the European Union (EU), San Marino, United States of America (USA), South Korea, New Zealand, Brazil, British Virgin Islands, Egypt, Kenya and South Africa were analysed. Data relating to the use of data and acquisition from a technological perspective were explored and extracted from the policy documents.

Both semi-structured interviews and document analysis were used to collect data in relation to the governance of data privacy in IoT environments in South Africa.

1.7.5 Data analysis

Data analysis involves analysing non-numerical or text data to develop a theory (Saunders & Lewis, 2012). Qualitative data analysis can be facilitated through the use of thematic analysis which allows for the emergence of categories from the data (Saldaña, 2009). Thematic

analysis involves “identifying, analysing and reporting patterns (themes) within data” (Braun & Clarke, 2006:79).

This research employed the six phases of thematic analysis as identified by Braun and Clarke (2006:87), including: “familiarizing yourself with your data, generating initial codes, searching for themes, reviewing themes, defining and naming themes and producing the report” to identify the categories and themes presented by the data. Both the interview and document analysis data were subjected to the thematic analysis steps. Five overarching contextual themes were developed from the analysis with twenty seven categories revealing the patterns and relationships from which emergent findings were appropriately drawn.

1.8 Ethics

The consequences of a researcher's actions should be given immense consideration when undertaking a project to ensure that the research is conducted in an ethical manner (Russell, 2006). This research followed prescribed ethical guidelines in conducting a scientific enquiry as recommended for researchers. For the purpose of this study, the researcher obtained ethical clearance from the Faculty of Informatics and Design (FID) at the Cape Peninsula University of Technology that fulfilled all ethical considerations required for the study. Before the interviews, participants were required to complete and sign a consent form and in so doing, confirmed participation in the research. The research subjects were informed that participation is voluntary and that they would be able to withdraw and refuse to answer any questions without repercussions. A more detailed explanation of how ethical considerations were covered in the research can be found in section 3.10.

1.9 Delineation

This research examined the implication of data collected, stored, aggregated and disseminated through IoT devices and applications on data privacy and not on data accumulated offline. Furthermore, the focus of the study was on compliance, governance and regulation of data privacy in IoT environments in South Africa and not on cyber security or the securing of data on devices. The framework is proposed for use in the context of South African IoT-based organisations. Thus, applicability to other environments and countries cannot be generalised, except where they fulfil similar contextual characteristics.

1.10 Contribution

This study contributed new knowledge by identifying the factors affecting data privacy regulation in South African IoT-based organisations. These factors provide an insight into the challenges faced by IoT-based organisations relative to the protection of personal information.

Furthermore, the study provided insight into best practices and guidelines towards the governance of data privacy in IoT environments in South Africa based on acceptable global standards. These guidelines and best practices was incorporated into a framework to inform and guide IoT-based organisations on how to effectively administer user's data privacy in line with stipulated regulations in South Africa and in adherence to global standards.

1.11 Summary

In this chapter an introduction to the study is presented and a broad overview of the research background, problem statement and the research question is provided. The research aim and objectives are presented and the research question is extended to formulate the research sub questions. The research methodology and contribution of the research are also outlined.

The research methodology expounds on the philosophical underpinning of the research. A subjectivist stance with an interpretivist approach was adopted to investigate and understand the nature of privacy regulation and governance in IoT environments in South Africa. A multiple-case study strategy was considered as appropriate for this study. It was employed to gain robust and meaningful information to explore the factors affecting the governance of data privacy in IoT environments in South Africa. The data were collected using a semi-structured interview and a document analysis of privacy regulation documents. A thematic analysis technique was utilised to identify the categories and themes from the data and to reveal relevant findings that provided rich insights into the research phenomenon.

The ethical considerations of the research in relation to participation in the study, data privacy, and consent, amongst others, were highlighted. Lastly, the delineation of the study and the contribution of the study to practice and the body of knowledge were also presented.

1.12 Thesis outline

The thesis is organised into seven chapters with the addition of references and appendices. The chapter contents and the progression of the thesis are illustrated in Figure 1.2 and a synopsis of each section is also provided.

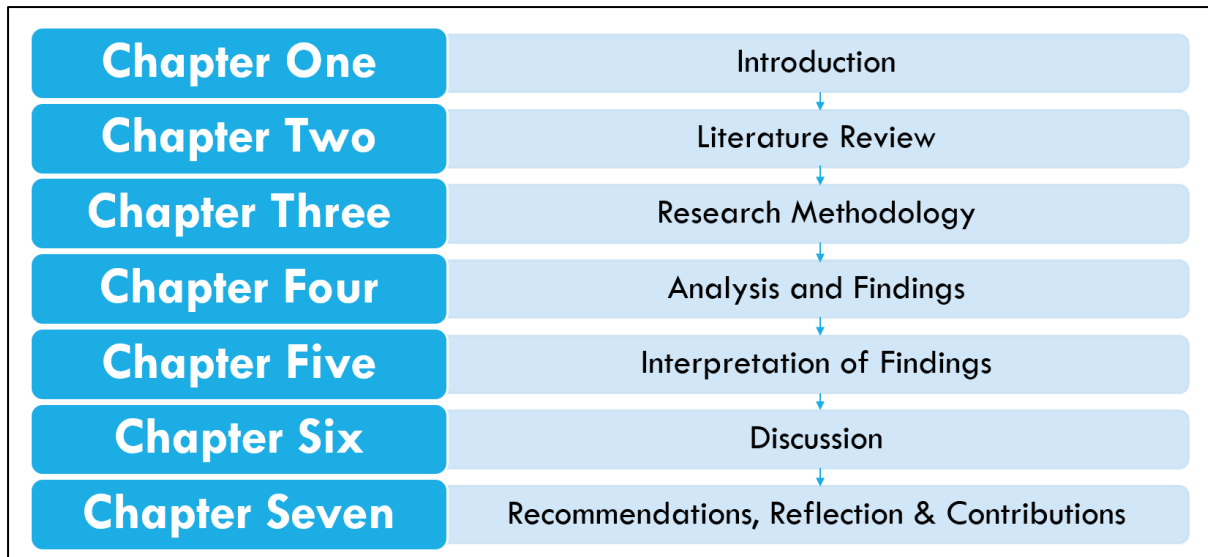


Figure 1.2: Thesis organisation and chapter clarification

Chapter One: This chapter introduces the study in terms of data privacy governance in IoT environments in South Africa. The chapter explores the lack of a general definition for privacy and the impact of technological advances on privacy as well as the increased susceptibility to cyber-attacks and data breaches. In addition, the chapter establishes the problem statement, aim, objectives and research questions. This chapter also briefly explores the research methodology employed, including the perimeters of philosophical underpinning, research approach and design. A view of the contribution and ethical considerations of the research are also presented.

Chapter Two: This component of the research provides a comprehensive review of the literature with regard to IoT and the effect it has had on the governance of data privacy. The review highlights various attempts from privacy academics to categorise privacy and provide classifications for privacy harms. The preferred nomenclature for the protection of personal information based on regulation, industry and academic literature is examined. In addition, the chapter explores the technological advances that have impacted privacy. It also offers an overview of IoT in relation to security, architectures, application domains, data privacy and IoT governance. Lastly, the chapter comprises of a related work section to explore other research and introduces the Activity Theory Framework which underpins the study.

Chapter Three: In this segment the research approach, design and methods adopted on the basis of the ontological and epistemological considerations, are presented. The chapter describes the research design adopted, expands on the research strategy, the sampling

methods, the methods of data collection and analysis, and the ethical considerations of the study.

Chapter Four: This chapter provides an overview of the context of the study. The data collection process for both the interviews and document review are highlighted. The outline of the analysis techniques employed for the interview data and document analysis are presented and summaries of emergent findings are illustrated.

Chapter Five: An interpretation of the findings are presented in relation to the Activity Theory Framework. Each of the components of the activity system (subject, tools, rules, community, division of labour, object and outcome) in relation to the study is described.

Chapter Six: This portion of the study provides a detailed discussion of the findings based on the research sub-questions. The chapter presents the collection of data, the categories, the themes and the findings derived from the analysis and uncovered by the research.

Chapter Seven: This chapter concludes the research with recommendations, a reflection, contributions of the research and the proposed framework of guidelines and best practices for governing data privacy in IoT environments in South Africa.

The literature review with a particular emphasis on the components in the context of the background and the problem statement are presented in the next chapter.

CHAPTER TWO: LITERATURE REVIEW

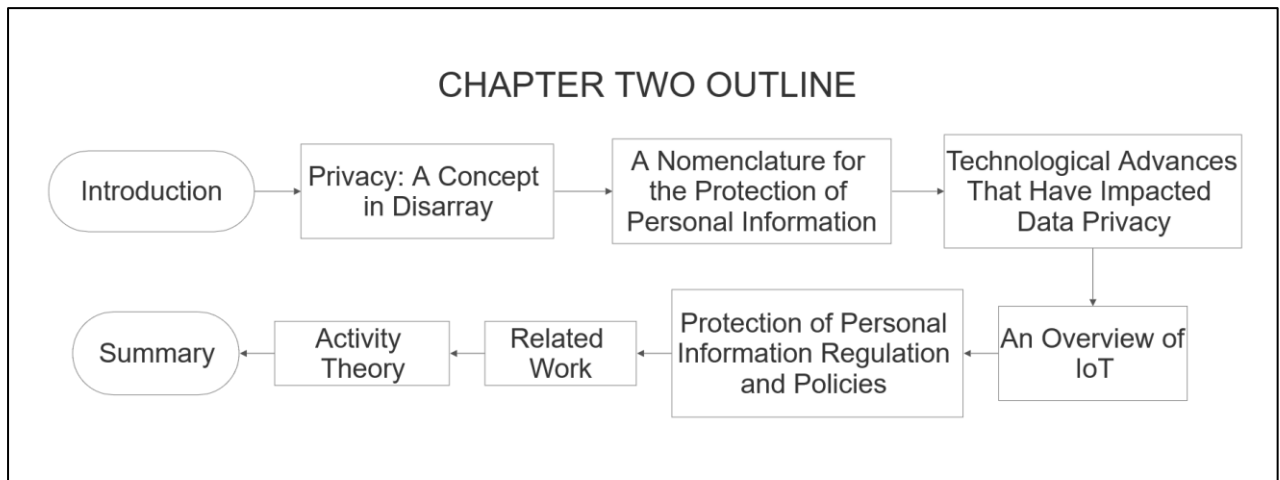


Figure 2.1: Chapter Two outline

2.1 Introduction

Privacy is a concept that transcends time. The Harvard Law Review published an article in December, 1890, titled “The Right to Privacy”, in which the authors called for an update to the law and for the right of a person “to be let alone”, due to “recent inventions and business methods” (Warren & Brandeis, 1890:195). This seminal article is considered the earliest proposition to gestate the concept of privacy as well as to highlight the requirement for amendments to the law brought on by advances in technology (Gutwirth, 2002; Zarsky, 2019).

The capacity to collect, store and analyse data has been greatly amplified with the advent of “computers and cyberspace” which has exponentially impacted privacy (Solove, 2004:3; van den Hoven et al., 2020). The argument that information technology intrudes on privacy has been prevalent in research and literature (Froomkin, 2000; Westin, 2003; Doyle et al., 2012; Lukacs, 2017). Innovations in technology amplify privacy concerns, as it generates voids within existing policies, thus leaving current legislative and security measures grappling to define meaningful solutions to rising privacy issues (Santanen, 2019).

Privacy concerns are exacerbated by growing global incidents which are evidenced by recent significant privacy protection updates to legislation by a number of nations. The EU’s 1995 Data Protection Directive, a set of principles and rules for the protection of data, serves as the basis for the General Data Protection Regulation (GDPR) which is considered the evolution of data protection for the digital age (European Commission, 2019). The GDPR was formally approved in 2016 and became enforceable in 2018. Consequently, it offers a more comprehensive regulation for the protection of personal data (Hoofnagle et al., 2019).

Likewise, in the USA, the State of California introduced the California Consumer Privacy Act (CCPA) in June 2018 which provides users with extensive control over the collection and usage of personal data by organisations, effective January 2020 (Persson et al. 2018; Palmieri III, 2020). However, in South Africa, despite the Protection of Personal Information (POPI) Act being signed in 2013, the final POPI Act regulations were only published five years later in December, 2018 by the South African Information Regulator (Moyo, 2019).

The implementation of the POPI Act has been marred by delays. It was initially due to take effect on the 1st of April 2020, but was further delayed by the COVID-19 pandemic. It finally came into effect on the 1st of July 2021 (Roux, 2021). Thus, the delayed implementation of the data privacy regulation in South Africa impacts on the governance of data privacy in general and in IoT-based environments, leaving the individual's personal data open to vulnerabilities, breaches and privacy invasions. In order to address the research problem, the literature review offers comprehensive evaluation of major concepts and constructs relating to the study.

The literature review provides an overview of privacy, data privacy and technological advances that have impacted on privacy and an overview of IoT (architectures, applications and challenges) as well as legislation, regulation and policies designed to govern privacy. The literature review was carried out using keywords stemming from the title, problem statement, research questions, aim and objectives of the study. These keywords were used in the exploration of relevant literature via CPUT's library electronic databases, i.e., Google Scholar, ScienceDirect, Scopus, Institute of Electrical and Electronics Engineers (IEEE), Emerald and Springer.

2.2 Privacy: a concept in disarray

Through the years researchers and scholars attempted to describe or define privacy, but it proved difficult to conceptualise in a generic manner. Examples of these are:

"A state in which one is not observed or disturbed by other people" or "being private and undisturbed" or "freedom from intrusion or public attention" (Thompson, 1993:711).

"The right to be let alone" (Warren & Brandeis, 1890:193).

"Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967:7).

“The selective control of access to the self or to one’s group” (Altman, 1975:18).

“Privacy is the interest that individuals have in sustaining personal space, free from interference by other people and organisations” (Clarke, 1999:60)

“The ability to control the acquisition or release of information about oneself” (Froomkin, 2000:1463).

Nevertheless, the general consensus amongst leading privacy academics is that privacy is a multifaceted concept which is factored over varying contexts and applications (Thomson, 1975; Clarke, 1997; Solove, 2002; Gutwirth, 2002; Moore, 2008; Finn et al., 2013). Consequently, the lack of an all-encompassing description of privacy led numerous scholars to rely on characteristics such as “classification, categorizing or listing of the different sub-areas” in a bid to define privacy as it applies within a particular circumstance or categorisation (Gutwirth, 2002:34; Watson et al., 2017).

In the late-90s, Clarke (1997) outlined four types of privacy, namely privacy of the person, privacy of personal data, privacy of personal behaviour and privacy of personal communication. Similarly, following an extensive investigation of cases within the law, Solove (2006:489) classified four undertakings detrimental to privacy: “information collection, information processing, information dissemination and invasion”. The classification provided by Clarke (1997) was further revised by Finn et al. (2013:272) to include seven privacy types: “privacy of the person, privacy of behaviour and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space and privacy of association (including group privacy)”. The above-mentioned privacy classifications are commonly referred to in privacy literature and are expanded on in the following section.

2.2.1 A categorisation of privacy

In his determination of privacy, Clarke (1997) takes a broad interpretation with his assertion that privacy involves a person's integrity and therefore includes every aspect of a human being's social needs. The outline discussed below can be seen as an evolutionary endeavour by a privacy academic to classify privacy in a way that is structured and logical (Finn et al., 2013).

Privacy of the person: It centres around the “integrity of an individual's body”, for example, “compulsory immunisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and compulsory sterilisation” (Clarke, 1997:2).

Privacy of personal behaviour: This concerns every facet of an individual's behaviour, specifically those of a sensitive nature, such as “sexual preferences and habits, political activities and religious practices, both in private and in public places” (ibid, 1997:2).

Privacy of personal communication: It relates to the capacity to communicate, by employing different media, free from being consistently observed and monitored by organisations and other individuals (ibid, 1997:3).

Privacy of personal data: This states that persons should have a modicum of authority over their personal data and their uses; the data should not be easily accessible to organisations and other persons (ibid, 1997:3).

2.2.2 A taxonomy of privacy harms

In a bid to exhaustively identify privacy issues, brought on by innovative technologies, Solove (2006) developed a classification for the identification of privacy infringements. The Solove Framework focusses on the adverse effect of technological advances on privacy rather than stipulating specific types of privacy (Santanen, 2019). The four privacy harms are discussed below and further expanded in relation to their impact on the individual.

2.2.2.1 Information collection

The methods of gathering data and procurement of information can cause damage, even if the information is not discovered or publicised; information collection comprises “surveillance and interrogation” (Solove, 2006: 491).

Surveillance: This pertains to audio (listening) and visual (watching) as well as the “recording of an individual's activities” (ibid, 2006:490).

- Methodical surveillance, enabled by evolving technologies, Brayne (2017) observes have come to be an inescapable feature of an individual's daily life. Technologies such as Radio Frequency Identification (RFID)-enabled passports and identification documents, Global Positioning System (GPS), unmanned aerial vehicles, Close Circuit Television (CCTV), can be employed for the purposes of profiling individuals, groups and communities (Mavriki & Karyda, 2018). Steinfeld (2017:1664) emphasises that digital surveillance integrate and access numerous databases, thereby increasing the “scope, reach and intensity” of

observation or “dataveillance”. As a result, individual “freedom, creativity and self-development” can be influenced negatively by the employment of surveillance as an instrument for social government (Santanen, 2019:10).

Interrogation: It concerns different forms of inquisitorial searches for information and involves the “pressuring of individuals to divulge information” (Solove, 2006:500).

- Interrogation utilises coercive measures to obtain information and can also result in the information being distorted if taken out of context (Santanen, 2019). Information can be deemed property. Therefore, Gryz (2017) asserts that efforts to obtain such property via coercive action signifies a violation of privacy.

2.2.2.2 Information processing

“Information processing” according to Solove (2006:506) relates to the management of data that have previously been accumulated and refers to data manipulation, storage and usage. It consists of: “aggregation, identification, insecurity, secondary use and exclusion”.

Aggregation: This entails the “gathering together of information about a person”, subsequently new facts may be unexpectedly revealed when the aggregated data are analysed (ibid, 2006:507).

- Separate pieces of data about a person, distributed across online and offline activities, divulge very little about an individual, however harms to privacy occur from the accumulation of data from a variety of sources to syndicate information (Pizzirani et al., 2017; Bailey et al., 2018). Consequently, an individual's personal information has become a soaring commodity to be “bought, sold and traded” by organisations (Santanen, 2019:11).

Identification: It relates to associating or linking true identifiable information (for example, ID numbers, fingerprints or DNA) to specific persons or possible identification by the inclusion of particular physiognomies that can distinguish individuals (Solove, 2006; Nissim & Wood, 2018).

Insecurity: This refers to issues arising from methods of protecting and handling of a person's information (Solove, 2006).

- Insecurity can be regarded as the inability to protect stored data from being leaked and prevent unauthorised access (Mansell, 2015, cited in Pizzirani et al., 2017). The storage of an individual's data intensifies the threat of exploitation through data leaks, identity theft and hacking (Santanen, 2019).

Secondary use: This encompasses using data contrary to its intended or specified purpose, without an individual's consent (Solove, 2006).

- Secondary use can be discerned as a confidentiality breach since information is used for purposes other than what was acquiesced to or desired (Pizzirani et al., 2017).

Exclusion: This involves the “failure to provide individuals with notice and input about their records” (Solove, 2006:523).

- Exclusion can be described as not having knowledge of what data are being gathered or the application of the information, therefore it inhibits inspection and possible correction of an individual's own records (McCausland et al., 2018; Santanen, 2019).

2.2.2.3 Information dissemination

The above-mentioned problems relate to “information collection, storage and use of data”, whilst Solove (2006:525) contends that the distribution of information and disclosure of personal data have far reaching implications for individuals, including: “breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation and distortion”.

Breach of confidentiality: This involves the “revelation of secrets about a person” and “violates the trust in a specific relationship” (ibid, 2006:256).

- Inevitably, these types of infringements result in a loss of trust amongst people or individuals and corporations (Santanen, 2019). Therefore, the type of data or its sensitivity, becomes irrelevant in confidentiality breaches, as it indicates an inability to safeguard information, resulting in a lack of trust of the parties or organisations involved (Oates et al., 2018).

Disclosure: It refers to the revelation of information that is true about an individual, thus causing reputational damage from the discovery (Solove, 2006).

- The adverse effect of information disclosure or misuse, Nissim and Wood (2018:2) establish can relate to a person's “relationships, reputation, employability, insurability or financial status” or become the basis of “civil liability, criminal penalties or bodily harm”. Disclosure threatens a person's safety and autonomy; the revelation of basic information poses a risk to lives, for example, “stalking, domestic abuse or witness protection” (Santanen, 2019:12).

Exposure: This closely relates to disclosure, however the information exposed causes an affront to social practices as opposed to information about an individual's personality or character (Solove, 2006).

- The exposed information can include undertakings of a private or delicate nature such as “grief, trauma, injury, nudity, sex and defecation” (Oates et al., 2018:32).

Increased accessibility: It relates to the ability to easily access publicly known information, thus increasing the possibility of disclosure (Solove, 2006).

- Public information is more readily accessible owing to the advances in technology (Gryz, 2017). Subsequently, the potential for disclosure becomes greater with increased accessibility to data and information that have been made public (Santanen, 2019).

Blackmail: It alludes to the threat of disclosure of information that individuals would prefer to remain secret, rather than actual disclosure (Solove, 2006).

- Gryz (2017) argues that blackmail only relates to privacy protection in a marginal way, since it may encompass threats other than the revelation of personal data. Nevertheless, exercising control or sway over persons or organisations through threats of dissemination of information can be seen as blackmail (Santanen, 2019).

Appropriation: It comprises of using the identity or character of an individual to further the motives and objectives of someone else and involves the public persona of an individual (Solove, 2006).

Distortion: This implies manipulating the perception and judgement of an individual by others, as well as publicly exposing inaccurate information concerning a person (ibid , 2006).

- It includes revealing information of an untruthful or deceptive nature that may be damaging to the reputation of an individual or origination (Santanen, 2019). Moreover, Oates et al. (2018) stress that the way in which a person is publicly perceived, is influenced through information that is misleading and untrue.

2.2.2.4 Invasion

The final categorisation does not require a relation to collection, processing or dissemination of information to be harmful and includes “intrusion and decisional interference” (Solove, 2006:552). Intrusions violate privacy of a psychological and physical nature and decisional interference relates to “autonomy and liberty” rather than privacy. Therefore, Gryz (2017:270) contends that these two harms do not directly violate “informational privacy”.

Intrusion: This pertains to onslaughts or infiltrations into an individual's daily life through the disturbance of the person's daily activities, altering routines, destroying solitude and creating feelings of unease and discomfort (Solove, 2006).

Decisional interference: It stems from unwanted interfering by the government into a person's determinations about their private life (ibid, 2006).

- This classification is further broadened by Oates et al. (2018) to include interference by corporate entities and organisations as well as mothers, fathers and guardians.

2.2.3 Seven types of privacy

A significant difference between the two classifications discussed above is the fact that, according to Solove (2006) "taxonomy of privacy harms are reactive" in nature and to Clarke (1997) those "types of privacy are pro-active and protective" (Finn et al., 2013:3). According to Finn et al. (2013), the expansion of the Clarke (1997) categories are compelled by the advances in technology and the classification's inadequacy to address the impending privacy issues arising from emergent technologies. Contrary to the Solove (2006) taxonomy that identifies privacy problems, this classification proposes seven types of privacy essential for practical safeguarding and reduction of the broad concept of privacy (Friedewald et al., 2015).

Privacy of the person: This includes the prerogative to retain the privacy of human characteristics, e.g. "genetic codes and biometrics" and functions (Finn et al., 2013:4).

Privacy of behaviour and action: It consists of actions that occur in public and private domains and relates to issues of a sensitive nature such as "sexual preferences and habits, political activities and religious practices" (ibid., 2013:4).

Privacy of personal communication: This relates to circumventing communication interception, use of wiretaps, "directional microphones", intercepting communications via telephone or over wireless connections or recording and accessing emails (ibid., 2013:5).

Privacy of data and image: It involves defending against the automatic availability of a person's data to organisations and other individuals and retaining some measure of control over the information and its usage (ibid, 2013).

Privacy of thoughts and feelings: This embraces a person's prerogative to keep their thoughts and feelings private and pertains to the "right to think whatever they like" as well as not having their thoughts and feelings made public (ibid, 2013:5).

Privacy of location and space: It comprises of having the freedom to venture out in public places or “semi-public spaces” without the possibility of identification, tracking or monitoring (ibid, 2013:5).

Privacy of association (including group privacy): This encompasses an individual’s right of association with anyone, without fear of being observed (ibid, 2013).

2.3 A nomenclature for the protection of personal information

The terminologies, *data privacy* or *data protection* were formulated to describe legislative action for the protection of personal information in the 1970s due to the increased usage of computerised databases for information storage (Bygrave, 2010; Greenleaf, 2013; Cobb, 2016). There have been divergent views on a universal nomenclature for the protection of personal information and the employment of the terms essentially depend on the continent or country (Bygrave, 2010; Cobb, 2016; Richardson et al., 2017; Schwartz, 2019).

To illustrate the varying definitions for the above-mentioned terms, the following section includes a compilation from legislative policies, industry-specific documents and scholastic articles.

2.3.1 Applied terminology for privacy regulation

A document analysis of recently updated personal information protection policies from ten countries between 2018–2021 was conducted in Chapter Four. It was established that the preferred term in the regulatory documents was *data protection*. Yet, none of the documents analysed, provided a concrete definition for the term.

2.3.2 Industry-specific definitions from Google search

A search of the internet for *data privacy* and *data protection* listed a plethora of descriptions from a range of industries. The different definitions found via a Google search for these terms have been catalogued in Table 2.1. Only those found on page one at the time of the search have been listed:

Table 2.1: Industry-specific definitions on Google

Terms	Definitions	Websites or Links	Context
Data Privacy	“governs how data is collected, shared and used” and is “concerned with the proper handling of data – consent, notice and regulatory obligations” (Peters, 2020).	https://www.varonis.com/blog/data-privacy/#dimensions	Varonis is a cybersecurity enterprise that provides protection for organisations’ data.

	<i>"describes the practices which ensure that the data shared by customers [are] is only used for its intended purpose" (Emotiv, n.d.).</i>	https://www.emotiv.com/glossary/data-privacy/	EMOTIV is a bioinformatics enterprise that tracks and monitors cognitive performance and emotions in physical and virtual objects.
	<i>"relates to how a piece of information—or data—should be handled based on its relative importance" (NortonLifeLock, n.d.).</i>	https://www.lifelock.com/learn-identity-theft-resources-what-is-data-privacy-and-why-is-it-important.html	NortonLifeLock is a cybersecurity company.
	<i>"is a part of the data protection area that deals with the proper handling of data" and "includes how data should be collected, stored, and shared with any third parties, as well as compliance with the applicable privacy laws" (Data Privacy Manager, 2020).</i>	https://dataprivacymanager.net/5-things-you-need-to-know-about-data-privacy/	Data Privacy Manager provides a data privacy platform to organisations for the control of personal data.
	<i>"is about authorized access — who has it and who defines it" (Robinson, 2020).</i>	https://blog.ipswitch.com/data-privacy-vs-data-protection	Ipswitch is a subsidiary of Progress, an organisation that aids enterprises in application development and digital experience technologies.
Data Protection	<i>"refers to the practices, safeguards, and binding rules put in place to protect your personal information and ensure that you remain in control of it" (Masse, 2018).</i>	https://www.accessnow.org/data-protection-matters-protect/	Access Now is a digital security organisation.
	<i>"is the fair and proper use of information about people" (Information Commissioner's Office, n.d.).</i>	https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/	The Information Commissioner's Office (ICO) is an independent organisation advocating the protection of information rights.
	<i>"is about safeguarding our fundamental right to privacy, which is enshrined in international and regional laws and conventions" and "is commonly defined as the law designed to protect your personal information, which is collected, processed and stored" (Privacy International, 2017).</i>	https://privacyinternational.org/explainer/41/101-data-protection	Privacy International aims to provide privacy protections by raising awareness of and monitoring threats to privacy.
	<i>"is about securing data against unauthorized access" (Robinson, 2020).</i>	https://blog.ipswitch.com/data-privacy-vs-data-protection	Ipswitch is a subsidiary of Progress, an organisation that aids enterprises in application development and digital experience technologies.

2.3.3 Definitions from academic literature

In this section definitions from academic literature are highlighted. The different definitions found via electronic databases such as Google Scholar and EBSCOhost are listed in Table 2.2. Although not exhaustive, the listings serve as a demonstration of the various descriptions for the terms.

Table 2.2: Academic literature definitions

Terms	Definitions	Area of Research	Context
Data Privacy	<i>"a derivative of the substantive right to privacy in that it is about data that has been created about an individual (1) by him- or herself, (2) by others through observations and analysis, or (3) by the consumption or processing (i.e., use) of that data about an individual by others"</i> (Dennedy et al., 2014:26).	Information Privacy and Security	Privacy engineering is introduced by the authors to enable the legitimate use, storage and distribution of private or personal information.
	<i>"is the necessity to preserve and protect any personal information, collected by any organization, from being accessed by a third party"</i> (Ahamd et al., 2018:9).	Information and Computing Technology	Describes threats to data security in cloud environments.
	<i>"the ability to control the acquisition or release of information about oneself"</i> (Froomkin, 2000:1463).	Law	The author explores the rapid deployment of privacy-destroying technologies by governments and businesses and the threats on informational privacy.
	<i>"that aspect of social order by which persons control access to information about themselves"</i> (Fried, 1968:493).	Law	The foundations of the right to privacy is examined by the author.
Data Protection	<i>"is ensuring that confidential and personal information regarding a stakeholder is maintained and processed in a secure and legally compliant manner and is prevented from passing from one person or entity without the consent of the individual. It is the implementation of administrative, technical, or physical measures to guard against the unauthorized access to data"</i> (Toker, 2013:752)	Business and Management	The article was found in the Encyclopaedia of Corporate Social Responsibility which provides an encompassing overview of societal issues.
	<i>"is concerned with the interest of the data subject, and is intended to prevent the abuse of the subject's data"</i> (Byrne & Pfefferle, 2015:18).	European Policy	The article proposes a framework for a comprehensive agreement for data protection between the EU and US.
	<i>"regulatory instruments (statutes, recommendations, guidelines, etc.) to protect privacy and related interests with regard to the processing of personal data"</i> (Bygrave, 2010:166)	Law	The author examines the development of governing tools for the protection of private or personal

			information in various regions.
	<i>"the protection of personal data in order to guarantee privacy"</i> (Diamantopoulou et al., 2017:192)	Technology and Engineering	The authors propose a number of privacy process patterns for Privacy by design solutions.

2.4 Technological advances that impacted on data privacy

The pervasive nature of advancing technologies, intensification of connectivity and expanding resources for information retrieval affected data privacy directly (Dunlap et al., 2017; van den Hoven et al., 2020). Therefore, it would be remiss to discuss privacy without an examination of a number of technological advances that impacted on data privacy (van den Hoven et al., 2020). The internet is the universally used method of information distribution today and established itself as a vital part of society (Kaur et al., 2017). This section explores a brief history of the internet and the influence of internet-based technologies and applications on society and data privacy.

2.4.1 A brief history of the internet

A worldwide phenomenon, the internet as we know it, had its origins as a small research network and grew to service over four billion users. Its growth from 2005–2019 is detailed in figure 2.2 (Clement, 2020).

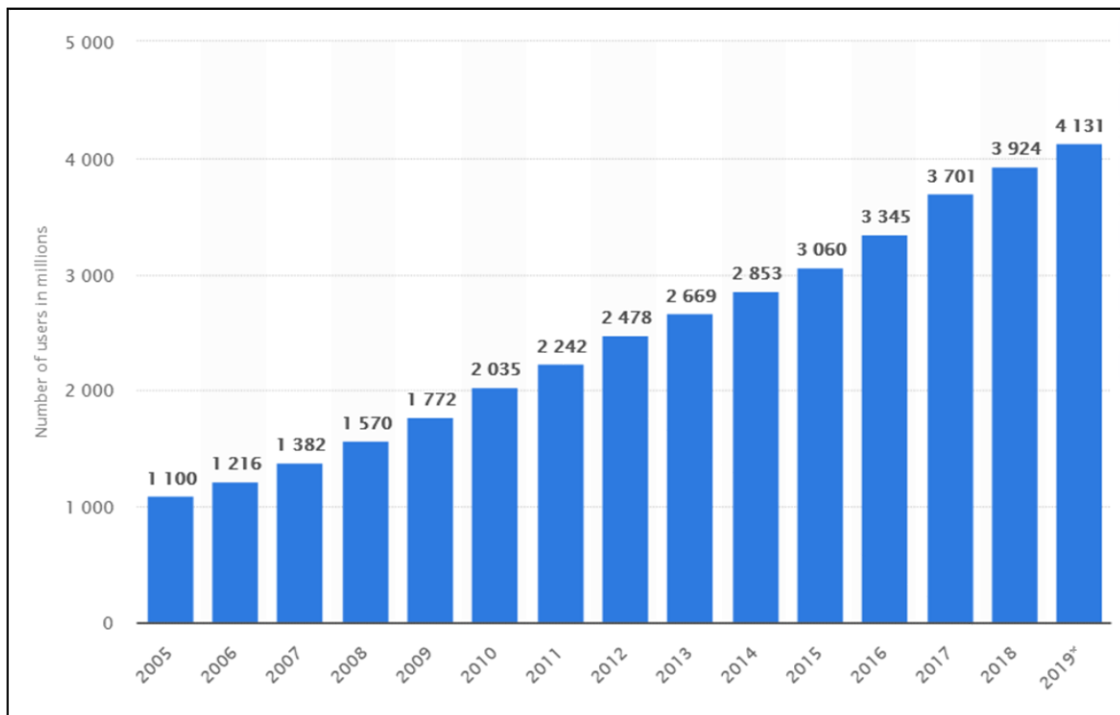


Figure 2.2: Global number of internet users 2005–2019 (Clement, 2020)

The Cold War between the USA and the Soviet Union necessitated the creation of a communications network that would withstand the devastation of a nuclear attack (Naughton, 2016). In the early 1960s, Paul Baran and Donald Davies, continents apart and unbeknownst to each other, designed a method of data transmission known as packet switching (Hafner & Lyon, 1996). The Advanced Research Projects Agency (ARPA) contracted the Bolt, Beranek and Newman (BBN) Corporation to build the first packet switch, called the Interface Message Processor (IMP), in December 1968 (Mowery & Simcoe, 2002). Development of the Advanced Research Projects Agency Network (ARPANET) was completed in 1972 and it connected fifteen sites across the USA at the time of its launch in Washington, DC (Leiner et al., 1997). Incidentally, that same year electronic mail (email) was introduced as a method of coordination for the developers of ARPANET (Cohen-Almagor, 2011).

Towards the mid-1970s, the developers at ARPA or rather DARPA (Defense Advanced Research Projects Agency) as it was now termed, found themselves working on three separate networks, thus accelerating the requirement for “internetworking” and the development of the networking protocol, Transmission Control Protocol/Internet Protocol (TCP/IP) (Naughton, 2016:9). In 1983, TCP/IP became the standard for ARPANET and in 1985, the National Science Foundation (NSF) prescribed the use of TCP/IP on its network (NSFNET) in all universities that were receiving funding from the Foundation, resulting in TCP/IP emerging as the principal network protocol for the internet (Leiner et al., 1997; Mowery & Simcoe, 2002; Cohen-Almagor, 2011). Additionally, November 1983 saw the establishment of an addressing scheme known as the Domain Name System (DNS) which was widely adopted in 1986 (Hafner & Lyon, 1996).

ARPANET was formally decommissioned on the 28th of February 1990 and NSFNET became the major backbone for the growing national network (Hafner & Lyon, 1996; Leiner et al., 1997; Mowery & Simcoe, 2002; Naughton, 2016). In the late 1980s, Western Europe developed its own infrastructure. However, it lacked in scale and standardisation which resulted in several European networks as well as networks from Canada, Australia, Israel, Japan, Mexico and New Zealand, joining NSFNET in 1988 and 1989 (Mowery & Simcoe, 2002). The Internet Society came into existence in 1991 and nine countries, including South Africa, joined NSFNET (Cohen-Almagor, 2011). Commercial organisations, known as Internet Service Providers (ISPs), replaced the NSF in providing the infrastructure for the internet in 1995 (Mowery & Simcoe, 2002; Naughton, 2016).

Meanwhile, at the end of 1990, Tim Berners-Lee, a researcher at CERN (Conseil Européen pour la Recherche Nucléaire or European Organisation for Nuclear Research) completed

development of a “new document format” named Hyper Text Mark-up Language (HTML) and a “document retrieval protocol” called, Hypertext Transport Protocol (HTTP) according to Mowery & Simcoe (2002:1378). Thereby giving birth to the World Wide Web (WWW) and further expanding the use of the internet (Cohen-Almagor, 2011).

The spring of 1993 brought with it the creation of Mosaic, a web browser, whose launch by the National Center of Supercomputer Applications (NCSA) would prove pivotal to the evolution of the web and the internet; one of the creators later formed Netscape, the forerunners in commercialising the web (Curran et al., 2012). The organisation created the Netscape Navigator which became the dominant browser and when the company went public in 1995, it initiated the “dot-com bubble”. The subsequent crash of the market in March 2000 eventually burst the proverbial bubble and ushered in the Web 2.0 era (Mowery & Simcoe, 2002; Cohen-Almagor, 2011; Naughton, 2016:14).

Postulations of the concept of Web 2.0 first emerged in 2004 when technology observer, Tim O’Reilly deliberated the shared key features of new organisations and those that have survived the market crash (O’Reilly, 2009; Harris & Rea, 2009; Naughton, 2016). These characteristics included:

- exploiting and utilising the “collective intelligence” available
- content generated by web users
- dynamically interconnected services called “mashup” through Really Simple Syndication (RSS) or Application Programming Interfaces (APIs)
- continuous enhancement of web services or a “perpetual Beta” stage
- using the web as a platform (O’Reilly, 2009; Levy, 2009:122; Naughton, 2016:16; Newman et al., 2016; Widiasari et al., 2018:119)

The emphasis of Web 2.0 applications were focussed on user participation, inclusive of, but not limited to: wikis, blogs, podcasts, social networks and virtual worlds (O’Reilly, 2009; Harris & Rea, 2009; Levy, 2009; Baxter et al., 2011; Widiasari et al., 2018). Thus, the ways in which society accesses and utilises the internet as well as infrastructure advancements to facilitate these changes, though evolutionary, negatively affected the privacy of individuals (Curran et al., 2012; Naughton, 2016; van den Hoven et al., 2020).

The section below explores a selection of transformative, internet-based developments and applications, specifically social media, big data, mobile devices, cloud computing and IoT as well as their implications on data privacy.

2.4.2 Social media

Social media comprises of technologies that provide a digital environment in which users share information or content (Appel et al., 2020). The scale of social media growth and its influence on individuals can only be described as unparalleled in its proliferation (Goel & Gupta, 2020). Worldwide, over 3.6 billion people were using social media in 2020. Illustrated in Figure 2.3 are the most popular social media networks. Notable is Facebook's (now known as Meta) 2.85 billion active monthly users as well as the sum of 3.51 billion users of their core products namely Facebook, WhatsApp, Facebook Messenger and Instagram (Statista Research Department, 2021b). Thus, social media giants such as Facebook (Meta), YouTube and TikTok possess and continue to amass an enormous quantity of "user-generated data" that could be used for valid purposes or with criminal intent (Beigi & Liu, 2020:2).

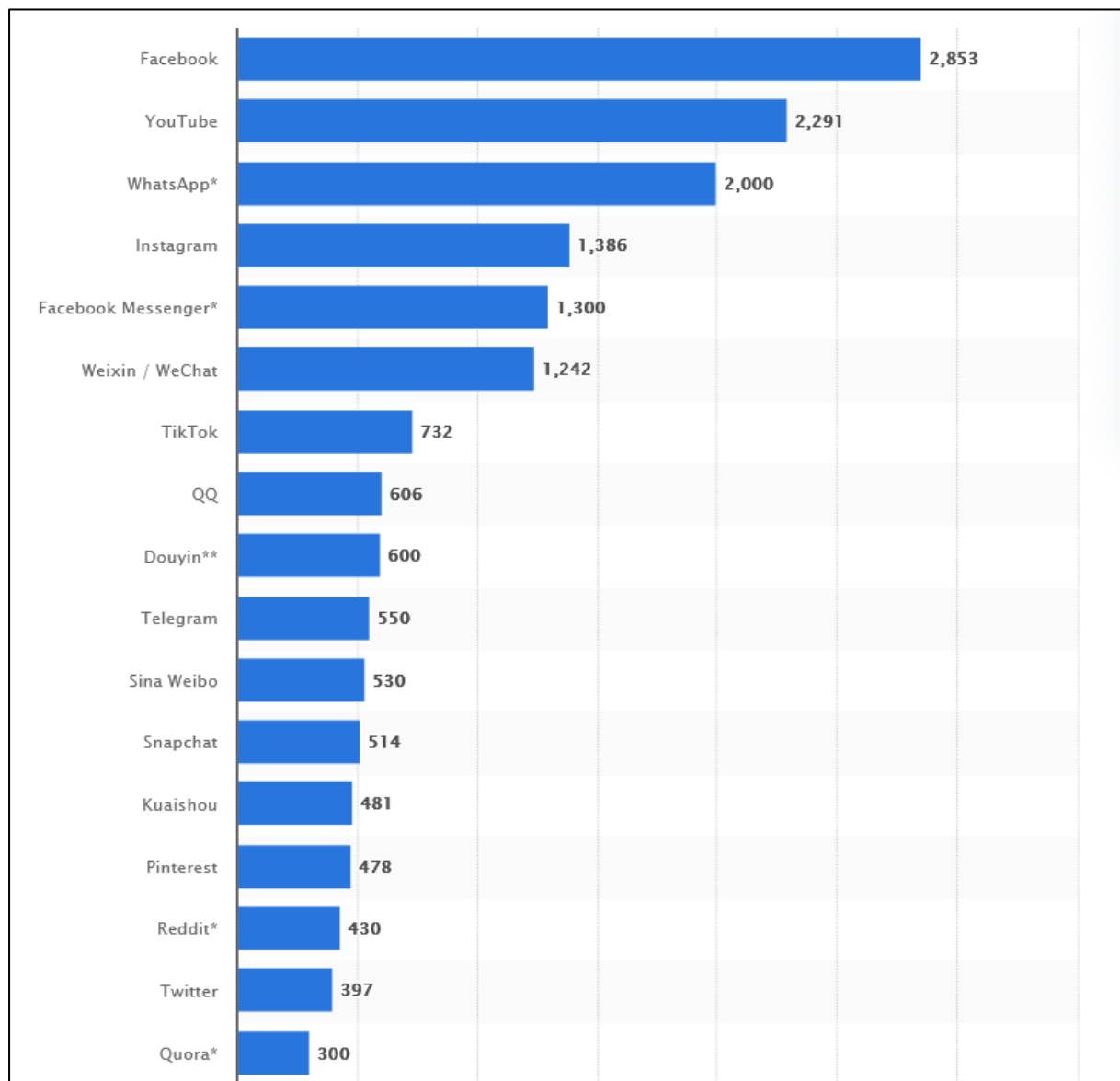


Figure 2.3: Popular social media networks worldwide (Statista Research Department, 2021b)

Van der Hoven et al. (2020) observe that Social media users are often enticed to share sensitive or personal information in order to use or receive the benefits of social networking sites. The gathering, mining, extraction and availability of sensitive or personal information became a concern for users' privacy due to the risk of possible disclosure (Jozani et al., 2020). Personal information disclosure relates to the possibility of users' identities being mapped to leaked data or the ability to make inferences about an individual's preferences or views in the event of a breach (Beigi & Liu, 2020).

2.4.3 Big data

The phrase, *big data* has its origins in the 1990's and was used to delineate "the explosion in the quantity (and sometimes, quality) of available and potentially relevant data, largely the result of recent and unprecedented advancements in data recording and storage technology" (Favaretto et al., 2020:2). The basic traits of big data, according to Oussous et al. (2018:433) are known as the 3Vs: "volume" (large amounts), "velocity" (rapid processing) and "variety" (diverse sources). Due to the availability of more quantities of data, additional attributes were added, including "veracity, value, and variability" (Favaretto et al., 2020). Thus, big data involves the extraction of useful information from substantial amounts of data that are gathered from an ever-growing variety of disciplines and applications, and as such, providing organisations with the means to analyse their clients' activities and habits (Saura et al., 2021; Talari et al., 2021). However, Wang et al. (2021) contend that user privacy is not only at risk by the gathering and utilisation of personal data, but also by negligent management of personal information evidenced by the increased incidents of data infringements.

2.4.4 Mobile devices

Mobile devices, according to Zaidi et al. (2021) are the preferred option for individuals for daily activities due to the advances in technology and access to affordable data plans, faster connections and Wi-Fi. Globally, the number of smartphone users exceeded six billion in 2020. O'Dea (2021) predicts a year-on-year growth of this figure. The extensive use of mobile devices and applications raise serious security concerns due to the accessibility to the individual's location, contacts, photos and other sensitive information (Wang et al., 2020). Consequently, the tracking of users' online mobile behaviour such as their location through GPS sensors, poses a risk to the individual in case of unauthorised access or a breach (Almusaylim & Jhanjhi, 2020). In addition to that, mobile devices at work increase the risk of security and privacy exposures for organisations as these devices can provide a gateway for malicious attacks on the organisation and access to confidential information (Belanger & Crossler, 2019).

2.4.5 Cloud computing

Cloud computing involves the provision of computing, storage and software resources that are located remotely and accessed over the internet (Almtrf et al., 2019; Sun, 2020). Emerging as the preferred solution for processing and storing immense volumes of data, cloud computing extends to a number of industries such as manufacturing, healthcare and education (Parikli et al., 2019). Cloud computing offers different deployment models, namely public, private, community and hybrid, indicative of how resources are shared (Stoyanova et al., 2020). Almusaylim and Jhanjhi (2020) point out that for the provision of services, it also offers three architectures: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

Although there are numerous benefits, the challenges for cloud computing include concerns over security and data privacy (Gahi & Alaoui, 2019). Almtrf et al. (2019) assert that the possibility of data breaches in cloud environments are amplified by the number of cloud users, meaning that access control poses another concern.

2.4.6 The Internet of Things (IoT)

A new era of the internet, fuelled by IoT, has led to the emergence of smart devices and technologies as well as intelligent services and applications (Wu et al., 2020). Everyday devices are able to communicate over the internet via sensors, thereby providing greater automated services and functionality (Wheelus & Zhu, 2020). The application of IoT seems to be limitless, from smart utility devices such as smart water meters and smart wearables, for example, smart watches to industry standard devices for automation of services. Hassija et al. (2019) predict that by 2022 the number of devices could be in the region of 20.4 billion. The benefits of IoT have been seen in many sectors, specifically in the healthcare sphere, for example in the fight against COVID-19, where IoT was used to enable remote monitoring and digital diagnostics (Peerzade, 2021). Nevertheless, privacy concerns have been raised, in particular with regard to the vast amounts of “behavioural and physiological” data smart wearables collect (Cilliers, 2020:1). As the number of IoT devices and services increase, so does the number of attacks targeting IoT devices (Stoyanova et al., 2020). In a report released by antivirus and cyber security firm, Kaspersky, there was approximately 1.5 billion incidents involving IoT devices in the first six months of 2021 (Seals, 2021).

In the following section the discussion regarding IoT into the key areas of interest in relation to the study is further elucidated.

2.5 An overview of IoT

This section expands on IoT as discussed above and includes an overview of the security requirements and challenges, architectures, application domains as well as data privacy and governance.

2.5.1 Security in IoT environments

The protection of devices, networks and data from unauthorised access and use is a major concern in IoT. Thus at a minimum, El-Gendy and Azer (2020) postulate that an IoT environment requires confidentiality, integrity and availability (CIA). Table 2.3 provides a brief overview of the security requirements and challenges in an IoT environment.

Table 2.3: Security requirements and challenges for IoT

Term	Description
Security requirements	
Confidentiality	Only intended parties are able to understand information being exchanged and only those with authorisation have access to available information (Rayes & Salam, 2017; Lin et al., 2017; Hatzivasilis et al., 2019).
Integrity	Guarantees data being transmitted have not been tampered with (Leloglu, 2017; Hatzivasilis et al., 2019).
Availability	Devices, data and services are available and not interrupted (Rayes & Salam, 2017; Hatzivasilis et al., 2019).
Authentication	Requested operations are only performed by those with permission (Leloglu, 2017; Singh et al., 2020).
Non-repudiation	Non-deniability of an action performed by an entity (Rayes & Salam, 2017; Gafurov & Chung, 2019).
Privacy	Only the corresponding user can control, access and process data (Lin et al., 2017; Gafurov & Chung, 2019).
Trust	Ensures that the objectives related to security and privacy can be achieved between objects, IoT layers and applications (Lin et al., 2017; Gafurov & Chung, 2019).
Security Challenges	
Interoperability	Functionality of interconnected heterogeneous devices should not be prevented by security solutions (Leloglu, 2017; Yebenes & Zorrilla, 2019).
Resource Constraints	Security techniques can be difficult to apply due to limited resource abilities (for example, storage, CPU, battery memory and transmission range) in IoT devices (Rayes & Salam, 2017; Altaf et al., 2019).
Data Volumes	The volume of generated data will be enormous, thus efficient safeguards should be established to secure the data (Leloglu, 2017; Yebenes & Zorrilla, 2019).
Multiple Technologies	Vulnerabilities of multiple technologies combined in IoT need to be secured (Rayes & Salam, 2017; Fahmideh & Zowghi, 2020).
Privacy Protection	Authentication mechanisms should be in place to prevent unauthorised access, modification and deletion of data (Leloglu, 2017; Jha et al., 2021).
Scalability	Proposed security mechanisms should be scalable to accommodate the billions of devices on an IoT network (Lin et al., 2017; Yebenes & Zorrilla, 2019).

2.5.2 Architectures for IoT

Currently, there is no universally adopted or agreed upon architecture for IoT, nevertheless researchers and academics have proposed three-, four- and five layer architectures (Sethi &

Sarangi, 2017; Burhan et al., 2018; Gafurov & Chung, 2019; Singh et al., 2020;) as depicted in Figure 2.4.

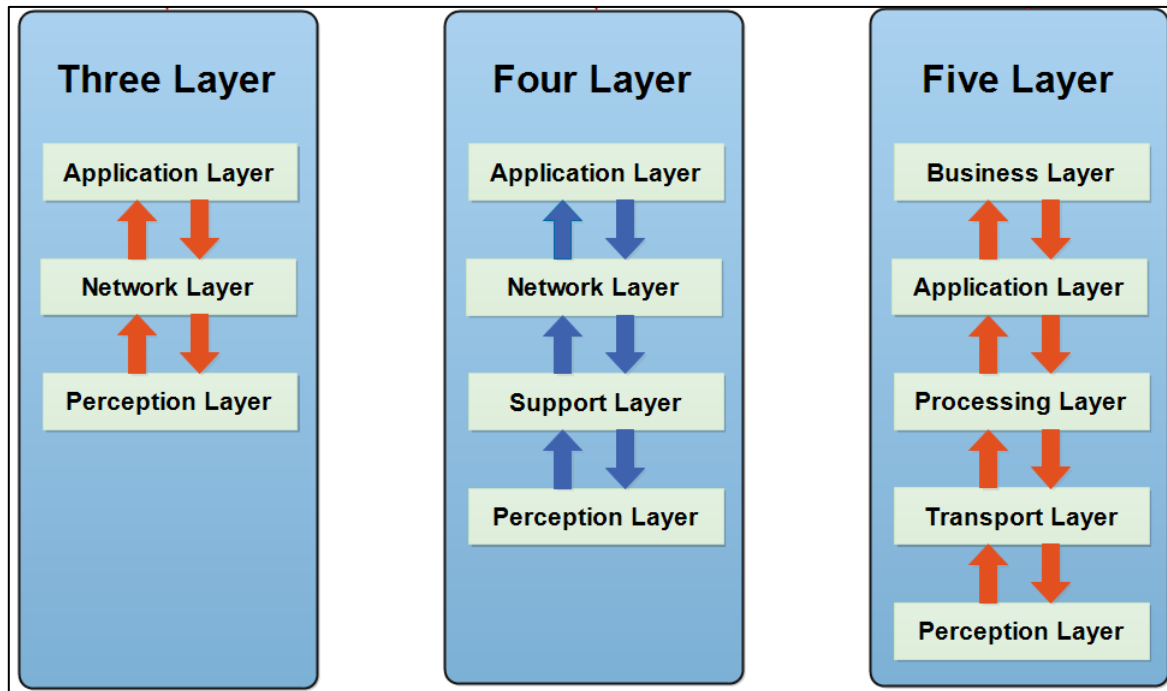


Figure 2.4: IoT architectures (Burhan et al., 2018:10)

Research, in the early stages of IoT, identified a basic three layer architecture which included the perception, network and application layers (Singh et al., 2020). Continuous IoT advancement and development led to the development of four layered architecture that includes a support layer between the network and perception layers (Burhan et al., 2018; Aly et al., 2019; Farooq & Waseem, 2020). The support layer is used for the authentication of users and information received from the perception layer as well as forwarding information to the network layer (Burhan et al., 2018; Tewari & Gupta, 2020). A five layer architecture was proposed to negate storage and security limitations within the four layer architecture (Singh & Mahapatra, 2020).

This study examined the five layered architecture which is considered to fulfil the IoT requirements for security and privacy (Burhan et al., 2018; Gafurov & Chung, 2019).

2.5.3 Five layer architecture, technologies and security threats

A description of the basic technologies and security vulnerabilities at each layer of the five layer architecture is presented in Figure 2.5.

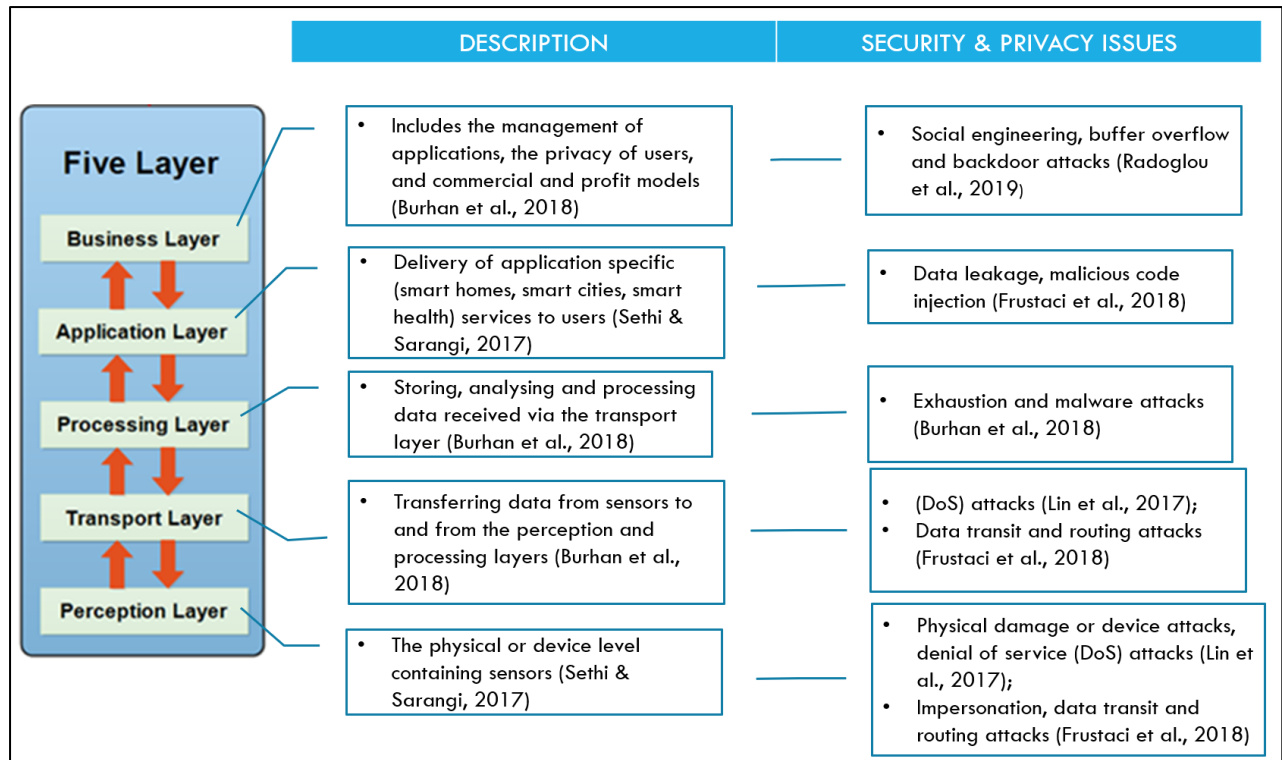


Figure 2.5: Five layer architecture with security and privacy issues adapted from (Burhan et al., 2018:10)

2.5.3.1 Perception layer

This layer contains the devices, fitted with sensors and actuators that support the collection and processing of data (Frustaci et al., 2018; Aydos et al., 2019). It provides the interconnection within the material and virtual world, and the type of sensors utilised depends on its purpose (Simha et al., 2018; Anand & Sharma, 2020). The common technologies and security vulnerabilities for data privacy for this layer are shown in Table 2.4.

Table 2.4: Common technologies and security vulnerabilities at perception layer

Term	Description
Common Technologies	
Sensor	Device that provides output based on changes in its physical environment (Rayes & Salam, 2017; Ud Din et al., 2019).
Radio Frequency Identification (RFID)	Uses radio frequency for object identification and tracking and consists of a tag containing an object's unique serial number and a reader for reading information on the tag (Virat et al., 2018; Kassab & Darabkh, 2020).
Near Field Communication (NFC)	Short-range wireless technology that connects devices through touch, simplifying transactions and digital content exchange (Muntjir et al., 2017; Kassab & Darabkh, 2020).
Actuator	Controls IoT systems through the use of data collected and analysed from sensors (Rayes & Salam, 2017; Ud Din et al., 2019).
Wireless Sensor Network (WSN)	Consists of a network of distributed nodes that operate independently, and sense and transmit status data through multiple hops (Virat et al., 2018; Kassab & Darabkh, 2020).

Bluetooth Low Energy (BLE)	Compared to other protocols, BLE has a lower energy consumption and a shorter range of communication that enables wireless networks termed, piconets; it allows for small packets of data to be transferred quickly at a rate of 1Mbps (Sethi & Sarangi, 2017).
Common Security Vulnerabilities	
Physical Attacks	The hardware components are the focus here, e.g. “node tampering” or “malicious code injection” (Lin et al., 2017; Aydos et al., 2019).
Impersonation	A fake identity is assumed by malicious nodes causing collision attacks (Frustaci et al., 2018).
DoS Attacks	The availability of IoT systems may be compromised by bombarding the network with huge amounts of traffic (Lin et al., 2017; Anand & Sharma, 2020).
Routing Attacks	“Intermediate malicious nodes (e.g., in a WSN) might modify the right routing paths during the data collection and forwarding process” (Frustaci et al., 2018:2484).
Data Transit Attacks	During data transit a number of attacks can occur on confidentiality and integrity, such as “sniffing, spoofing, sinkhole, man-in-the-middle and wormhole” (Frustaci et al., 2018; Aydos et al., 2019).

2.5.3.2 Transport layer

This layer is responsible for the secure, wired or wireless broadcast of collected data between the adjacent (perception and processing) layers as well as supporting IoT devices in connectivity and communication (Sethi & Sarangi, 2017; Virat et al., 2018; Noor & Hassan, 2019). The common technologies and security vulnerabilities for data privacy for this layer are shown in Table 2.5.

Table 2.5: Common technologies and security vulnerabilities at transport layer

Term	Description
Common Technologies	
4G-LTE	“4G is the fourth generation of broadband cellular network technology; LTE (Long-term Evolution) is a wireless broadband communication standard for mobile devices that employs orthogonal frequency-division multiplexing” (Virat et al., 2018:456).
Wi-Fi	Allows for the communication of computers and devices over a wireless signal (Muntjir et al., 2017; Singh & Mahapatra, 2020).
ZigBee	Facilitates short-term communication within a wireless network with low-energy consumption and supports star, cluster tree and mesh topologies (Lin et al., 2017; Aydos et al., 2019).
Common Security Vulnerabilities	
Routing Attacks	“Intermediate malicious nodes (e.g., in a WSN) might modify the right routing paths during the data collection and forwarding process” (Frustaci et al., 2018:2484).
Denial of Service (DoS) Attacks	The availability of IoT system may be compromised by bombarding the network with huge amounts of traffic (Lin et al., 2017; Anand & Sharma, 2020).
Data Transit Attacks	During data transit a number of attacks can occur on confidentiality and integrity, e.g. “sniffing, spoofing, sinkhole, man-in-the-middle and wormhole” (Frustaci et al., 2018:2484; Aydos et al., 2019).

2.5.3.3 Processing layer

Information received via the transport layer is collected and processed, useful data extracted, extra information discarded, thus eliminating big data issues in IoT (Burhan et al., 2018;

Gafurov & Chung, 2019). Database management technologies are utilised to store and retrieve data (Virat et al., 2018; Tewari & Gupta, 2020). The common technologies and security vulnerabilities for data privacy for this layer are shown in Table 2.6.

Table 2.6: Common technologies and security vulnerabilities at processing layer

Term	Description
Common Technologies	
Cloud Computing	Enables services that are available on demand and shareable resources with limitless storage, space and low cost computational capacity. These are beneficial for the application, service and resource management of IoT (Tewari & Gupta, 2020).
Big Data Analytics	Creates parallel execution environments and a number of servers for data distribution and improved processing speeds (Virat et al., 2018; Singh & Mahapatra, 2020).
Mobile Computing	Employed for the achievement of interoperability (Virat et al., 2018; Tewari & Gupta, 2020).
Common Security Vulnerabilities	
Exhaustion Attacks	System resources are exhausted as a result of attacks, e.g. DoS attack, thus disturbing processing within the IoT system (Burhan et al., 2018; Anand & Sharma, 2020).
Malware Attacks	Confidentiality of user data is comprised through malware, e.g. viruses, spyware, adware, Trojans and worms (Burhan et al., 2018; Gafurov & Chung, 2019).

2.5.3.4 Application layer

The various applications in which IoT has been deployed are defined at the application level (Burhan et al., 2018; Anand & Sharma, 2020). It also has the responsibility management of smart applications, as well as providing users with application-specific services (Sethi & Sarangi, 2017; Singh & Mahapatra, 2020). The common security vulnerabilities for data privacy for this layer are shown in Table 2.7.

Table 2.7: Common security vulnerabilities at application layer

Term	Description
Data Leakage	Known vulnerabilities of an application or service are exploited with the aim of stealing users' data (Frustaci et al., 2018; Amiri-Zarandi et al., 2020).
DoS Attacks	Access to applications or services are made inaccessible to legitimate users through flooding the system with redundant requests (Burhan et al., 2018; Anand & Sharma, 2020).
Malicious Code Injection	Known vulnerabilities in software applications are exploited by uploading malicious code (Frustaci et al., 2018; Aydos et al., 2019).

2.5.3.5 Business layer

The full IoT system is maintained in this layer, including user privacy, commercial and profit modules and applications (Virat et al., 2018; Singh & Mahapatra, 2020). This layer also plays a role in determining how information is created, stored and altered (Burhan et al., 2018; Singh

& Mahapatra, 2020). The common security vulnerabilities for data privacy for this layer are shown in Table 2.8.

Table 2.8: Common security vulnerabilities at business layer

Term	Description
Social Engineering	Users are coaxed into revealing confidential information or unknowingly performing malicious actions, e.g. phishing (Radoglou et al., 2019).
Buffer Overflow	Allows the attacker to exceed the data capacity within the buffer with the aim of gaining control of the system by overwriting current information to insert malicious code (ibid, 2019).
Backdoor	A software code segment that is activated by specific credentials or a sequence of events that enable an attacker to perform malicious actions (ibid, 2019).

2.5.4 Application domains for IoT

The application capacities of IoT technologies are widespread and their impact touches on all aspects of people's daily lives (Horn et al., 2019). Due to this ubiquitous nature, the National Intelligence Council of the United States (2008) listed IoT as one of six potential disruptive developments over a decade ago. It was cited that by 2025 advances and demands in technology would dictate IoT's extensive distribution, subsequently culminating in information security risks that surpass the internet. The possible applications for IoT are extensive as illustrated in Figure 2.6. In this section the researcher will provide a brief description of the applications within the industrial, smart city and health wellbeing domains.

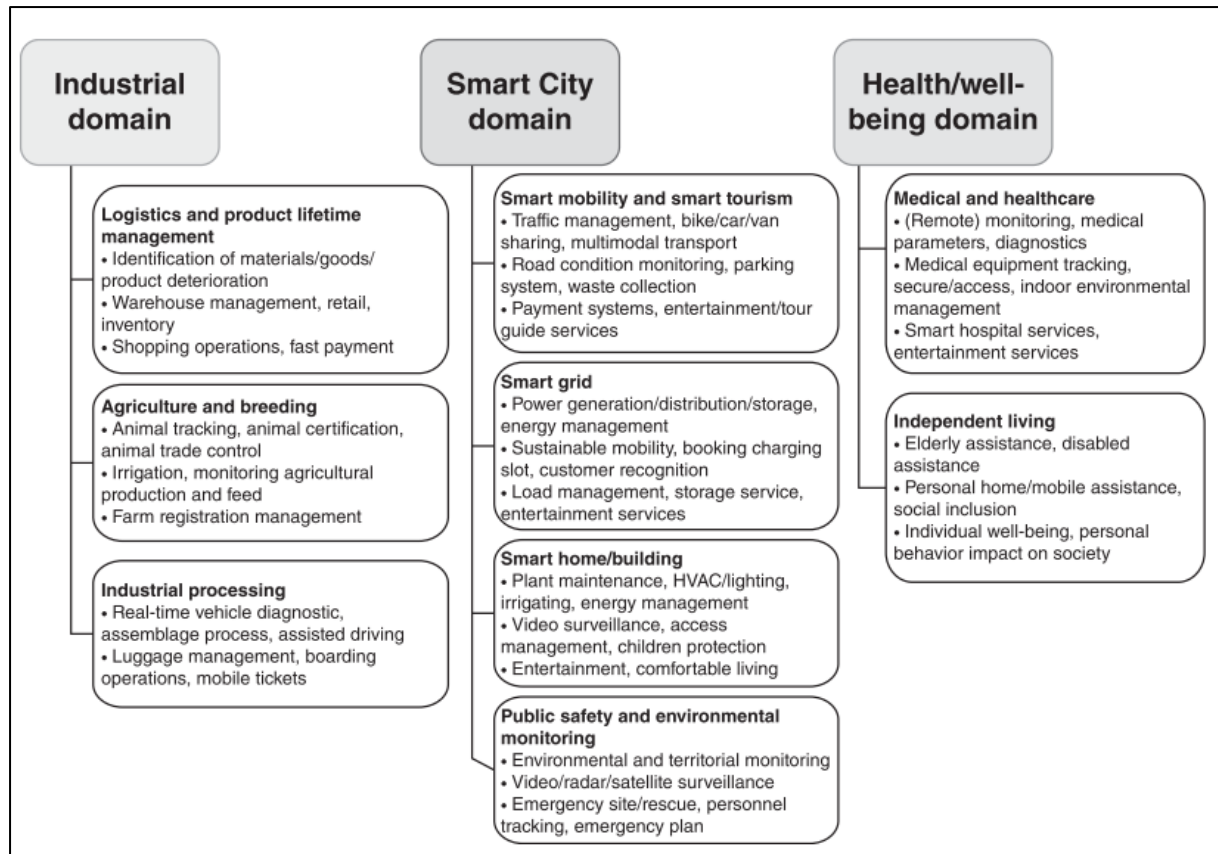


Figure 2.6: Application domains of IoT (Hassan, 2018:34)

2.5.4.1 Industrial domain

Activities related to the Industrial Internet of Things (IIoT) have become commonplace as organisations look to exploit the benefits of IoT to provide innovative service solutions that are more efficient and cost effective (Ivankova et al., 2020). This section explores the industrial domain of IoT applications, as depicted in Figure 2.5.

- **Logistics and product lifetime management:** This is when smart logistics are enabled by attaching sensors to objects and products for efficient warehouse and inventory management (Pico-Valencia et al., 2018).
- **Agriculture and breeding:** This is employed to aid higher crop production where IoT sensors can be utilised to monitor soil moisture, crop growth and irrigation as well as livestock tracking, detection and control of diseases among animals and plants (Anand & Sharma, 2020).
- **Industrial processing:** This provides improved efficiencies through automation, predictive maintenance, connected factories and mines and supply chain management (Kaur & Kaur, 2017; Priharti et al., 2020).

2.5.4.2 Smart city domain

The aim in smart city domains is the efficient use and management of public resources. Examples of the application of IoT towards achieving this goal include traffic congestion, energy consumption and smart lighting (Kassab & Darabkh, 2020). This section explores the smart city domain of IoT applications, as portrayed in Figure 2.5.

- **Smart mobility and smart tourism:** This focuses on efficient monitoring of highways, railways and waterways to provide a number of services including smart parking, aid traffic congestion alerts and instant updates to train schedules (Virat et al., 2018); based on tourists' location and preferences, a smart tourist guide can provide recommendations (Pico-Valencia et al., 2018).
- **Smart grid:** It uses distributed energy generators and smart metering to monitor and manage energy consumption to enable sustainable environments (Kassab & Darabkh, 2020).
- **Smart home or building:** This enables the monitoring and optimisation of energy consumption through smart meters. Smart homes can include connected appliances, security systems and motion sensors (Muntjir et al., 2017; Goyal et al., 2019).
- **Public safety and environmental monitoring:** It provides improved emergency services and natural disaster management. Surveillance equipment can aid public order and safety, and monitoring of the structural integrity of buildings (Kassab & Darabkh, 2020).

2.5.4.3 Health wellbeing domain

For the past two years, the world has been in the grip of the COVID-19 pandemic, a respiratory disease spread through contact with others (World Health Organisation, 2021). Minimal contact with patients was made possible by the medical applications of IoT via the remote monitoring of patients by medical professionals (Haghi Kashani et al., 2021). This section explores the health and wellbeing domain of IoT applications, as shown in Figure 2.5.

- **Medical and healthcare:** It refers to the monitoring and analysis of users' health data, such as blood pressure, diabetes and heart rate; patients and medical personnel can monitor medication intake and allergic reactions (Khanna & Kaur, 2020; Goyal et al., 2019).
- **Independent living:** This pertains to assisted living solutions which include remote monitoring of bodily functions and activities of individuals and rapid response if required (Horn et al., 2019).

2.5.5 Data privacy and governance in IoT

The Internet of Things (IoT) presents novel methods of data collection, thus leading to complex data privacy challenges, such as consent, user control, customisation and choice in what data

to share as well as data use limited to the purposes stated (Naeini et al., 2017; Anand & Sharma, 2020). The governance of data privacy in an organisation should be closely linked to its privacy policy and should set out guidelines for the processing and protection of personal data (Swartz et al., 2019). In addition to that, the requirements for data privacy in IoT include the essential three security components, namely “privacy, integrity and accessibility” (Aydos et al., 2019:10).

According to Patra et al. (2018) IoT governance should address the following aspects: deciding on the correct sensor or device to collect data; network transportation and storage of data to the cloud; data analysis to predict and optimise outcomes; data distribution to other applications and consumers; data privacy and security management. Dasgupta et al. (2019:211) claim that IoT governance can be seen as supplementary to IT governance which is concerned with managing IT resources, where the “lifecycle of IoT devices, data managed by IoT solutions and IoT applications” are the focus of IoT governance. Morar et al. (2021) contend that although the term, *IoT governance* is relatively new and requirements still lack clarity, the challenges for IoT governance include data governance, privacy rights and security.

2.6 Protection of personal information regulation and policies

The individual’s data have been a hot commodity for many organisations, with companies like Google and Facebook building their business models on collecting clients’ data and being accused of using it unscrupulously (Gruschka et al., 2019). However, in recent years countries have attempted to address privacy concerns through the promulgation of data privacy laws, necessitated by the proliferation of technological advances that aid the aggressive collection and indiscriminate use of personal data (Rudo & Reagan, 2021). Predominantly, these data privacy laws intend to regulate the collection of information, notification to data subjects and data subjects’ control over their information as well as stipulate consequences for non-compliance (Carson, 2021). According to Alginahi and Kabir (2019) the proper use of data balanced by the privacy rights of individuals can be determined as the objective of data protection regulations. However, Andrew and Baker (2021:568) argue that the use of “de-identifying techniques” such as anonymisation, as specified within various regulatory policies, can have implications on the use of “de-identified data” to “monitor and predict” user behaviours.

The implementation of the EU's GDPR in 2018 can be seen as the catalyst for global regulatory efforts towards protecting the personal information of individuals (Reinwarth, 2019). An internet search revealed a total of twenty-five countries with updated information protection regulation between 2018–2021 as illustrated by Figure 2.7. The countries are grouped under

the following regions: Europe, North America, Asia-Pacific, Central and South America, the Caribbean, the Middle-East and Africa. The subsequent document analysis of the updated regulations can be found in Chapter Four.

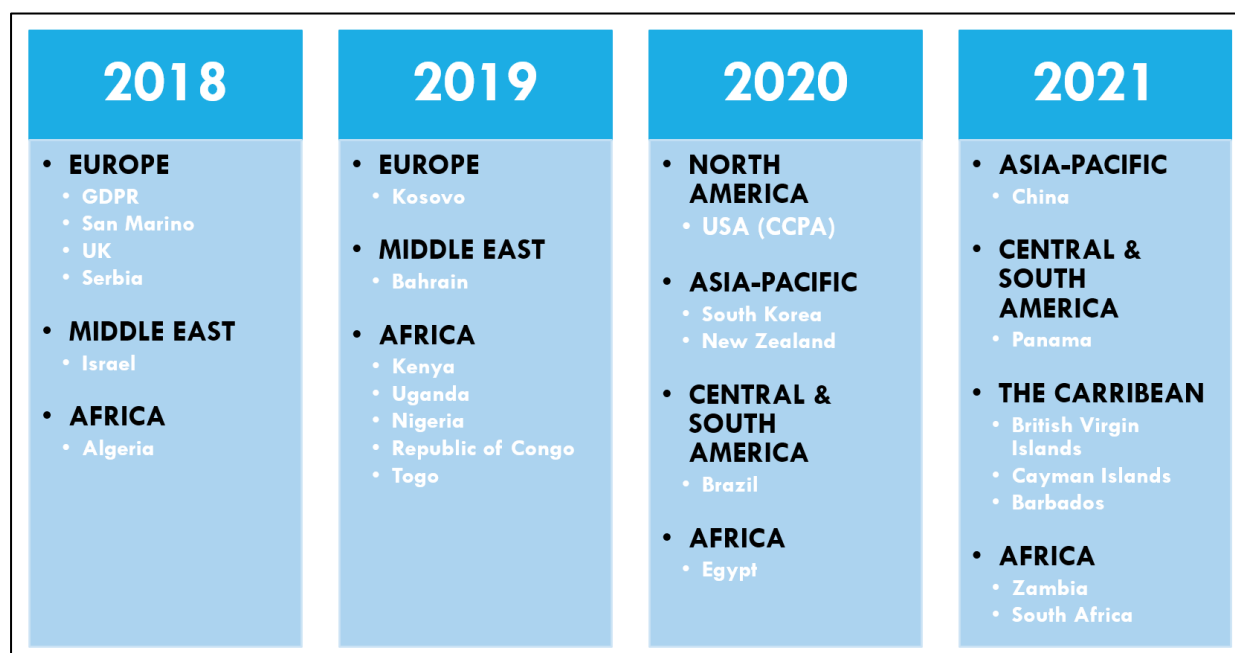


Figure 2.7: Countries with updated privacy regulations (2018–2021)

Since the implementation of GDPR three years ago, there have been notable penalties imposed on companies who are not compliant. These include: Google (€50m/£43.2m), H&M (€35.3m/£32.1m), Tim - Telecom Italia (€27.8m/£24m), British Airways (£20m) and £18.4m for Marriott International Hotels (BBC, 2021). Figure 2.8 shows the biggest breaches and settlements worldwide, as from August 2020 (Statista Research Department, 2021a).

South Africa's penalties for non-compliance equals fines of up to R10 million and a possible twelve months or ten years imprisonment (Kandeh et al., 2018). However, in an interview with the Daily Maverick, the Information Regulation admitted to being swamped by the recent number of breaches due to a lack of resources and budget (Mahlaka, 2020). Since the implementation of the POPI Act in July 2021 there has been no visible enforcement of penalties on the part of the Information Regulator. According to Jacobs (2021), the Information Regulator threatened WhatsApp with legal action in May 2021 following updates to the company's privacy policy. However, in June 2021 the Information Regulator postponed the implementation of the clause that pertains to the processing of unique identifiers (without the permission of the regulator) which includes mobile numbers to February 2022 (Business

Insider SA, 2021). In so doing, WhatsApp is free to process the mobile numbers of South Africans for another six months.

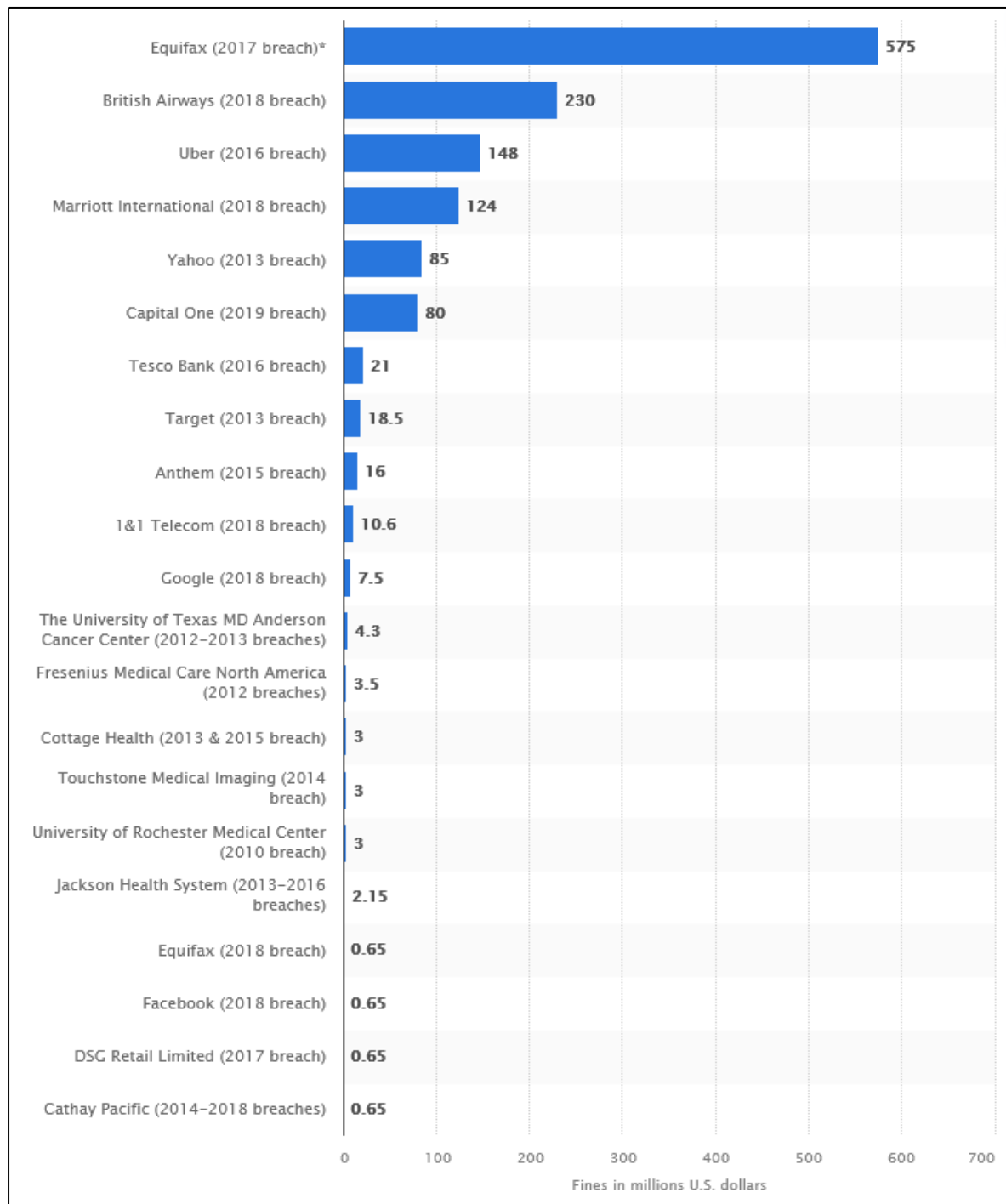


Figure 2.8: Biggest data breach fines and settlements worldwide (Statista Research Department, 2021a)

2.7 Related work

Advancements in technology have sparked numerous research articles with proposed approaches, guidelines and frameworks for managing concerns related to the security of IoT

services and devices. However, frameworks addressing IoT applications' privacy issues are lacking (Thorburn et al., 2019).

A selection of privacy frameworks are discussed below and summarised in Table 2.9:

Following a review of six privacy frameworks, Thinakaran et al. (2017) proposed a conceptual privacy framework presenting fundamental principles for the development of health applications within IoT that are cognisant of privacy. The proposed framework was developed based on the extraction of common principles, combining relevant principles and removing unrelated requirements. The 4I (Identify, Insulate, Inspect and Improve) Framework was developed by Dasgupta et al. (2019), following a study of academic literature of numerous existing data governance frameworks. The proposed framework aims to support data stewards in managing and defining guidelines, rules and data assets for the delivery of enterprise-wide data governance and quality for digital Information Systems environments within IoT.

In the context of South Africa, the researcher found three research articles in relation to proposed privacy frameworks or guidelines which are discussed below:

Subsequent to the analysis of existing IoT (five layer architecture) and cyber-physical systems (CPS) reference architectures (CPS 5C architecture and the solutions layer architecture) Baloyi and Kotzé (2018), propose a merged architecture for data privacy within these domains. By combining the proposed architecture with The Zachman Framework for Enterprise Architecture, the researchers proposition a model for data privacy focussing on the technological and organisational characteristics for compliance with the POPI Act. A conceptual privacy governance framework has been proposed by Swartz et al., (2019:2). Through the comparison of four existing privacy governance frameworks ("Information and Privacy Commission of New South Wales: Privacy Governance Framework" (IPC); "Common Privacy Framework of the Information Privacy Commissioner of Ontario – CCIM Assessment Projects"; "Privacy Management Program – The Office of the Privacy Commissioner of Canada" (OIPC); and "The Office of the Australian Information Commissioner (OAIC) – Privacy Management Framework"), the researchers have incorporated an inclusive set of privacy components to facilitate the management of privacy governance within organisations. A list of privacy compliance guidelines is proposed by Baloyi and Kotzé (2019), for the purpose of aiding organisations in complying with privacy legislation within CPS and IoT environments. The legal (based on South Africa's POPI Act), technical and organisational aspects of data privacy compliance were considered by the study to provide organisations with further direction for data privacy compliance research.

Table 2.9: Summary of related work

Authors	Paper Title	Purpose	Country	Environment	Approach / Methodology	Limitations in Comparison to this Study
Thinakaran, Dhillon, Gunasekaran & Chen (2017)	A Conceptual Privacy Framework for Privacy-Aware IoT Health Applications	To propose a framework that models the privacy requirements for IoT health applications.	Malaysia	IoT-based health applications	Literature review	Specifically aimed at IoT health applications and therefore, does not provide a holistic framework for IoT.
Dasgupta, Gill & Hussain (2019)	A Conceptual Framework for Data Governance in IoT-enabled Digital IS Ecosystems	To address the data governance challenges in IoT and proposes the development and evaluation of the 4I (Identify, Insulate, Inspect & Improve) framework.	Australia	Healthcare Industry	Design Science Research (followed DSR activities: awareness, suggestion, development, evaluation and conclusion)	The case study was aimed solely at the health sector and therefore the proposed framework cannot be termed as holistic.
Baloyi & Kotzé (2018)	A Data Privacy Model Based on Internet of Things and Cyber-physical Systems Reference Architectures	To propose a privacy model, including both organisational and technological viewpoints, that can serve as a reference model for data privacy in IoT and CPS.	South Africa	IoT and Cyber-physical Systems (CPS)	Literature review	The proposed model called IoT and CPS Architecture-based Model for Data Privacy (ICAMP) was aimed specifically at IT professionals.
Swartz, Da Veiga & Martins (2019)	A conceptual privacy governance framework	To develop a conceptual privacy governance framework to govern the implementation of privacy requirements and laws, such as POPIA in organisations.	South Africa	Focused on organisations in general	Literature review	The framework proposed is conceptual and untested, as well as not intended for IoT.
Baloyi & Kotzé (2019)	Guidelines for Data Privacy Compliance: A Focus on Cyber-physical Systems and Internet of Things	To propose a list of data privacy compliance guidelines.	South Africa	IoT and CPS	Design Science Research (followed DSR activities: awareness, suggestion, development, evaluation and conclusion)	The guidelines provided require further testing and refinement of the non-technical aspects of privacy compliance within an organisation.

All of the above-mentioned research articles proposed frameworks based on the analysis of existing frameworks and architectures. The contribution to the body of knowledge is undeniable, however there are certain limitations when compared to the aims and objectives of this study, as expanded below.

The framework proposed by Thinakaran et al. (2017) was specifically aimed at IoT-based health applications and therefore, does not provide a holistic framework for IoT. Although, Dasgupta et al. (2019) claim that the framework proposed is a holistic framework, the case study was aimed solely at the health sector and therefore cannot be termed as holistic. Baloyi and Kotzé (2018) proposed an untested model, called the IoT and CPS Architecture-based Model for Data Privacy (ICAMP), aimed specifically at IT professionals only. The framework proposed by Swartz et al. (2019) is conceptual in nature and untested by the researchers, as well as not intended for IoT or IoT environments. Baloyi and Kotzé (2019) provided IT professionals with guidelines within the IoT and CPS fields to aid data privacy compliance in transmission which left out the aspects of regulation, and user informed consent. Although extensive, the guidelines provided require further testing and refinement of the non-technical aspects of privacy compliance within an organisation. Nonetheless, the guidelines developed from the study were based on the POPI Act which came into effect on 1st of July 2021. This presents a serious challenge, considering limitations of the Act to deal with the ever-growing interconnected society currently experienced in South Africa

This study will firstly explore the factors affecting data privacy governance within IoT environments in South Africa and secondly develop a holistic framework for governing data privacy use within IoT environments in South Africa based on the basic requirements for the preservation of privacy, namely the user's informed consent, relevance to the purpose of use, specification of purpose, usage limitations, transparency, notification and correction or deletion of data, and accountability. A major point of departure of this study from the aforementioned research efforts will be the utilisation of the components of activity theory discussed in the next section, while incorporating global best practices and the basic requirements for the preservation of privacy.

2.8 Activity Theory

Activity theory has its origins in Russian psychology and stems from the early works of Vygotsky and Leontiev [Leont'ev] (Kaptelinin & Nardi, 2006). Through the examination of activities in the context of an individual's daily circumstances, activity theory seeks to understand humans through their interactions (Jonassen & Ronrer-Murphy, 1999). Researchers, Allen et al. (2011:784) highlight are provided with greater understanding of the

context of an activity system by inspecting “rules and norms, tools, community, and division of labour”. Furthermore, Hasan and Kazlauskas (2014) emphasise that activity theory provides a framework for sense-making of discoveries through observation or interviews in studies related to modern organisations, education and communities. Vakkayil (2010) argue that the advantages of activity theory as an analytical lens is tremendous, however questions have been raised in its use as a theoretical framework. According to Jonassen and Ronrer-Murphy (1999), the activity theory is less of a predictive theory and recognized as a more robust and clarifying explanatory tool.

Activity Theory, Nathanael et al. (2002:140) assert relies on the idea of “contradiction” and the focus is on continual development of the activity system which is in contrast with systematic approaches. In addition, claims have been made that the individual subject and collective activity relationship in activity theory is vague (Vakkayil, 2010). Based on the work of Blunden (2009), four limitations of activity theory are highlighted by Khayyat (2016):

- activity theory models lack the motivational catalyst for individuals to achieve the object
- the absence of any acknowledgement of difficulties individuals may face when conducting an activity
- there is a need for the clarification of the term *object*
- the unclear relationships and contradictions of components

Nevertheless, academics have used activity theory in a variety of disciplines such as education, healthcare, psychology and information systems to support qualitative and interpretative research (Hashim & Jones, 2007). The application of activity theory in information systems was originally presented at a conference in Copenhagen in 1991 (Mursu et al., 2007). Subsequently, studies in Information Systems and Human Computer Interaction emerged as the practical application of activity theory in the field became evident (Kuutti, 1995; Hashim & Jones, 2007; Allen et al., 2011).

2.8.1 Overview of activity theory

Activity theory, Mavrommati et al.(2013:73) states: “puts emphasis on social factors as shapers of interaction between agents and their environments”. According to Allen et al. (2011) the notion of activity was introduced by Leontiev who made a distinction between action and the collective activity by proposing that the subject initiates an action, based on a need (the motive) to achieve an object (the goal) through the implementation of tools (the means). Hence a need is satisfied by activities which in turn comprise of actions. Vygotsky and Leontiev represented two of the three theoretical generations of Cultural Historical Activity Theory (CHAT) as summarized by Daniels and Guitierrez (2009).

The third theoretical generation of Activity Theory (also referred to as the General Activity Theory or Scandinavian Activity Theory) extends the first two and is based on the work of Engeström (Roos, 2012). Engeström further developed the ideas of Leontiev with the inclusion of aspects pertaining to “community, the division of labour and rules/norms” as illustrated by Figure 2.9 (Allen et al., 2011:781). Furthermore, Activity Theory allows for the existence of a network of activity systems in which components of an activity may be used or may have a bearing on other activities (Mursu et al., 2007).

This research utilised the third generation of Activity Theory as a lens to analyse the interactions and data patterns of the study.

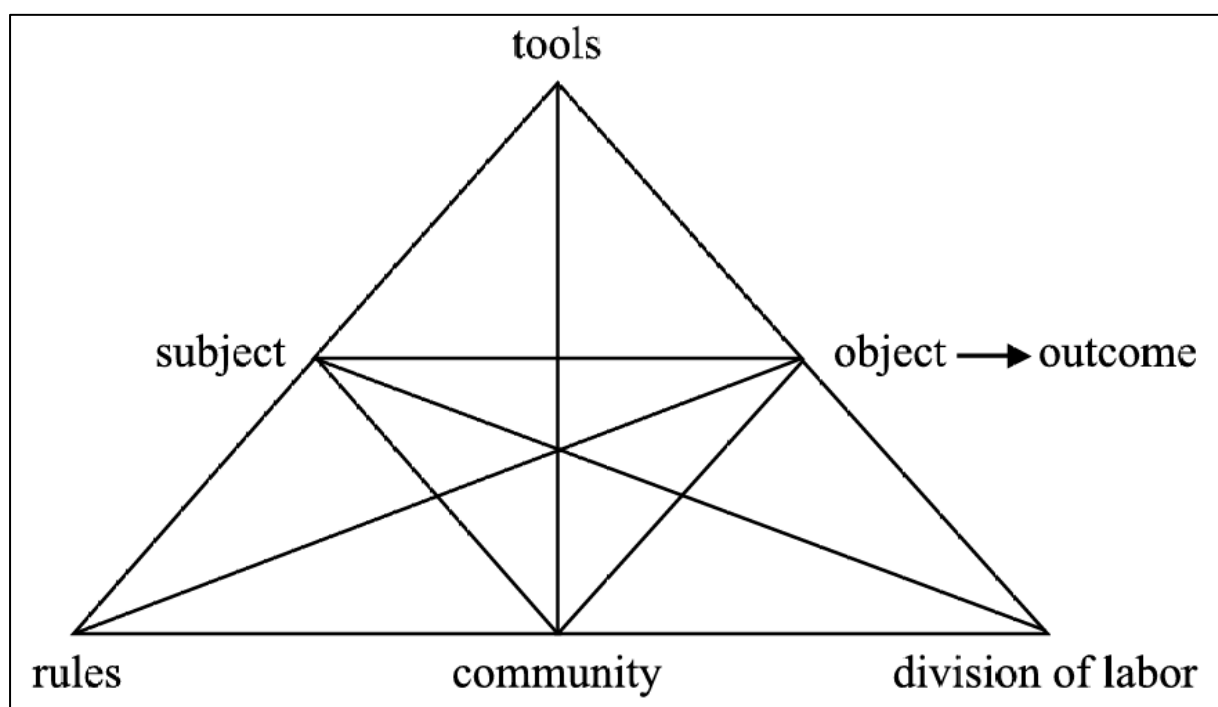


Figure 2.9: The activity system, adapted from Engeström, (1987), cited in Allen et al., (2011:781)

2.8.2 The activity system

Engeström's activity system shifted the focus from the “subject-object relationship” to a model that depicted an activity as a “collective phenomenon” (Nardi et al., 2006:99). According to Kuutti (1995:14) in the updated model from Engeström there are three mutual relationships between the “subject, object and community”, each mediated by a different component as follows.

- i. Tools mediate the subject and object relationship.
- ii. Rules and norms mediate the subject and community relationship.
- iii. The division of labour mediates the object and community relationship.

Therefore, an activity system, as depicted in Figure 2.8, comprises of the tools, the subject, the rules, the community, the division of labour and the object (Allen et al., 2011). A brief description of each component is presented next as well as their context in relation to the study in Table 2.10.

Table 2.10: Components of an activity system, description and context

Components	Description	Context of the Study
Tools	a variety of tools or artefacts are contained within an activity in a mediating role (Kuutti, 1995).	Smart devices, applications and IoT environments, Security measures and protocols, Regulatory compliance measures
Subject	the source of activity is always the subject and its interaction within the world (Roos, 2012).	Users of smart devices, applications and IoT environments, Responsible parties and operators (aka data controllers and processors), Information officers, Information Regulator
Rules	norms and rules that govern subjects' activity within a community (Allen et al., 2011).	Data Privacy / Protection Regulation, Compliance Contracts / Agreements
Community	involves subjects performing their activities, individually or in groups and their interactions with other subjects who utilise a similar object (Kuutti, 1995).	Users of smart devices, applications and IoT environments, Responsible parties and operators (aka data controllers and processors), Information Regulator
Division of Labour	represents the administration of a community, i.e. the roles and responsibilities of the subjects (Kuutti, 1995).	Roles and responsibilities of the subjects within the community
Object	an object can be material in nature or less physical, for instance a plan or an idea (Kuutti, 1995).	The establishment of guidelines and best practices for the governance data privacy within IoT environments in South
Outcome	involves the transformation of the object based on activities of the subject (Kuutti, 1995).	The effective governance of data privacy within IoT environments in South Africa

The Activity Theory has proved useful in developing research instruments as a data analysis framework as well as understanding use and usability issues that affect systems, and the comprehension of user behaviour (Roos, 2012).

2.9 Summary

This chapter provided a review of the literature in relation to the research problem. Firstly, the chapter reviewed the concept of privacy from the perspective of academia and law. It also covered the preferred nomenclature for the protection of personal information, namely, *data privacy* or *data protection* and the employment of the term based on regulation, industry and academic literature.

Secondly, technological advances, such as social media, big data, mobile devices, cloud computing and IoT and their impact on the privacy of individuals were discussed comprehensively. The different aspects of IoT were then explored, including the architecture, application domains, the challenges, the common technologies and security vulnerabilities at the different layers of the five-layer architecture as well as data governance in IoT. The

regulations and policies in relation to the protection of personal information were also reviewed.

The chapter concluded with a discussion on the role of Activity Theory as an underpinning theory to study and analyse the interactions and data patterns from the study as it relates to the activities of data governance in IoT environment in South Africa.

CHAPTER THREE: RESEARCH METHODOLOGY

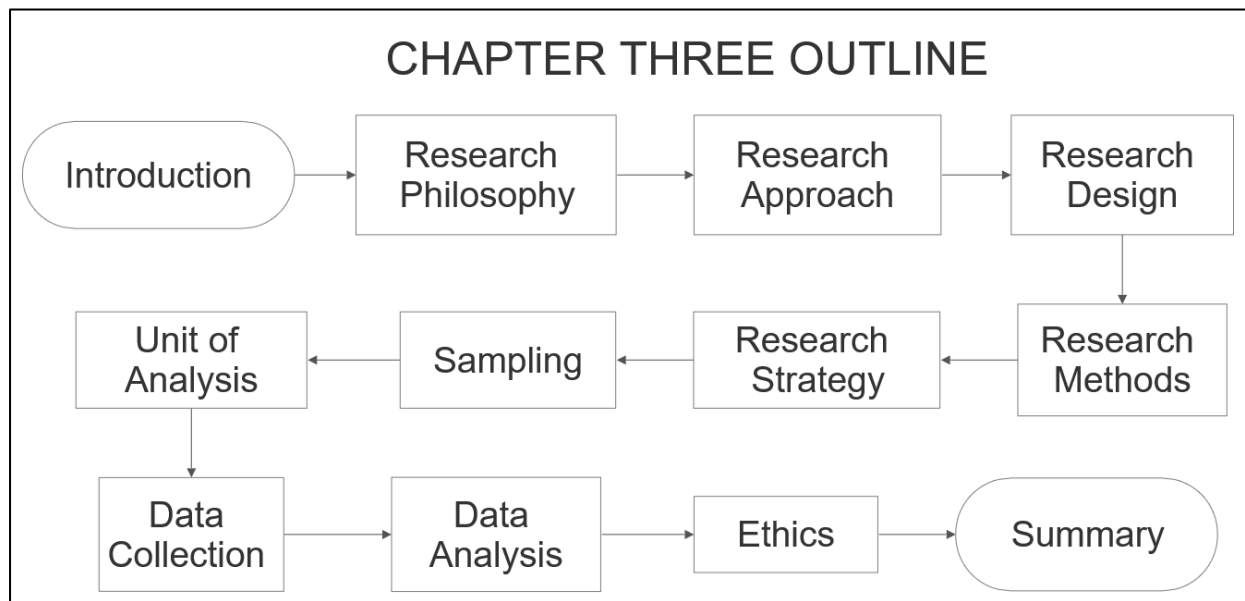


Figure 3.1: Chapter Three outline

3.1 Introduction

Research has become a common practice in people's everyday existence. Whether it is for business (a new product or service) or personal choices (a new home or car), it requires the collection of information for the purpose of decision-making (Wang & Park, 2016). Humans possess a natural inquisitive instinct, therefore the desire for knowledge and the techniques for acquiring information can be regarded as research (Kothari, 2004). However, a formal approach to academic or social research requires a systematic process, encompassing identification of a problem, hypothesis formulation, information gathering, evidence evaluation, drawing conclusions and presentation of findings, ultimately adding to the body of knowledge (Kothari, 2004; Saunders et al., 2009). Furthermore, the classification of research requires that the process be “controlled, rigorous, systematic, valid and verifiable, empirical and critical” (Kumar, 2011:28; Mligo, 2016:17).

The use of methodology in research applies to how a phenomenon can be scientifically and systematically investigated. In other words, it outlines the structure within which to conduct research (Kothari, 2004; Holden & Lynch, 2006; Saunders et al., 2009). Methodology and methods are often used interchangeably, but a clear distinction can be drawn. The framework for the research is underpinned by the methodology, whereas the means for collecting and analysing data are provided by the methods (Hammond & Wellington, 2013). There are various methods available for conducting research which are discussed in detail further in this chapter.

The fundamental elements of the research process and their correlation with the research aim and objectives are discussed in relation to the research phenomenon. These core components are divided into sections which consist of the underpinning research philosophy, research approach, adopted research design, research strategy employed, the applied sampling technique and the corresponding unit of analysis, the process of data collection and complementary analysis, and in conclusion, the ethical principles and guidelines followed in the course of the study are discussed.

3.2 Research Philosophy

The choice of research, methodology and methods employed in a pursuit of knowledge or an explanation to a conundrum is influenced by the researcher's beliefs and presuppositions about the world (Grix, 2001; Saunders et al., 2019). It has been argued that the lexicon of social science lacks uniformity and precision, resulting in nomenclatures either being misunderstood or misused in conducting research (Grix, 2002). Research philosophies, according to Saunders et al. (2019:133), can be categorised into three types of assumptions, namely ontology ("nature of reality"), epistemology ("what constitutes acceptable, valid and legitimate knowledge") and axiology ("the role of values and ethics"). The relationship between the researcher's beliefs and philosophy influences the research design as shown in Figure 3.2.

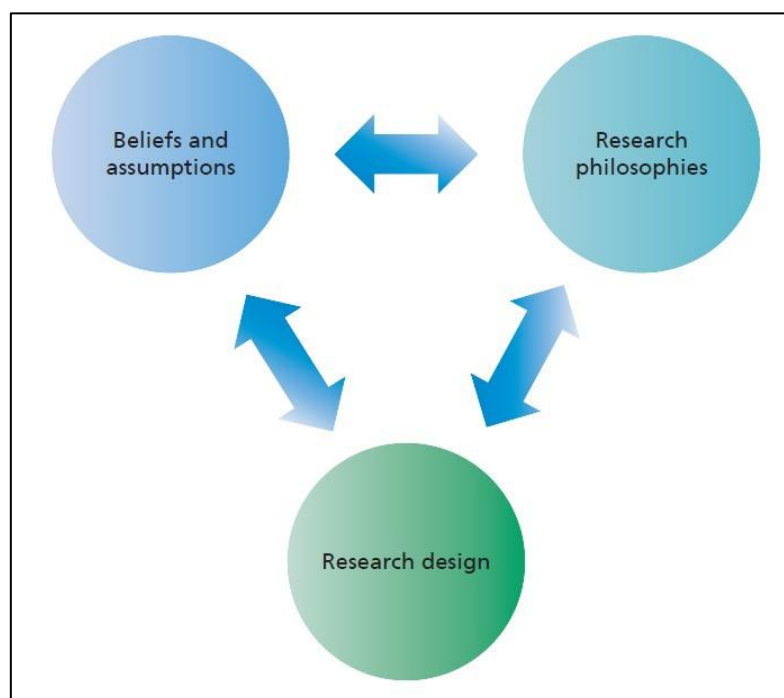


Figure 3.2: Influence of researcher's beliefs and assumptions on research design (Saunders et al., 2019:132)

Hammond and Wellington (2013) argue that philosophical considerations in research are often neglected, observing that the researchers are simply adopting either a method or methodology, without due consideration to the influence of belief system on the research. To demonstrate the validity of the research methodology, a thorough understanding of ontological and epistemological suppositions are critical for defending philosophical choices in relation to the adopted process (Saunders et al., 2009).

The ontological and epistemological positions, in relation to the research aim and objectives, are further expanded in the following section.

3.2.1 Ontological considerations

Ontology concerns an individual's belief of what embodies social reality or fact, that is, the "nature of reality" (Grix, 2001:26; Saunders et al., 2009:110). Questions of an ontological nature, described by Marsh and Furlong (2002:18), pertain to "whether there is a real world out there that is independent of our knowledge of it". Therefore, a researcher's ontological assumptions influence the way in which they view the world and underpin their approach to research (Grix, 2001; Saunders et al., 2019). These presuppositions pertain to whether social actors are independent (objective) or influential (subjective) on perceived fact of reality (Saunders et al., 2009; Bryman, 2012).

3.2.1.1 Objectivism and subjectivism

Bryman (2012:33) defines objectivism as: "an ontological position that asserts that social phenomena and their meanings have an existence that is independent of social actors". Thus, human knowledge and values are not created by the ideas or feelings an individual (social actor) has, but are rather determined by those which are perceived as reality by collective measure (Saunders et al., 2019). In terms of research, objectivist positions are impartial and detached from the subject matter and their beliefs, while values and interests have no bearing on the choice of research methods employed (Holden & Lynch, 2006).

The contrast to the before-mentioned ontological position is subjectivism which Saunders et al. (2009:110) describe as: "social phenomena created from the perceptions and consequent actions of those social actors concerned with their existence". Researchers with a subjectivist persuasion, according to Holden and Lynch (2006:10), are unable to remain completely impartial and unbiased from "what is being observed, the study's subject matter or the methods of the study". Subjectivism is dynamic, as it involves the construction of reality through a different lens of social interactions which tend to vary from one reality to another based on experience, views and beliefs (Orlikowski & Baroudi, 1991). With regard to this study, a

subjectivist ontological stance was taken to explore the subject matter based on the participants' points of view and experience of the phenomenon of the study.

3.2.2 Epistemological considerations

Epistemology is closely linked to ontology and relates to the theory or nature of knowledge and the individual's belief of how one gains knowledge and understanding about the world (Grix, 2001). For instance, Bhattacharjee (2012) states that if the researcher's view of knowledge is static, objective and tangible, the methods utilised require an alignment with natural science. While on the other hand, if knowledge is perceived as personal, subjective and unique, natural science methods are rejected and the researcher would thus have greater interaction and involvement with the research subjects (ibid, 2012). Additionally, epistemology entails a consideration for what represents "acceptable, valid and legitimate knowledge" and the communication of this knowledge (Bryman, 2012:27).

In the following sub-section, the four major epistemological paradigms, namely positivism, realism, interpretivism and pragmatism are discussed and the applicability of the adopted epistemological position to the research is articulated.

3.2.2.1 Positivism

In the mid-19th century, Auguste Comtè argued that humankind was influenced by "cause and effect" which could be demonstrated through empirical observations and simulating the tenets of natural sciences (Howell, 2013a:39). Subsequently, positivism emerged which prescribes that research related to social reality should employ the procedures recognised in natural sciences (Bryman, 2012). Positivism has been dominant in social science since 1945, with the foremost positivist fields being experimental psychology and economics (Neuman, 2014).

Positivists believe that social reality can be objectively observed and interpreted, encouraging "unambiguous and accurate knowledge" (Saunders et al., 2019:144). Hence, a hypothesis can be substantiated or refuted through empirical data *sans* bias or prejudice from the researcher or observer (Harrison, 2014). Researchers who take a positivist stance will have a preference for quantitative (numerical) data, most likely obtained through surveys or experiments, for analysis and verification of causal hypotheses, laws and facts (Cullen et al., 2012; Howell, 2013a). Thus, positivists adhere to an objective ontological position and are concerned with identifying causal relationships between and explanations of social phenomena (Marsh & Furlong, 2002; Holden & Lynch, 2006). The positivist paradigm does not provide a fit for this study, since the research aim and objectives do not support the use of methods associated with the paradigm.

The exploratory nature of this study sought to comprehend the factors affecting the governance of data privacy in South African organisations. Consequently, the employment of quantifiable and measurable methods for studying of the phenomenon are not suitable.

3.2.2.2 Realism

The fundamental nature of realism indicates that the truth of reality is portrayed by our senses, that is, the existence of objects can be regarded independently of the human mind (Saunders et al., 2009). In other words, the world is comprised of “hard, tangible, and relatively immutable structures” (Kuada, 2012:73). Similarly to positivism, the development of knowledge in realism is based on a scientific approach which supports the collection and explanation of data (Bryman, 2012). However, contrary to the positivist stance, realists believe that not every social occurrence and their relationships are capable of being observed (Marsh & Furlong, 2002). Realism thus offers an alternative approach to understanding reality and offers a different position that neither supports nor rejects the positivist paradigm (Williams et al., 2017). Realism is expressed in two main forms, empirical and critical realism, as discussed below.

3.2.2.2.1 Empirical realism

Empirical realism maintains that “objects, events and regularities” do not have “structure or powers”, and specifically “no unobservable qualities” (Sayer, 2000:11). The empirical realist assumes the existence of a close to perfect correspondence “between reality and the term used to describe it”. In other words, the world is accurately portrayed by what people encounter through their senses (Moon & Blackman, 2014:1170; Saunders et al., 2019). According to Bryman (2012) empirical realism contends that reality can be understood by applying the appropriate methods and is often referred to as naive realism. The opposing view to the aforementioned stance is critical realism which is discussed in the next section.

3.2.2.2.2 Critical realism

Critical realism is focussed on the explanation of what people discern visually and experience, in relation to the constructs of the individual’s notion of reality of a discernible occurrence (Saunders et al., 2019). Although the existence of a single reality is assumed by the critical realist, Moon and Blackman (2014:1170) contend that this single reality cannot be fully comprehended due to human intellect being flawed as well as the unmanageable “nature of phenomena”. Additionally, Howell (2013:51) asserts that there is a differentiation between the knowledge produced by individuals, for example, theories (“transitive objects of knowledge”), which are changeable and knowledge discovered of things that are independent of human action, such as gravity (“intransitive objects of knowledge”). Moreover, in relation to science,

transitive objects continuously evolve to deepen knowledge about reality or the world they pertain to, that is “the intransitive object” (Danermark et al., 2002:23).

For instance, the theory of the earth being flat has switched to the hypothesis of the earth being round, nevertheless it does not automatically imply that the shape of the earth has changed with the revision of the theory (Sayer, 2000). Therefore, critical realism positions that scientific theories are open to modification and reconstruction due to the conditional characteristics of phenomena descriptions and explanations (Reed, 2005). With regard to the social world or social science, it is more complicated, as social constructs have knowledge of themselves and therefore do not exist totally independent of human activity, since such “an intransitive dimension of knowledge” cannot be clearly illustrated (Howell, 2013:51). However, Sayer (2000) cautions that the acquired knowledge would most likely not be projected by present day researchers, but rather as an historical or past knowledge.

In addition to that, critical realism subscribes to a “stratified ontology”, as displayed in Figure 3.3 and further defines and distinguishes between “the real, the actual and the empirical” (Saunders et al., 2019:147).

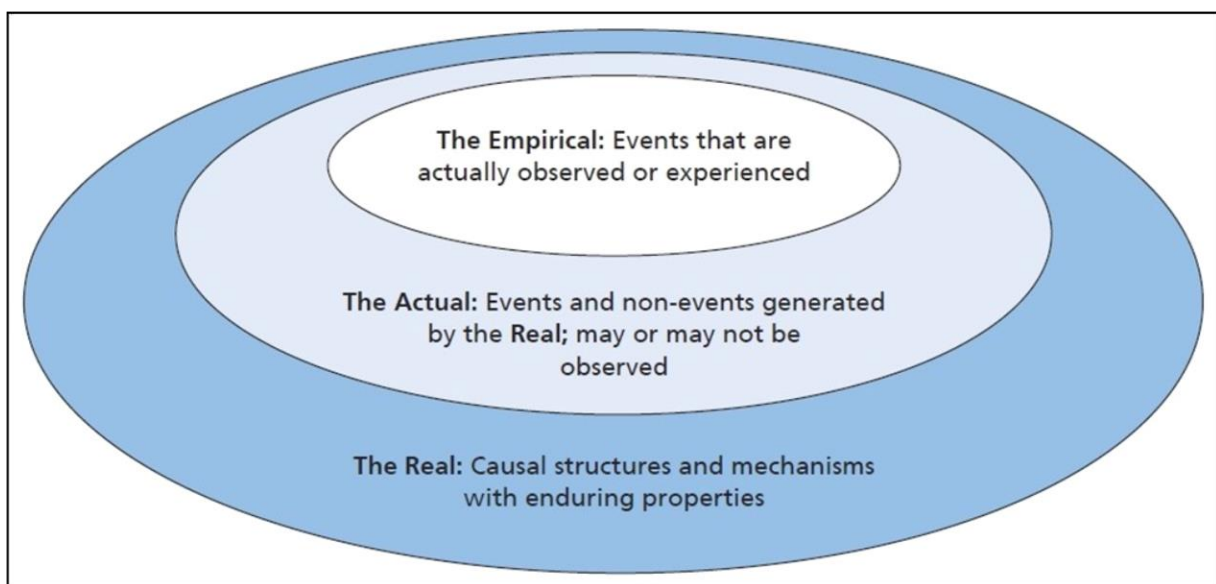


Figure 3.3: Critical realist stratified ontology (Saunders et al., 2019:148)

Hence, critical realism concludes that empirical events are produced by “underlying structures and mechanisms” that are indirectly perceived or sensed, and processed through “retroductive reasoning” to identify the causal constructs of phenomena (Reed, 2005:1630; Bryman, 2012:29; Saunders et al., 2019).

In relation to this study, neither empirical nor critical realism were applicable as the study sought to explore the subjective and practical meanings participants employed to describe their individualistic experience and knowledge of the phenomenon. Thus, they were not merely observing the theoretical construction of the phenomenon or explaining the underlying causal mechanisms.

3.2.2.3 Pragmatism

Saunders et al. (2019) claim that researchers who question the relevance of the above-mentioned ontological and epistemological philosophies would in all probability have an inclination towards pragmatism. The concept of pragmatism as a research paradigm originated from the intellectual labours of US philosophers “Charles Pierce, William James and John Dewey” (Saunders et al., 2019:151). Pragmatism contends that antecedent notions should not have direct bearing on the knowledge of the meaning of a concept. However, a requirement exists to consider its practical implications (ibid, 2013). In efforts towards understanding of phenomena, pragmatists focus on research problems rather than methods and employ all available techniques in the pursuit of practical outcomes (Creswell, 2014; Saunders et al., 2019).

According to Kuada (2012) the pragmatic researcher views some tasks objectively or subjectively, or as a combination, if they will lead to a tangible and applicable contribution. Consequently, the often rigid differentiation between the application of qualitative and quantitative methods are disregarded, thereby challenging the view that methods utilised should be dictated by assumptions linked to a specific paradigm (Creswell et al., 2003; Saunders et al., 2009; Hammond & Wellington, 2013; Creswell, 2014; Klenke, 2016).

This study aims to explore the subjective and practical meanings participants employed to describe their individualistic experience and knowledge of the phenomenon.

3.2.2.4 Interpretivism

Scholars in early-twentieth-century Europe argued that social sciences research, owing to the divergent nature in which humans generate and experience social realities, ought to be conducted differently from research in natural sciences, thereby leading to the emergence of interpretivism (Bryman, 2012; Saunders et al., 2019). Offering an alternative to the positivist stance, interpretivism postulates that research “must be observed from subjective reasoning through the direct experience of people”, rather than “objectively observed” (Mack, 2010:8). As a result, the interpretivist researcher embraces a subjectivist position and acknowledges

that their own beliefs and principles will have a bearing on the research process (Klein & Myers, 1999; Moon & Blackman, 2014; Saunders et al., 2019).

Influences on interpretivism include hermeneutics, phenomenology and symbolic interactionism which embody drawing knowledge from interpretations of observed experiences of social constructs (Crotty, 1998, cited in Saunders et al., 2019; Blaxter et al., 2010; Bhattacharjee, 2012).

Hermeneutics, according to Bhattacharjee (2012:117), "is the study of interpretation and the theory and practice of interpretation". Imported into social sciences from theological studies, it is often applied to the interpretation of "text, symbols, stories, images" and human behaviour (Saunders et al., 2019:149). Therefore, interpretations of a subjective nature are the focus of a hermeneutic approach, aiming to highlight the meanings of data from the originator's perspective as well as from the context in which the data originated (Bryman, 2012).

Phenomenology in interpretivist research centres on how human beings experience the world and interpret that experience, that is existing presuppositions (Saunders et al., 2009; Bryman, 2012). Thus, to understand social phenomena, consideration is given to the subjects' "lived experience" and their interpretation to comprehend and describe the divergent subjective views (Bhattacharjee, 2012; Saunders et al., 2019:149). Symbolic interactionism, on the other hand, emphasises that meaning can be derived from the interaction amongst individuals, the differing roles at work and how language is used (Saunders et al., 2009; Hammond & Wellington, 2013). Generally speaking, interpretivism highlights that the individual's explanation and experience of the social world are sculpted by "language, culture and history" (Crotty, 1998, cited in Saunders et al., 2019:149).

Interpretivist studies aim to generate novel, comprehensive understandings and meanings of the research participants' perspective of their social world and circumstances (Orlikowski & Baroudi, 1991; Klein & Myers, 1999; Saunders et al., 2009; Mack, 2010; Saunders et al., 2019).

Thus, it was appropriate that this research adopted an interpretivist approach to study the phenomenon and provide meaningful interpretation of the findings.

3.2.3 Axiology

The term, *axiology*, has its roots in ancient Greek, originating from the word, *axios*, that is defined as value and refers to the values and ethics of the researcher (Killam, 2013; Saunders et al., 2019). Axiology relates to behaviour and involves “defining, evaluating and understanding” what is deemed acceptable and unacceptable actions within research (Kivunja & Kuyini, 2017:28). The researcher's chosen approach as well as the actions taken, will be determined by their axiological values, beliefs and suppositions (Spencer et al., 2014). Therefore, the researcher's philosophical stance on ontology and epistemology will be harmonised by their axiological position (Aliyu et al., 2015). All human action is guided by values. Thus, the researcher will need to determine the degree of influence of their own beliefs and values, in addition to how to deal with the beliefs and values of the research participants (Heron, 1996, cited in Saunders et al., 2019).

This researcher was consciously aware of possible bias, thus participants were free to convey their views and their responses without interference from the researcher. Findings from the study were derived as a result of the systematic steps of analysis applied to deduce patterns of meaning from the collected data.

3.3 Research approach

The research approach, according to Grix (2001), is contingent on the researcher's philosophical assumptions and entails the various means in which knowledge can be obtained. Theory development in research is frequently dictated by either deductive or inductive reasoning, as represented in Figure 3.4. Yet, it can also be abductive (Saunders et al., 2019). Constructing explanations, making predictions and drawing conclusions from existing knowledge can be characterised as reasoning in research (Johnson-Laird, 1999; Hughes & Nimmo, 2017).

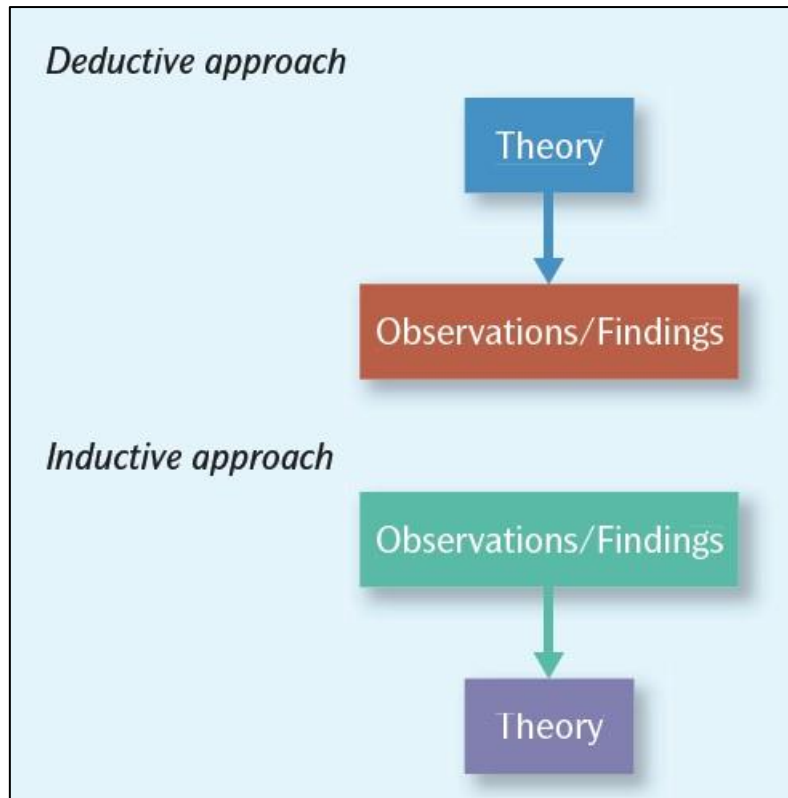


Figure 3.4: Deductive and inductive approaches to the relationship between theory and research (Bryman, 2012:26)

A deductive approach is generally synonymous with quantitative research, whereas an inductive approach is associated with qualitative research (Grix, 2001). An abductive approach would incorporate either quantitative or qualitative research methods or a combination of both (Dudovskiy, 2018). In the following sub-section, the different approaches (deductive, inductive and abductive) are discussed in relation to this study.

3.3.1 Deductive approach

A deductive approach to research involves deriving specific and true conclusions, employing logical arguments or reasoning, emanating from general premises or statements that are each true (Grix, 2001; Saunders et al., 2019). The depiction of a deductive approach is demonstrated in Figure 3.5, using a simple deductive argument or syllogism.

All living things will eventually die.	(General statement – first premise)
This animal is a living thing.	(Inference – second premise)
Therefore, this animal will eventually die.	(Conclusion)

Figure 3.5: Example of a simple deductive argument or syllogism (Walliman, 2011:18)

The true nature of the deductive premise determines the true nature of the conclusion. For example, if the major premise or generalisation is: “All men are immortal”, and the minor premise or inference is: “Socrates is a man”, the logical conclusion would be: “Socrates is immortal”, which would be false (Walliman, 2011; Hammond & Wellington, 2013:42). Dominant in natural sciences, deductivism entails theory development that rigorously test hypotheses and patterns utilising newly found empirical data (Bhattacharjee, 2012; Saunders et al., 2019). Hence, the data collection process is prescribed by theory and the deduced hypothesis, with the resulting findings, either leading to the confirmation or rejection of the hypothesis and validation or disproof of the theory (Bryman, 2012).

Consequently, the deductive approach relates to the total rejection of the hypothesis necessitating a fresh start, as well as the exactness of the premise, establishing the accuracy of the conclusion (Walliman, 2011; Hammond & Wellington, 2013). The deductive approach is often linked to quantitative studies and normally not applicable for exploratory qualitative research.

3.3.2 Abductive approach

The term, *Abductive Approach*, was developed by Charles S. Peirce at the beginning of the 20th century as an extension of deductive and inductive reasoning – abduction is useful at the initial phase of establishing and evaluating scientific hypotheses (Ladyman, 2002; Walton, 2005; Neuman, 2014; Garrett, 2018). Abductive reasoning reverses from “effect to cause” and involves formulating and selecting a hypothesis based on the evidence that best explains a phenomenon (Ladyman, 2002; Butler, 2010; Garrett, 2018; Hughes & Nimmo, 2017:18; Saunders et al., 2019).

Abduction involves researchers departing from “conventional wisdom” and applying the “common-sense reasoning” humans engage in on a daily basis (Neuman, 2014; Garrett, 2018:42). If we consider: “The body is a mortal thing” as a truthful premise, and “The soul is

an immortal thing” as a minor probability; it stands to reason that the predicated conclusion of: “The soul survives the body” has a degree of uncertainty. However, it is the most fitting explanation (Butler, 2010:113). Therefore, it can be said that abductive reasoning, due to the lack of concrete evidence, is merely clever guesstimating (Walton, 2005). Be that as it may, the strength of abduction is in its promotion of the understanding and comprehension of a phenomenon through the elimination of plausible conclusions, often applied in law as a basis for reasoning (Neuman, 2014).

3.3.3 Inductive approach

In contrast to deductive reasoning, in an inductive research approach the outcome is the theory gleaned from observations of an occurrence and founded on a premise, culminating in broad conclusions or theories (Bhattacharjee, 2012; Saunders et al., 2019). Inductive reasoning specifies that general conclusions are derived from specific observations of a phenomenon as presented in Figure 3.6 (Neville, 2005; Hughes & Nimmo, 2017). These conclusions have a probability of truth, rather than a certainty; therefore the aim of inductive reasoning is the extension of knowledge (Butler, 2010; Hughes & Nimmo, 2017).

All the giraffes that I have seen	(Repeated observations)
have very long necks.	
Therefore I conclude that all	(Conclusion)
giraffes have long necks.	

Figure 3.6: Example of inductive reasoning (Walliman, 2011:17)

Inductive reasoning employs a “bottom-up approach” for the construction of theories, encompassing the identification of patterns and commonalities within data (Hammond & Wellington, 2013:87). Reliable conclusions or theories, derived from an inductive approach, depend on making numerous observations that are repeated under varying situations and conditions (Walliman, 2011). Bryman (2012:27) remarks that, more often than not, in inductive research researchers merely end up with “empirical observations” rather than developed theories. Nevertheless, the strength of inductivism stems from understanding the circumstances surrounding an occurrence, as well as the individual’s interpretations of their social world (Saunders et al., 2019).

Therefore, this study adopted an inductive approach to explore and understand the factors affecting the governance of data privacy in South African organisations, in order to infer findings from the empirical data to theory.

3.4 Research design

A research design facilitates the fulfilment of research aims and objectives, in relation to the research problem, by providing a road map that guides the researcher during the research process (Creswell et al., 2003; Kothari, 2004). Research design is often confused with research methods, however the former constitutes the framework or structure for the implementation of the research method, that is data collection and analysis (Walliman, 2011; Bryman, 2012). According to Vogt et al. (2012) the research design extends beyond data collection and analysis methods and encompasses the interpretation and reporting of findings. Therefore, Kothari (2004), stresses that to obtain relevant information on a subject matter, requires the implementation of a framework to conduct scientific research which is inclusive of:

- a clearly stated research problem
- information gathering techniques and procedures
- a well-defined research population
- data processing and analysis methods

The design of research can be classified as either descriptive, explanatory or exploratory (Kothari, 2004; Saunders et al. 2009; Bhattacharjee, 2012). This study employed an exploratory approach to investigate the nature of the research phenomenon. Thus, the purpose of this research design, strategy and complementary methods applied to this research problem are further elaborated on in the following sub-section.

3.4.1 Descriptive research

Descriptive research aims to provide details of, or describe a person or a group as well as occurrences or circumstances, inclusive of “characteristics, behavioural patterns, attitudes, or opinions” (Kothari, 2004; Saunders et al., 2009; Wang & Park, 2016:85). Accordingly, based on the scientific method, a phenomenon must be carefully observed, and results meticulously documented (Bhattacharjee, 2012). The type of information required dictates the observation techniques employed – ranging from interviews and questionnaires to visual recordings (Walliman, 2011).

Researchers employing a descriptive study ask clearly defined factual questions, focussing on “how” and “who”, rather than “why” (Neuman, 2014:39). In other words, the causes and

effects of an occurrence are less important than the description of that occurrence (Wang & Park, 2016). Therefore, descriptive research can be viewed as a precursor to either exploratory or explanatory research, according to Saunders et al. (2009). As such, it is in conflict with the exploratory aim of this study.

3.4.2 Explanatory research

An explanatory study seeks to elucidate the causal factors of observed issues, behaviours or phenomena (Neville, 2005; Saunders et al., 2009; Bhattacharjee, 2012). That is to say, explanatory research seeks to go further than a mere description of an occurrence, but strives to clarify the antecedent causes and reasons behind it (Kumar, 2011; Neuman, 2014). Therefore, researchers who carry out explanatory studies are interested in “why and how” questions to explain underlying causes of a situation or problem and the relating factors (Kumar, 2011; Bhattacharjee, 2012:6).

Neuman (2014) explains that explanatory studies can utilise multiple research strategies for the development of new explanations of phenomena. Frequently explanatory research designs, according to Wang & Park (2016) include experiments or quantitative questionnaire surveys. Thus, explanatory research is divergent from the exploratory nature of this research.

3.4.3 Exploratory research

Exploratory research supports the development of preliminary ideas about a phenomenon, newly identified issues, or subjects that require more knowledge (Neuman, 2014). Deeper comprehension of phenomena are gained through posing “what, how and why questions” (Gupta & Awasthy, 2015:16). Generally speaking, the goal of the researcher is to find some foundational information to justify further studies into emergent problems or occurrences in need of clarification (Kothari, 2004; Wang & Park, 2016). Observations indicate that researchers who adopt an exploratory study should have creativity, open-mindedness, flexibility and an investigative nature (Neuman, 2014).

Exploratory research design requires a certain degree of versatility and adaptability to compensate for any changes dictated by new insights (Kothari, 2004; Saunders et al., 2009). In an exploratory study there are very few signposts or guidelines, the direction of the study continuously shifts, the scope to generalize is limited and findings may require further examination relative to contextual factors. (Neuman, 2014; Wang & Park, 2016). Be that as it may, the strength of exploratory research lies in its initial assessment of a given situation and subsequent theory development from empirical data (Kothari, 2004; Bhattacharjee, 2012;

Neuman, 2014; Gupta & Awasthy, 2015). Moreover, important results can be contributed by a well-formulated explorative study (Mayring, 2014).

The adoption of an exploratory design is complementary to the aim of this study which sought to explore the research phenomenon that may provide insights into the factors affecting the governance of data privacy in South African organisations.

In the following section the research methods in relation to this study are discussed in detail.

3.5 Research strategy

The research strategy employed largely depends on the researcher's approach to the study, be it deductive or inductive (Hammond & Wellington, 2013; Neuman, 2014). A deductive approach is optimal for the testing of hypotheses, whereas an inductive approach is concerned with generating insights, as well as the exploration and explanation of phenomena (Hammond & Wellington, 2013). In addition to that, Bhattacharjee (2012) asserts that the deductive approach employs strategies such as experiments and surveys which are often associated with a descriptive design, while case studies, ethnography, action research, grounded theory, archival research and narrative inquiry are most likely adopted in an inductive approach which is associated with exploratory and explanatory designs.

This study adopted an inductive approach with an exploratory multiple-case study design to understand the factors affecting the governance of data privacy in IoT-based organisations in South Africa. The afore-mentioned strategies are further discussed in the subsequent sub-sections in this chapter.

3.5.1 Experimental research

The objective in experimental research is to examine, in a controlled environment, the causal links between variables by measuring the observable outcomes when circumstances are manipulated (Kothari, 2004; Bhattacharjee, 2012). In other words, the cause and effect of phenomena are investigated by altering an independent variable and observing the impact on a dependent variable (Walliman, 2011; Bryman, 2012). According to Neuman (2014) experimental research can be conducted with a relatively small number of participants, either in the field or in a laboratory setting. Broadly speaking, experimental studies can be categorised as either true experimental or quasi-experimental designs (Russell, 2006; Soiferman, 2010; Bhattacharjee, 2012; Creswell, 2014).

3.5.1.1 True experimental design

Participants in a true experimental design are randomly selected and assigned to experimental or control groups, where a “planned intervention or manipulation” will be administered to the experimental group and the control group will remain intervention free (Saunders et al., 2009:142; Bhattacharjee, 2012; Creswell, 2014). As depicted in Figure 3.7, the dependent variable is tested before and after manipulation to determine the effects of the administered intervention on the dependent variable (Creswell, 2009; Saunders et al., 2009; Walliman, 2011; Bhattacharjee, 2012).

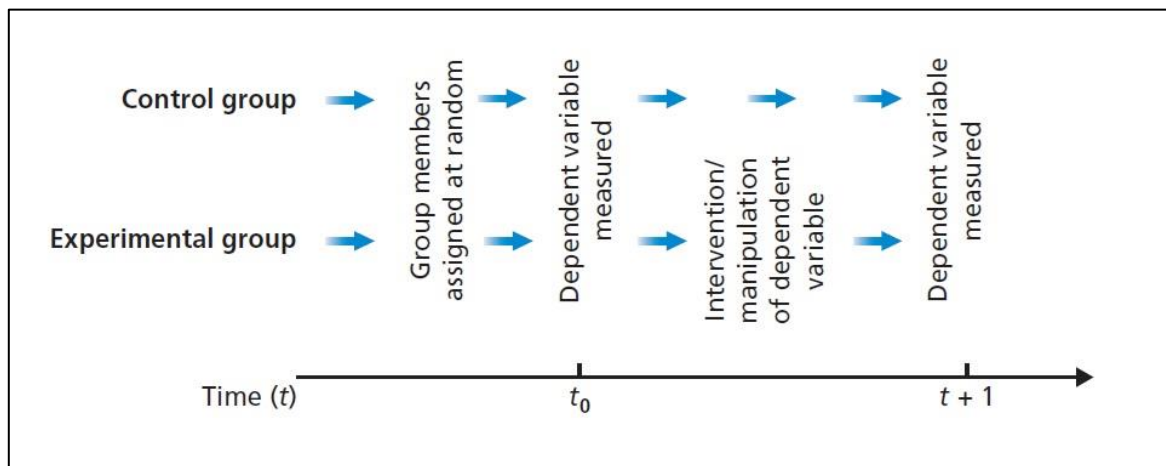


Figure 3.7: Example of a true experimental design (Saunders et al., 2009:142)

The five steps in true experimental design are described by Russell (2006) as:

1. Hypothesis is formulated.
2. Experimental or control group participants are randomly assigned.
3. The dependant variable(s), in one or both groups, is (are) measured.
4. Manipulation or intervention is introduced.
5. The dependant variable(s), in one or both groups, is (are) measured again.

True experimental designs enable the isolation, control and intense examination of variables, consequently these types of experiments are the most reliable (Walliman, 2011; Bhattacharjee, 2012). On the other hand, Hammond and Wellington (2013) argue that experimental research can be challenged based on:

- the small sizes of groups.
- the novelty effect of the manipulation, thus predictions of future behaviour are unreliable.
- the focus is on what works rather than how it works.
- interventions of a medical, educational and social nature can be unethical if deemed more favourable to one group.

3.5.1.2 Quasi-experimental design

In a quasi-experimental design, the random choosing of participants cannot be achieved and the use of naturally established groups are necessitated, for example a family unit, company or students at a school. Nevertheless, the control and experimental groups are matched as closely as possible (Walliman, 2011; Creswell, 2014). In the absence of a control group, experiments are performed on parallel groups and the consistency of the outcomes compared (Walliman, 2011). The inability of selecting participants at random might bring into question the internal validity of a research, due to unequal groupings of participants or subjects (Marczyk et al., 2005; Bryman, 2012). Moreover, the independent variable is less controllable by the researcher (Neuman, 2014). Therefore, results obtained through true experimental designs are more reliable than results from quasi-experimental designs (Walliman, 2011).

Experiments were not deemed suitable for this research study due to the subjectivity involved in the selection of participants according to specified criteria.

3.5.2 Surveys

Surveys enable the study of representatives of a population in order to provide a numerical account of circumstances, attitudes, or beliefs, resulting in generalisations on the part of the researcher based on the feedback of the population sample (Bhattacharjee, 2012; Neuman, 2014; Creswell & Creswell, 2018). Survey research consists of a cross-sectional design that enables the detection of patterns from the collected body of quantifiable data (Bryman, 2012). Descriptive and exploratory research tend to utilise surveys towards answering questions related to “who, what, where, how much and how many” enquiries (Saunders et al., 2009:144). Additionally, survey research aims to answer questions of a descriptive nature, “questions about the relationship between variables”, and “questions the about predictive relationship between variables over time” (Creswell & Creswell, 2018:245). Survey strategies can be broadly classified as questionnaires or structured interviews (Saunders et al., 2009; Blaxter et al., 2010).

Questionnaires comprise of a list of structured (answer selected from list provided) or unstructured (answer in own words) questions that record the replies from respondents which include, “mail-in, group-administered, or online surveys” (Bhattacharjee, 2012:78). On the other hand, a structured interview is administered by an interviewer who employs an interview schedule which is a set of predetermined, identical and closed-ended questions (Bryman, 2012). Interpretivist studies utilising surveys would generally comprise of open-ended questions, while positivist studies tend to favour closed-ended questions (Howell, 2013b). A

survey was deemed inadequate for this study due to the nature of the subjects and the need to obtain deep insights into the research problem which a survey strategy does not offer.

3.5.3 Action research

Action research, a term first coined by Kurt Lewin in the late 1940s, refers to an iterative cycle of action and evaluation to address social and organisational issues (Adelman, 1993; Saunders et al., 2009; Hammond & Wellington, 2013). Figure 3.8 represents one full circle of Lewin's proposed model for action research, however a number of circles might be included in a complete project, each taking into account the outcomes and considerations of the preceding circle (Willis & Edwards, 2014). Essentially, the aim of action research is to provide suggestions for change to current practices or behaviours that are deemed problematic (Bell, 2005). Subsequently, the appeal of action research can be seen in various fields and projects, including “community activism and development, citizenship, professional learning, and product design”; as well as professional areas such as social care, education and health (Blaxter et al., 2010; Hammond & Wellington, 2013:5).

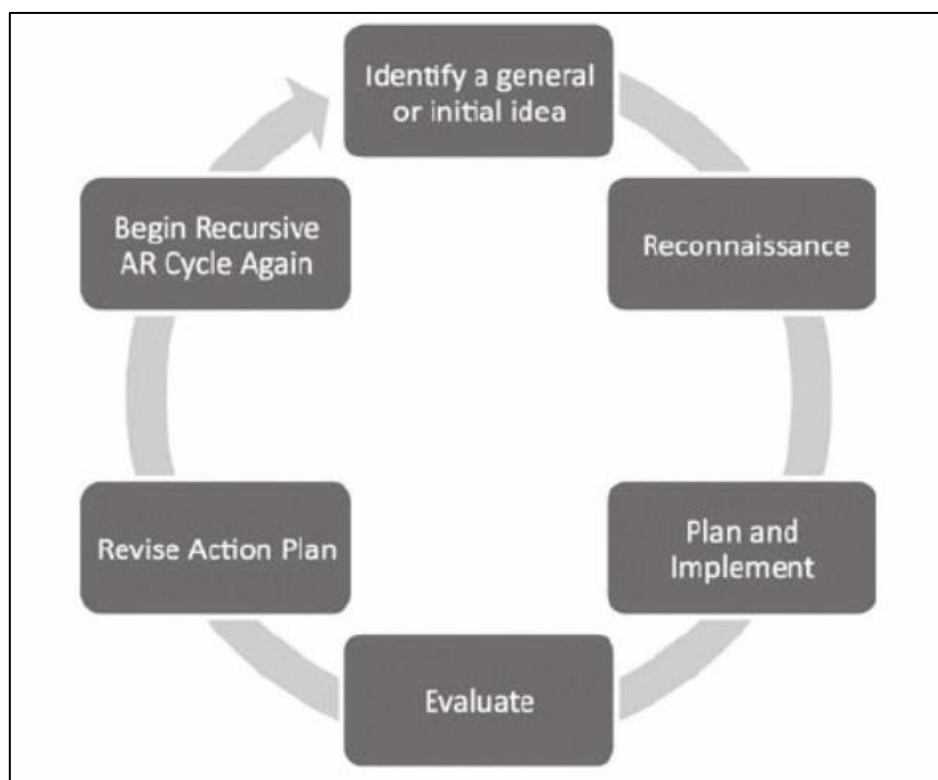


Figure 3.8: Kurt Lewin's original plan for action research (Willis & Edwards, 2014:13)

The advantage of action research lies in its bottom-up, adaptable and iterative approach which avoids the pitfalls of a top-down approach found in conventional research (Hammond & Wellington, 2013). However, the results from action research might be difficult to generalise

as it pertains to a specific issue or situation (Walliman, 2011). The focus of this exploratory research study did not allow for the consideration of action research that will require the implementation and evaluation of interventions which are beyond the scope of this study.

3.5.4 Participatory research

In participatory research the direction of the research is informed by the participants selected from the chosen population. This type of approach often seeks to empower disadvantaged communities by addressing “inequity, health disparities, or a social injustice” (Fetters et al., 2013:2139). According to Saunders et al. (2019:143) the “experiential and practical” knowledge and the acquisition thereof, are emphasised in participatory research as well as participants’ active involvement in knowledge creation. In other words, the divide between participants and researchers is minimised and research findings are customised to the demands of the community through increased participation and engagement (Kumar, 2011). As such, this active collaboration facilitates significant and valuable solutions that could assist the wider community, in addition to enhancing effectiveness, and saving time and money (Cornwall & Jewkes, 1995; Higginbottom & Liangputtong, 2015). However, the usefulness of participatory research is twofold. Firstly, it involves recognising the appropriateness of utilising a participatory approach and secondly, the establishment of partnerships and stakeholder collaboration at different levels of the community (Tadevosyan & Schoenhuth, 1997). This research does not relate to community empowerment and participation, therefore it was not deemed appropriate for this study.

3.5.5 Grounded theory

Sociologists Glaser and Strauss first introduced grounded theory in 1967 as an approach to the development of theory that grounds or roots itself in the data instead of empirical theory testing (Dey, 2004; Merriam & Tisdell, 2016; Mohajan, 2018). In other words, the research data generate the theory through the “theoretical sampling” of numerous sources or sites that facilitate the testing and refinement of new concepts emerging from the data (Dey, 2004:80). The successive rounds of data collection and analysis will be informed by the insights obtained from each round until the point of saturation as illustrated in Figure 3.9 (Leavy, 2017). Grounded theory, therefore employs an iterative process to compare and contrast previously collected data and new data to identify the “patterns of interaction” by linking “two or more data categories” (Gupta & Awasthy, 2015:27). The strategy was unsuitable for this study, because of the requirement to explore prior literature and theory relating to the subject matter and research phenomenon.

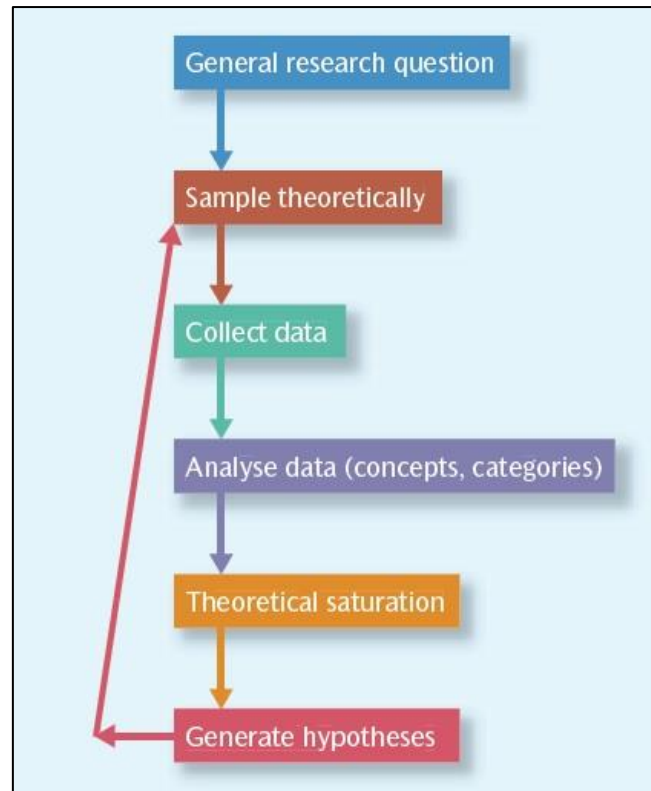


Figure 3.9: The process of theoretical sampling (Bryman, 2012:420)

3.5.6 Ethnography

Inspired by anthropology, ethnography is an interpretive research design that involves researchers immersing themselves in the culture or social world of the participants being studied over a prolonged period of time (Bhattacharjee, 2012; Bryman, 2012; Hammond & Wellington, 2013; Creswell & Creswell, 2018). According to Williams (2007) the ethnographic approach involves obtaining access to the site to be researched, building trust and establishing a connection with the subjects as well as identifying the key informants. Predominately, the data collection techniques in an ethnography study involve interviews and participant observation (Saunders et al., 2009; Hammond & Wellington, 2013; Creswell & Creswell, 2018).

The role of the ethnographic researcher as it relates to participant observation can be either covert or overt and range from full participation to non-participation (Neville, 2005; Greener, 2008; Bryman, 2012; Leavy, 2017). As per Bryman (2012), this role and participation can be further categorised and described as:

- **Covert full member:** The researchers are full members of participating groups, however, it is not known that they are researchers.
- **Overt full member:** The researchers are full members of participating groups and it is known that they are researchers.

- **Participating observer:** The researchers are not members, but are actively involved in the undertakings of the groups.
- **Non-participating observer with interaction:** The researchers are not actively engaged in the undertakings of the groups, observations are minimal and interactions occur via other methods.

The aim of an ethnographic approach is to provide detailed and nuanced descriptions and explanations of the subjects' natural setting or circumstances, as if they were explaining and describing it themselves (Saunders et al., 2009). As such, ethnography is a very resource-intensive and time-consuming strategy that generates context-specific findings (Bhattacharjee, 2012). An ethnography strategy was not applicable to this study, because of the inability to contextually situate the researcher for observation, time constraint and other limiting factors.

3.5.7 Archival research

Mills and Mills (2018:32) posit the purpose of archival research is to obtain an understanding of a professional group, leader or an organisation through the "study of collections of documents and artifacts". In essence, Moore et al. (2017:4) determine archival research:

"involves making sense of sources – the traces, what remains of people and events of the past – in a particular kind of location called an archive, which is a repository of some kind for holding and making available collections of things, ranging from institutional and formal edifices to personal collections shared between family or friends".

According to Allen (2017:48) the approaches to archival research can vary based on: "the systematic examination of old or historical materials", "an investigation of materials accessed at a formal archive" or "an investigation of collections of rare materials". Thus, the source material required will not only dictate the approach, but also the type of archive, and access requirements (Grix, 2001).

A major advantage of archival research is that it is non-reactive, that is, the individual's conduct or actions cannot be modified after the fact (Russell, 2006). Even so, the issue of access to an archive is critical to the success of archival research. For instance, there may be a waiting list, an affiliation to an institution may be required or special clearance might be needed (Grix, 2001; Schwartz-Shea & Yanow, 2012).

3.5.8 Narrative inquiry

Narrative research encompasses a comprehensive study and understanding of people's lives and experiences through their stories, told over a period of time and then recounted by the researcher in a chronological narrative (Clandinin & Caine, 2013; Creswell & Creswell, 2018). A narrative approach, according to Bell (2005) gives voice to human experience through the participants' personal accounts of incidents or events. A range of techniques can be used by the narrative researcher to develop a theme, including "diary entries, blog posting and interviewing", as well as "reflective autobiography, life story, or the inclusion of excerpts from participants' stories" (Bell, 2005:21; Hammond & Wellington, 2013:110).

The narrative researcher therefore, would adopt an interpretivist stance strongly influenced by a hermeneutic philosophy which as previously highlighted, relates to the study of written text (Merriam & Tisdell, 2016). However, Bold (2012:14) asserts narrative research can be expanded to include materials such as "drawings, photographs, poetry, plays, video recordings, interview scripts, ad hoc conversations and sequential observations", as well as "gestures, body language, visual images and different media effects". The data captured ought to provide an insight of the meaning for actors in the circumstances of their daily lives, thus providing the narrative researcher with valuable interpretations and descriptions of phenomena (Salkind, 2010).

The above-mentioned approaches, in the researcher's opinion, were not appropriate to understand and gain meaningful information of the factors affecting the governance of data privacy in IoT-based organisations. Therefore, a multiple-case study was employed as explained in the next section.

3.5.9 Case study

Case study is described as the investigation of a case with the purpose of observing and understanding the intricacy and specific nature of the case (Stake, 1995; Bryman, 2012). A case study strategy is employed to cover the contextual conditions of the phenomenon being studied (Yin, 2003). Case study research emphasises the focus on a snippet or small quantity of instances to gain in-depth knowledge and understanding of the whole (Hyde, 2000; Gerring, 2007; Neuman, 2014). The appropriateness of a case study relates to finding answers to "how" and "why" questions and the initial description or identification of the "case" or "unit of analysis" is dependent on the researcher (Yin, 2003:22).

The determining factor for the unit of analysis relates to the focal point of the research. For instance, it can be an individual, an organisation, a group(s), a social situation, or an event

(Neuman, 2014; Stewart, 2014). The researcher should therefore, closely examine the study's research questions as a guide to selecting the appropriate unit of analysis (Benbasat et al., 1987). In reference to Figure 3.10, Yin (2003) differentiates between single- and multiple-case study designs in which the unit of analysis can either involve a singular unit (holistic) or multiple units (embedded).

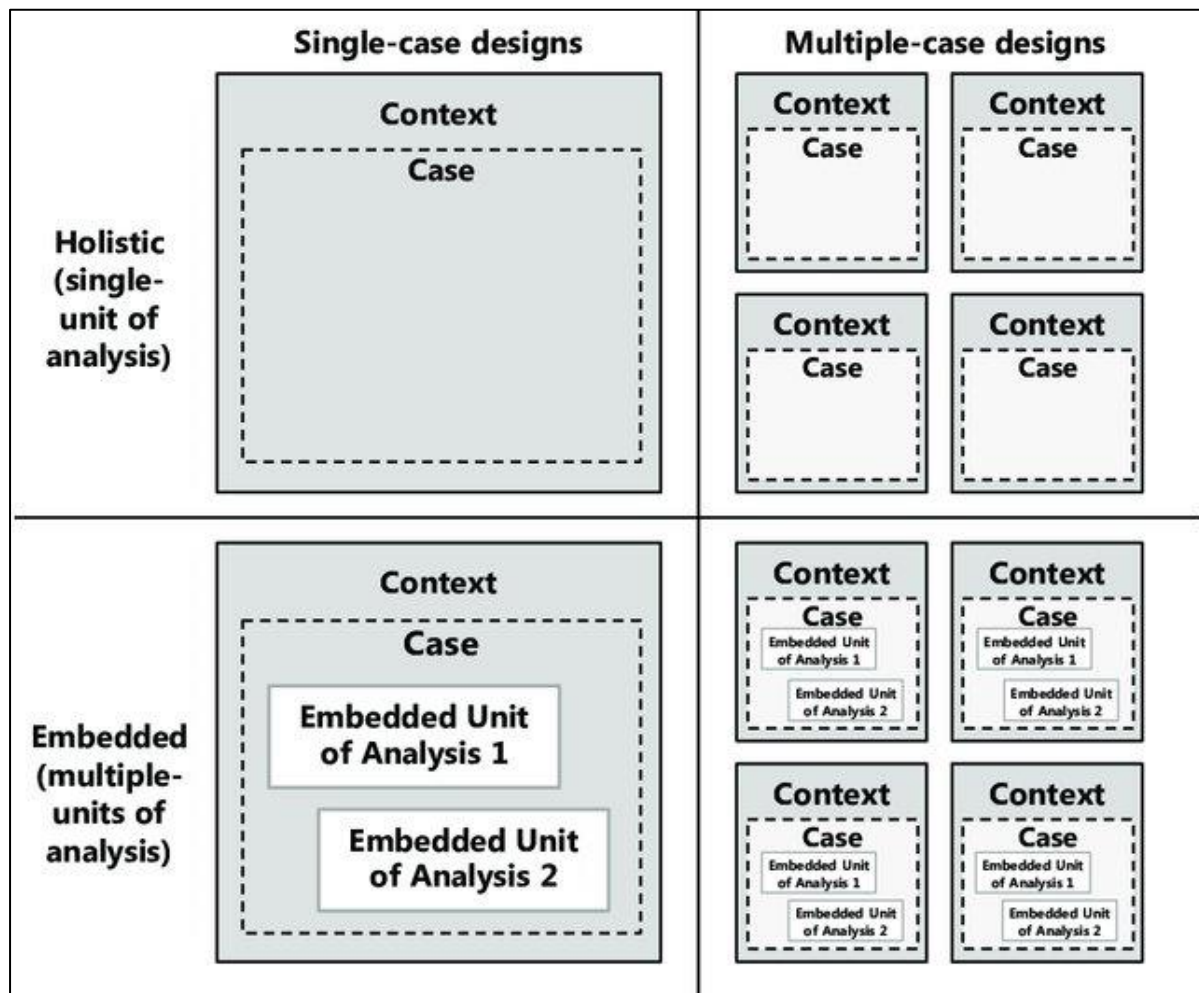


Figure 3.10: Basic types of designs for case studies (Yin, 2014:60)

The establishment of boundaries for a case study is imperative for the project to remain within scope. Baxter and Jack (2008:546) stress that these can include “time and place”, “time and activity”, or “definition and context”. The overall purpose of the research will steer the choice of a particular type of case study design. Thus, the researcher needs to give consideration to the appropriateness of the case study to be conducted (Baxter & Jack, 2008; Robson & McCartan, 2016).

Yin (2003) classified case studies as either descriptive, explanatory or exploratory as well as further differentiated into four types of case studies, as indicated in Figure 3.9. However, Stake

(2005), distinguishes between intrinsic, instrumental and collective case studies. To demonstrate the practical choices that influence the applicable case study type, Table 3.1 provides a description of the types of case study specified by the afore-mentioned authors.

Table 3.1: Types of case study

Types of case study	Purpose / Description
Descriptive	To describe an occurrence within the context of its real world (Baxter & Jack, 2008; Yin, 2014).
Explanatory	To explain how or why an occurrence or sequence of events transpired or did not transpire (Yin, 2014).
Exploratory	To explore situations where the evaluated occurrence has no clear outcome (Baxter & Jack, 2008).
Single-case	There are a number of conditions in which a single-case study will be appropriate, and the key reasons for selection can include: “critical, unusual, common, revelatory, or longitudinal” (Yin, 2014:40). These designs can be either holistic or embedded, with either one or several units of analysis, as shown in Figure 3.9 (Yin, 2003).
Multiple-case	Can be used in instances where there are more than one case within a study, for example, several organisations or schools (Yin, 2003). Careful consideration is required in case selection as comparisons need to be drawn from the cases and the aim is to replicate results across cases (Baxter & Jack, 2008).
Intrinsic	The researcher has an inherent interest in a particular case, thus there is no selection of the case, but the object of study is given, such as a teacher studying a pupil's learning difficulties (Stake, 1995).
Instrumental	By studying a particular case we might gain insight into an issue, thus a case plays a key part in acquiring an understanding of something else (ibid, 1995; Simons, 2014).
Collective	Instead of studying one case, the researcher opts to study multiple cases and each case provides insight into the effects of an issue (Stake, 1995).

This researcher adopted Yin’s (2003) case study classification, as it seems to best resonate with the exploratory research design employed by this study. Yin (2003:39) asserts that case studies can be clearly distinguished as either “single- or multiple-case study designs”, as depicted in Figure 3.9. After selecting the case or unit of analysis and the applicable case study type, it must be decided if the phenomenon under investigation would be better understood through a single- or multiple-case study design (Baxter & Jack, 2008).

3.5.9.1 Single-case designs

A single-case study design is concerned with studying a phenomenon at an overall level, concentrating on a single unit, such as an individual or organisation and is generally more useful for generating a theory (Bhattacharjee, 2012; Robson & McCartan, 2016). Researchers often select a single-case design that is representative of being either critical, unusual, common, revelatory or longitudinal (Yin, 2003; 2014). Table 3.2 provides a brief description of the reasons for selecting a single-case study design.

Table 3.2: Rationale for single-case designs

Rationale for case	Description
Critical	Useful to test a hypothesis and to gain insight into the conditions in which the theory will hold true or not (Yin, 2003; Bryman, 2012).
Unusual (Extreme)	Involves cases that deviate from everyday practices or accepted norms, such as those found in clinical research (Yin, 2014).
Common (Representative or Typical)	Commonplace activities are studied to record the situations and conditions of their occurrences (Yin, 2003).
Revelatory	This occurs when a social science study, that was previously inaccessible, becomes available for observation and analysis (Yin, 2009).
Longitudinal	Involves the same case being studied at different junctures to ascertain the changes over time (Yin, 2014).

A single-case study design may be applicable in certain situations. However the findings might not be generalisable, therefore a multiple-case study design would be appropriate for a more holistic perspective of the phenomenon (Bhattacharjee, 2012).

3.5.9.2 Multiple-case designs

A multiple-case design involves a study that includes more than one case and the purpose is to comprehend the “similarities and differences between the cases” (Baxter & Jack, 2008:550). Therefore, Yin (2003) emphasises the careful selection of each case in order to arrive at results of a similar nature or unveil results of a contrasting nature where the reasons are predictable. In addition, Bhattacharjee (2012:94) indicates that multiple-case designs are applicable in studies where the aim is to develop “richer and more nuanced interpretations of a phenomenon” or “for establishing generalizability of inferences”.

A multiple-case study strategy was deemed appropriate for this study. It was employed to gain robust and meaningful information to explore the factors affecting the governance of data privacy in IoT environments in South Africa. This study featured multiple cases of similarly related organisations with relevant knowledge on the subject matter.

3.5.10 Research methods

Fundamentally research methods refer to the instruments and techniques applied (Kothari, 2004; Saunders et al., 2009; Mishra & Alok, 2017). Methods are often deliberated as either concerned with numerical (quantitative) or text (qualitative) data (Hammond & Wellington, 2013; Creswell, 2014). The methods utilised in research, according to Kothari (2004), can be categorised into three groups, namely:

- data collection methods,
- statistical methods for determining the connection between an unknown and the data,
- evaluation techniques used to verify the accuracy of findings.

The research aim, objectives and research questions will dictate the method chosen by the researcher (Creswell, 2009).

The two major research methods (qualitative and quantitative) are expanded below.

3.5.10.1 Quantitative research

According to Williams (2007:66), the starting point in quantitative research is the “problem statement and involves the formation of a hypothesis, a literature review, and a quantitative data analysis”. If the aim of the research is to quantify a phenomenon then quantitative research is applicable (Kothari, 2004). Furthermore, Creswell (2009:22) established that “quantitative research is a means for testing objective theories by examining the relationship among variables”. Bryman (2012) contends that quantitative research is normally associated with a deductive approach with a positivist stance. As previously stated, this study adopted an inductive approach with an interpretivist position to explore the factors affecting the governance of data privacy in IoT-based organisations in South Africa. Thus, a qualitative research method was applicable to this study and is discussed in the following section.

3.5.10.2 Qualitative research

According to Creswell (2009:22), “qualitative research is a means for exploring and understanding the meaning individuals or groups ascribe to a social or human problem”. Williams (2007) determined that qualitative research involved discovery of a holistic nature within the natural surroundings of the phenomenon under inquiry. Bryman (2012:380) described three key features (apart from relating to words) of qualitative research which includes “an inductive view of the relationship between theory and research”, an epistemological position described as interpretivist” and a subjectivist ontological position. There are several approaches to conducting qualitative research such as, but not limited to “ethnography, grounded theory, narrative research, phenomenological research and case studies” (Creswell, 2009:30).

In the following section the research strategies in relation to this study are discussed in detail.

3.6 Sampling

Sampling, as noted by Leavy (2017:75) centres around the “who or what” of the research; where the “who” represents the “subjects, respondents, participants, or collaborators”, and the “what” can include data such as images or text. The purpose of sampling is to select a subset or sample of a population that closely represents the features of interest in a study; the population of the study refers to the “group of elements” under investigation (Neuman, 2014;

Leavy, 2017:76). The techniques for sampling, Neville (2005:31) states can be classified as either, “probability or non-probability sampling”, as illustrated in Figure 3.11.

This study employed non-probability, purposive sampling with the aim of selecting organisations and individuals who are best able, in the researcher's judgement, to provide relevant information on the factors affecting the governance of data privacy in IoT environments in South Africa.

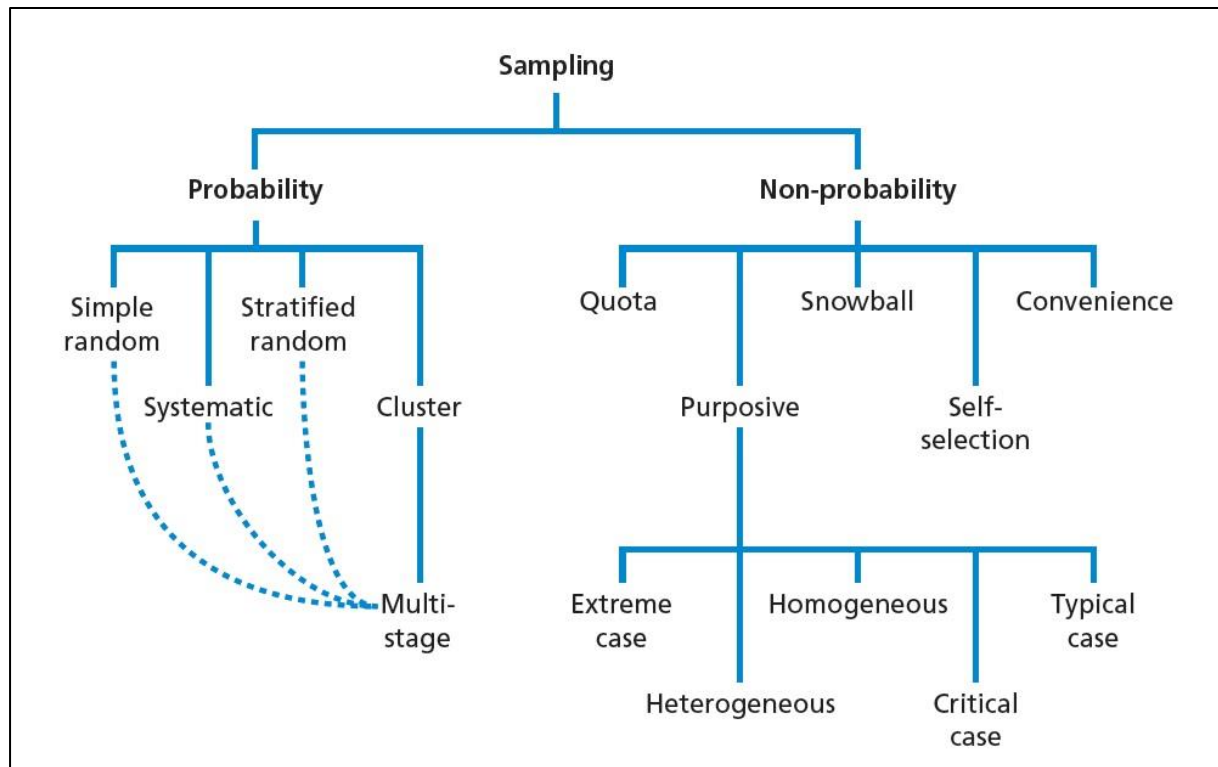


Figure 3.11: Techniques for sampling (Saunders et al., 2009:213)

The sampling techniques highlighted in the diagram above are further discussed in the following sub-section.

3.6.1 Probability sampling

Probability sampling typically occurs in quantitative research and involves a strategy in which elements within a population have “a known or nonzero” possibility of selection (Phillips, 2014; Leavy, 2017:78). Survey-based research strategies are frequently associated with probability sampling where data need to be collected from the whole or a large portion of the population (Saunders et al., 2009). A brief description of the probability sampling techniques highlighted in Figure 3.10 is given below.

- **Simple random sampling**

Simple random sampling involves an equal chance or probability of an element being chosen from the population for inclusion in the sample (Kothari, 2004). Simple random sampling benefits from having access to an exact and easily available sampling frame of the whole population, such as a list of employees in an organisation or a list of students at a university (Saunders et al., 2009). Using simple random sampling negates issues related to human bias and subject availability at the initial stage of selection (Bryman, 2012).

- **Systematic sampling**

Systematic sampling encompasses the random selection of the first element in the study population and continues by selecting every k^{th} element, where k represents the sampling fraction (Bhattacharjee, 2012; Leavy, 2017). To calculate the sampling fraction, the researcher applies the following formula: sampling fraction (k) = sample size (n) / population size (N) (Saunders et al., 2009; Bryman, 2012).

- **Stratified random sampling**

Stratified random sampling entails the division of the population into subgroups or strata based on a selection of features or characteristics (Saunders et al., 2009). The researcher then randomly selects an equal number of elements from each stratum or a proportionate representation of the elements in the total population (Kumar, 2011). For instance, if a population consisted of 49 percent males and 51 percent females, the gender ratio should be maintained in the sample (Neuman, 2014).

- **Cluster sampling**

Cluster sampling comprises of the population being divided into groups based on parameters such as geographical areas, such as provinces or institutions, for example, schools (Kothari, 2004; Russell, 2006). These groupings are termed clusters and the complete list of clusters will constitute the sampling frame from which the researcher randomly selects a number of clusters (Saunders et al., 2009; Leavy, 2017).

- **Multi-stage sampling**

Multi-stage sampling develops the idea of cluster sampling further and generally relates to big investigations that could involve an entire country (Kothari, 2004). Multi-stage sampling includes some form of random sampling for the selection of a series of cluster samples. The first stage may encompass the selection of “sampling units such as states, then districts, then towns and finally certain families within towns” (Kothari, 2004; Saunders et al., 2009).

3.6.2 Non-probability sampling

Described as a qualitative research method choice for sampling, non-probability sampling pertains to the selection of samples based on the researcher's "subjective judgement" (Saunders et al., 2009:233; Merriam & Tisdell, 2016). Researchers employ non-probability sampling in cases where the possibility of selection cannot be determined or elements of the population have a "zero chance" of being selected (Bhattacharjee, 2012:69). Non-probability sampling, according to Russell (2006:186) is appropriate for "labor-intensive, in-depth studies of a few cases", "large surveys" where it is impossible to obtain a "probability sample" or where "expert informants, not randomly selected respondents" are needed. The non-probability sampling techniques highlighted in Figure 3.11 are further expanded below.

3.6.2.1 Quota sampling

Quota sampling involves the researcher identifying certain characteristics of interest required of the study population as well as the overall presentation of these features in the population (Leavy, 2017). Following the segmentation of the population based on the characteristics, the researcher will non-randomly select elements from each segment or stratum to satisfy a predetermined allocation (Bhattacharjee, 2012).

According to Bryman (2012) the objective of quota sampling is to categorise relative portions of individuals, based on say age, gender or ethnicity, to produce a sample representative of the population. Quota sampling, as per Saunders et al. (2009) is commonly used for interview surveys and can be seen as a type of non-random stratified method of sampling. Therefore, because of the non-probability of the resulting sample, it is not possible to generalise the findings to the entire sampling population (Kumar, 2011). However, Bryman (2012) contends that the strengths of quota sampling are located in the fact that it is more cost-effective and quicker than probability sampling techniques.

3.6.2.2 Snowball sampling

Snowball sampling emanates from the identification of one or two participants who then inform the researcher of potential participants who in turn inform the researcher of more potential participants and so forth, imitating a snowball that grows and expands (Neuman, 2014). Snowball sampling can be useful in exploratory research when knowledge of the population is limited or elements are difficult to locate, for instance homeless people and drug users (Abbott & McKinney, 2013; Wang & Park, 2016). However, Saunders et al. (2009) warn that snowball sampling can result in a homogeneous sample and issues related to informant bias can arise.

3.6.2.3 Convenience sampling

Convenience sampling pertains to subjects that are selected based on the accessibility or availability, such as time and location (Abbott & McKinney, 2013; Merriam & Tisdell, 2016). Therefore, the researcher considers the most suitable participants in the population to whom they have access, until the required sample size is reached (Leavy, 2017). Although convenience sampling is a technique that is widely used, it can be open to stimulus beyond the researcher's control or susceptible to bias (Saunders et al., 2009). In addition to that, the data obtained from a convenience sample are not “generalisable to any relevant population” as the participants are not “representative of a relevant population” (Abbott & McKinney, 2013:123).

3.6.2.4 Self-selection or voluntary sampling

Self-selection or voluntary sampling allows individuals to present their interest in participation in a study. This could be following a request in the form of an online appeal or advertisement in a magazine or newspaper (Neville, 2005). In experimental research where human subjects are required, self-selection or voluntary sampling is an effective sampling strategy which allows participants to willingly partake in research such as drug trials (Mujere, 2016). Therefore, voluntary or self-selection sampling can be less expensive and time-consuming. However, it can lead to a level of self-selection bias or a sample that does not fully represent a population (Alvi, 2016; Mujere, 2016).

3.6.2.5 Purposive sampling

Purposive sampling, also referred to as judgemental sampling, involves the researcher using their own judgement in selecting units that will provide answers to the research questions and objectives (Saunders et al., 2009). Thus, to produce the best data, the researcher aims to select the best conceivable or “information-rich cases” that will best address the overall purpose of the study (Leavy, 2017:79). The research questions would generally provide an indication of the cases or units to be sampled which can include “people, organisations, documents, departments, and so on” (Bryman, 2012:416). Therefore, purposive sampling is useful in exploratory research where deeper understandings of certain situations require in-depth investigations of particular cases or units (Neuman, 2014). The common strategies for purposive sampling outlined above in Figure 3.11 are further expanded below.

- **Extreme case**

The focus of extreme case sampling, also referred to as deviant case sampling, is on special or unusual cases where “notable outcomes, failures or successes” are highlighted (Mujere, 2016:119). Extreme case sampling provides valuable insights about an occurrence where the

knowledge acquired about peculiar conditions or outcomes often serves to guide future programs or practices (Patton, 2015; Mujere, 2016). Researchers who employ extreme case sampling actively search for cases that are atypical from mainstream cases and where general patterns and characteristics differ significantly from the norm (Neuman, 2014). Therefore, this researcher believes that greater comprehension and explanations are to be gained from these extreme cases than from conventional cases (Saunders et al., 2009).

- **Heterogeneous case**

Heterogeneous or maximum variation sampling relates to the selection of units or cases that encompass a diverse range of perspectives on the key dimensions of interest in the study (Robson & McCartan, 2016; Leavy, 2017). By looking at all angles, considerable understanding into a phenomenon can be gained and consequently lead to the identification of central themes within the sample (Mujere, 2016). Thus, emerging commonalities from maximum variation can be valuable and of interest in “capturing the core experiences and central, shared dimensions” involved in an occurrence (Patton, 2015:283). The employment of a heterogeneous sampling strategy, oftentimes involves seeking instances of a phenomenon that are either contrary or invalidating (Merriam & Tisdell, 2016).

- **Critical case**

Critical or crucial case sampling involves the selection of a key case in order to draw conclusions about the occurrence being studied (Bryman, 2012). Exploratory qualitative research can benefit from using critical case sampling, especially in studies where resources are limited and where an explanation of a phenomenon can be obtained from a single or small number of cases (Mujere, 2016). Logical generalisations, based on the findings from each critical case, can therefore be made to other similar cases in the same category (Patton, 2015).

- **Typical case**

Typical case sampling entails choosing and studying cases that are representative of a situation to gain understanding and illustrate what is normal and typical (Saunders et al., 2009). Therefore, typical case sampling would encompass a person, organisation or situation that is the average of the occurrence of interest (Merriam & Tisdell, 2016). Typical case sampling enables the researcher to compare findings of the study to similar samples rather than generalising the finding to a population (Mujere, 2016). For instance, community development research where studying a typical village highlights key issues (Patton, 2015).

▪ **Homogeneous case**

Homogeneous sampling involves the selection of units or cases that share similar traits and characteristics, such as “age, gender, background, occupation” (Mujere, 2016:119). The researcher chooses a homogeneous sampling strategy when “a particular type of person, organization, or place” is of interest, and the study’s research questions pertain to the characteristics of a specific group that require detailed examination (Saunders et al., 2009; Patton, 2015:283).

This study employed non-probability, purposive sampling of homogeneous dimension to select organisations and individuals who are best able, in the researcher's judgement, to explore the factors affecting the governance of data privacy in IoT environments in South Africa. The sample for the study was drawn from IoT-based organisations located in four of the provinces in South Africa. The sample size was fifteen IoT-based organisations, varying in size, with similar operational scope. Data were collected from selected representatives till the point of saturation was reached.

3.7 Unit of analysis

To establish the unit of analysis, the research questions should be closely examined as well as whether findings will be generalised, for instance to individuals or other organisations (Benbasat et al., 1987). In addition to that, Baxter and Jack (2008), remark that to determine the unit of analysis the researcher should aim to answer: “What do I want to analyse?”. As a result, the focus of the study will determine the unit of analysis, that is, whether it is an individual, an organisation, a group(s), a social situation or an event (Neuman, 2014; Stewart, 2014).

For the purpose of this study, the unit of analysis included selected IoT-based organisations in South Africa. The selected IoT-based organisations collect, store, aggregate and disseminate data obtained through IoT environments in South Africa. The unit of observation comprised high-level executives in these organisations which included the person(s) responsible for privacy compliance (data controllers, data processors, compliance officers, etc.).

3.8 Data collection

The validity and reliability of research rely on the successful collection of data (Palić et al., 2015). Following the definition of the research problem and objectives as well as the completion of the research design, the researcher needs to give consideration to the appropriate data collection techniques of the study (Kothari, 2004). A quantitative approach is

synonymous with data collection methods that generate numerical data, such as a questionnaire, whereas a qualitative approach would employ techniques that produce non-numerical data, for example interviews (Saunders et al., 2009). Ultimately, the researcher decides which methods are best and what data collection instruments would be suited for the study based on the research aim and objectives and the corresponding methodological choices and position (Bell, 2005). Furthermore, the researcher needs to determine whether secondary or primary data are relevant to be collected (Kothari, 2004).

For the purpose of this study, primary data were collected through semi-structured interviews of participants, from high-level executives of fifteen IoT-based organisations as well as a systematic document analysis of privacy protection policies from countries with recently updated regulations following GDPR in 2018.

3.8.1 Secondary data

Secondary data include data that have previously been collected and analysed for a different purpose, but which could provide a useful source for some aspects of a new study (Saunders et al., 2009). The utilisation of secondary data requires the researcher to examine a variety of sources, published or unpublished, such as government publications, journals, newspapers, books, magazines as well as business and industry reports (Kothari, 2004). There are a number of elements to consider, as advised by Walliman (2011) when assessing secondary data sources.

These elements include the quality of the evidence provided, the validity of arguments presented, the author(s) reputation and qualifications as well as comparisons of different data sources. Additionally secondary data should be reliable, suitable and adequate for purpose (Kothari, 2004; Walliman, 2011). There are pros and cons to weigh up, Saunders et al. (2009) observe when it comes to using secondary data.

One key advantage of secondary data is its effectiveness where resources, such as time and money, are limited (Bhattacharjee, 2012). Nevertheless, not all secondary data may be fit for the purpose of a researcher's study as it may have been collected as primary data for something else (Saunders et al., 2009).

3.8.2 Document analysis

Reviewing or evaluating of printed or electronic documents using a systematic procedure can be termed document analysis (Bowen, 2009). Impartial and consistent analysis of policies are facilitated by applying document analysis (Wach, 2013) in order to "elicit meaning, gain

understanding and develop empirical knowledge” (Bowen, 2009:27). Research that involves investigating the nature and source of an issue can employ document analysis to assess “what lies behind and within” a document, specifically documents related to policies (Cardno, 2019:625).

To guard against bias, Gross (2018:380) notes that document analysis can be used in conjunction with other data sources, such as interviews, to “corroborate or refute, elucidate, or expand on findings”. However, document analysis can also be used as a singular method in qualitative studies that only rely on analysing documents, for example, historical research (Bowen, 2009).

3.8.3 Primary data

Primary data relate to data that have been collected specifically for the purpose of the study being undertaken (Kothari, 2004). Primary data can be collected using methods such as observation, questionnaires and interviews, further discussed below (Saunders et al., 2009).

3.8.3.1 Observation

Before selecting observation as a data collection technique, the researcher needs to consider what the key interest areas are, what is to be observed, and why, in the researcher’s mind, the data required will be produced via observation (Bell, 2005). Observation essentially pertains to the “systematic observation, recording, description, analysis and interpretation” of human behaviour (Saunders et al., 2009:288). Observation is a data collection method that can be utilised in both quantitative and qualitative studies, though is more frequently used in the latter. Techniques include participant and direct observation (Flick, 2009; Bhattacharjee, 2012; Sani CIn, 2013).

3.8.3.1.1 Participant observation

Participant observation involves the researcher becoming fully immersed in the daily affairs of participants to gain insights into the activities and interactions of, and amongst subjects in their environment or setting of interest (Hammond & Wellington, 2013). Participant observation requires prolonged immersion, on the part of the researcher or observer, in order to extract meaningful data about subjects’ behaviour in their surroundings (Bryman, 2012). Inevitably, the researcher or observer becomes a member of the “group, organisation or community” under observation to share in their experiences and obtain an understanding of their lives (Kothari, 2004; Saunders et al., 2009:289).

3.8.3.1.2 Direct observation

During direct observation, the researcher has very little involvement in the occurrence under scrutiny and merely acts as an impartial or neutral observer (Bhattacharjee, 2012). The objective of the researcher or observer is to obtain a “detached view” of occurrences by appearing “invisible” in activities in given circumstances (Walliman, 2011:100). Direct observation, according to Sani Cln (2013) is the preferred choice of researchers for recording human behaviour as it encompasses comprehensive logging of actions, activities, and the context surrounding the activities and actions.

3.8.3.2 Questionnaires

Questionnaires are data collection tools commonly employed in a survey strategy and generally used to obtain quantitative data (Saunders et al., 2009; Walliman, 2011). The main type of questions are factual in nature, such as the respondent's age and gender or opinion questions related to the respondent's viewpoints and prejudice (Sani Cln, 2013). Questionnaires, according to Walliman (2011) can be delivered through the internet, in person, or using mail services. The types of questions a questionnaire can incorporate, Phillips and Stawarsk (2008) list as:

- Open-ended questions that allow respondents to fill in blank spaces with responses.
- A checklist that has a number of responses listed and participants check those that are applicable.
- Two-way questions that require respondents to choose between two possible responses, for instance no or yes.
- Multiple-choice questions that allow respondents to choose the most applicable answer from a number of options available.
- Ranking scale type questions in which the respondent is required to list items in order of importance.

The aim of a questionnaire is to capture participants’ responses in a standardised fashion and the general form of the questionnaire can be either structured or unstructured (Bhattacharjee, 2012).

3.8.3.2.1 Structured questionnaires

Structured questionnaires consist of “definite, concrete and pre-determined questions”, or “fixed questions, batteries of questions, tests (e.g. psychological) and/or scales” which are presented in the same order and wording to all respondents with pre-coded choices of response (Kothari, 2004:101; Bowling, 2005:204). Thus, a structured questionnaire provides respondents with a set of response options which can be easily collated by the researcher for

analysis (Bhattacharjee, 2012). Structured questionnaires are fairly simple and inexpensive to administer and analyse. On the other hand, it can be limited by the fact that respondents are not able to elaborate in their own words. In these situations unstructured questionnaires would be more appropriate (Kothari, 2004).

3.8.3.2.2 Unstructured questionnaires

Unstructured questionnaires provide respondents with the freedom to express their views in response to open-ended questions (Walliman, 2011; Bhattacharjee, 2012). Responses are given in textual statements that describe problems and the respondents' opinions, thus providing the researcher with rich and meaningful data (Adams et al., 2014). Primarily, questionnaires are utilised in studies of fairly large groups due to its efficiency and are therefore more likely to be structured rather than unstructured (Anastas, 1999).

Exploratory research and studies that, to a greater extent, require open-ended questions will not benefit from the use of questionnaires. Thus, questionnaires are most often used in explanatory or descriptive research (Saunders et al., 2009). This study employed an exploratory approach to investigate the research phenomenon and collect empirical data through the use of semi-structured interviews.

3.8.3.3 Interviews

Prominent in both quantitative and qualitative studies, is the research interview which involves the researcher, through a series of questions and answers, exploring the experiences of informants and the meanings the informants attach to these experiences (Bryman, 2012; Grosseohme, 2014). Interviews, according to Bhattacharjee (2012) and Saunders et al. (2009:318) are the most frequently used data collection technique in interpretive research, facilitating the collection of "valid and reliable data" in relation to the study's aims and research questions. Interviews can be conducted either via the telephone, face-to-face, or using video-conferencing, hosted on digital platforms such as Skype or Zoom (Anastas, 1999; Leavy, 2017). The subjective experience of the interviewee also comes into focus in the latter two techniques, thus enabling the interviewer to capture physical and emotional reactions (Krishnaswami & Satyaprasad, 2010). According to Phillips and Stawarsk (2008) a successful interview process involves the following key steps.

- Development of the questions
- Testing of the interview
- Interviewer(s) preparation
- Clear instructions should be given to the interviewees
- Interviews should be scheduled

By employing structured, unstructured or semi-structured interviews, the researcher can pose general questions on a specific topic as well as guide subjects on communicating the issues of interest (Carter & Henderson, 2005).

3.8.3.3.1 Structured interviews

Structured interviews are typically used in survey research where descriptive and relational studies are required for a general portrayal of a population or situation (Anastas, 1999; Bryman, 2012). Structured interviews involve administering an interview schedule by asking, without deviation, a pre-established and identical set of questions and recording the answers using pre-coded or closed format responses (Saunders et al., 2009). Thus, the standardisation of the questions and answers lead to error reduction and greater accuracy (Bryman, 2012). Due to the tightly scripted nature of the structured interview, it is referred to as a spoken or interview-administered questionnaire and is often used in the collection of quantifiable data (Rugg & Petre, 2007). Compared to the structured interview method, Saunders et al. (2009) remark that unstructured interviews are non-standardised and far less rigid in nature.

3.8.3.3.2 Unstructured interviews

Unstructured interviews encompass informal discussions in which the interviewer has little or no control over the responses of the participants. This enables freedom of expression which allows the participants to set the pace of the interview (Russell, 2006). In unstructured interviews, there is no pre-established set of questions. Yet, the researcher has a clear idea of themes to explore (Saunders et al., 2009). Unstructured interviews allow for the collection of rich data, especially in studies related to history and journalism to which the researcher might return several times to build and record a picture of the interviewee's life and experiences (Carter & Henderson, 2005). Consequently, employing unstructured interviews might be quite time-consuming and lack comparability between interviews. Thus, data analysis can be a lot more difficult (Kothari, 2004). In circumstances where the researcher has only one opportunity for an interview, it is advisable to utilise semi-structured interviews (Russell, 2006).

3.8.3.3.3 Semi-structured interviews

Semi-structured interviews offer a flexible middle point between structured and unstructured interviews which enable the interviewer to adapt the interview process based on the participants' responses (Palić et al., 2015). A range of topics or various lines of questioning to detailed open-ended questions as well as potential follow-up questions are listed in an interview guide which aims to steer the researcher during the interview (Grossoehme, 2014; Leavy, 2017). The interviewer can move the proposed order of the questions around, omit

some questions, or add questions; as a result, a semi-structured approach provides a common framework with a flexibility in layout and implementation (Brown & Hale, 2014). Semi-structured interviews are advisable in cases where efficient use of time is required and the researcher is expected to exercise a level of control intermingled with a degree of leeway (Russell, 2006).

Adapting the semi-structured interview format, this researcher designed a series of questions formulated to address the research objectives, and captured it in an interview guide (Appendix E). All interviews took place on a digital video conferencing platform because of the health restrictions as a result of the pandemic. The data collection period spanned between July and September 2021, due to the availability of participants and scheduling challenges. Following the completion of data collection, this researcher proceeded to analyse the data using the thematic analysis technique presented in the following section.

3.9 Data analysis

Following the collection of data, this researcher was required to process and analyse the data to determine the findings (Leavy, 2017). The researcher, through methods such as “coding, annotating, labelling, selection and summary”, drilled down to specific pieces of data which were deemed significant to the purpose of the study (Kothari, 2004; Blaxter et al., 2010:229). Thus, the dissecting, sense-making and finding meaning from the data can be termed data analysis (Creswell & Creswell, 2018). Popular qualitative research approaches to the analysis of empirical data include content analysis and thematic analysis (Vaismoradi et al., 2016).

3.9.1 Thematic analysis

Allowing for the emergence of categories from the data, thematic analysis can be applied to most qualitative research (Saldaña, 2009). According to Braun and Clarke (2006:79) thematic analysis involves “identifying, analysing and reporting patterns (themes) within data”. Therefore, a theme can be seen as an encompassing label or descriptor for a “group of repeating ideas” that facilitates the answering of research questions (Vaismoradi et al., 2016:101). The six stages of thematic analysis identified by Braun and Clarke (2006), are described in Table 3.3.

Table 3.3: The phases of thematic analysis (Braun & Clarke, 2006:87)

Phase	Description
1. Familiarizing yourself with your data	Transcribing data (if necessary), reading and re-reading the data, jotting down initial ideas.
2. Generating initial codes	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.
3. Searching for themes	Collating codes into potential themes, gathering all data relevant to each potential theme.
4. Reviewing themes	Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic 'map' of the analysis.
5. Defining and naming themes	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells, generating clear definitions and names for each theme.
6. Producing the report	Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back to the analysis of the research question and literature.

The approach in the above-mentioned table involves an “iterative and reflective process” that requires going back and forth through the phases (Nowell et al., 2017:4).

3.10 Ethics

The ethics of research, Saunders and Lewis (2012:74) define as: “the appropriateness of the researcher’s behaviour in relation to the rights of those who become the subject of a research project or who are affected by it”. The participants’ privacy, confidentiality and anonymity were guaranteed in this study, by following the guidelines set out by the Cape Peninsula University of Technology (CPUT) which are:

- **Privacy:** The participants’ audio recordings, responses and interview notes were only used for the purpose of this study and only the researcher had access to them.
- **Confidentiality:** The researcher employed steps such as utilising password-protected recording and storage devices to ensure that subjects’ personal information was kept confidential and limiting the risk of exposing participants’ identities.
- **Anonymity:** The subjects’ anonymity was preserved through the use of pseudonyms.

The following issues forming part of the ethics approval process of this study as requested by the FID of the CPUT were addressed as:

- **Protection of people:** The research process and objectives were fully communicated with intended participants and free from pressure or coercion. Participants were given the opportunity to consent freely or refuse to participate. The confidentiality of research participants was maintained, and subjects’ anonymity was preserved through the use of pseudonyms. The identity or comments from participants would not be divulged without their written permission. Participants had the prerogative to decline responding to

questions they were not comfortable with as well as the right of removal from the research at any time.

- **Informed consent:** Each participant was required to complete an informed consent form before participation in this study. All participants were made aware of:
 - The nature of the study including its aims and objectives
 - The right to decline participation
 - The measures put in place to safeguard the data
 - The right to request turning off recording device
 - The right to make enquiries or clarify questions
- **Observation and records:** Audio recordings of participants' responses were made during the interview process. The recording devices included an online voice recorder and a smartphone as back-up in the event of any technical difficulties with the primary device. The devices were password-protected by the researcher who had sole access to the audio recordings and were backed up in a secure remote cloud storage.
- **Data storage:** The data collected in the research were stored on a password-protected USB, with the researcher having sole access to the data. Hard copies, for example, interview notes were securely locked away and only accessed by the researcher. Before storage, the data were anonymised to protect the identity of the participants. Any identifying data were stored separately and were password-protected.

Participants were given an opportunity to review this information to determine their participation, devoid of pressure or coercion. After confirmation of their full understanding of the process, all participants were required to sign the consent form prior to data collection.

Upon satisfaction of the ethical requirements laid out by the FID, clearance was provided to commence data collection (Appendix A).

3.11 Summary

In this chapter, the research methodology was presented, including the research philosophy, research approach, research design, research strategy, sampling, data collection and analysis as well as the ethical considerations.

The first part of the chapter provided an overview of research philosophy, the ontological and epistemological considerations. In terms of the study, a subjectivist ontological stance was taken to explore the phenomenon based on the participants' point of view and experience and an interpretivist epistemological approach was adopted to investigate and comprehend the subject of the study and interpret the findings.

Next, the approaches to the study were explored. The development of theories is generally dictated by inductive or deductive reasoning. An inductive approach was followed to formulate a new theory through the observation of the phenomenon. In addition to that, an exploratory case study design was adopted to understand and explore the phenomenon.

The study employed non-probability, purposive sampling to select fifteen participants, based on the researcher's judgement, who were best positioned to provide insightful information on the factors affecting the governance of data privacy in IoT environments in South African organisations. The unit of analysis included selected IoT-based organisations in South Africa and the unit of observation included high-level executives in the organisations.

After obtaining permission from the fifteen participants, primary data were collected virtually, using semi-structured interviews. The study also collected secondary data from the document analysis of recently updated privacy protection policies of ten countries between 2018–2021. Subsequently, the data collected from both data sources were analysed by applying a thematic analysis technique to extract the common themes and draw findings from the data.

The chapter concluded with an explanation of the ethical considerations taken into account to preserve the privacy, confidentiality and anonymity of the participants of the study.

In the following chapter, the details on how the data were analysed using the steps discussed in this chapter and the subsequent emergent findings, in relation to the research questions are presented.

CHAPTER FOUR: ANALYSIS AND FINDINGS

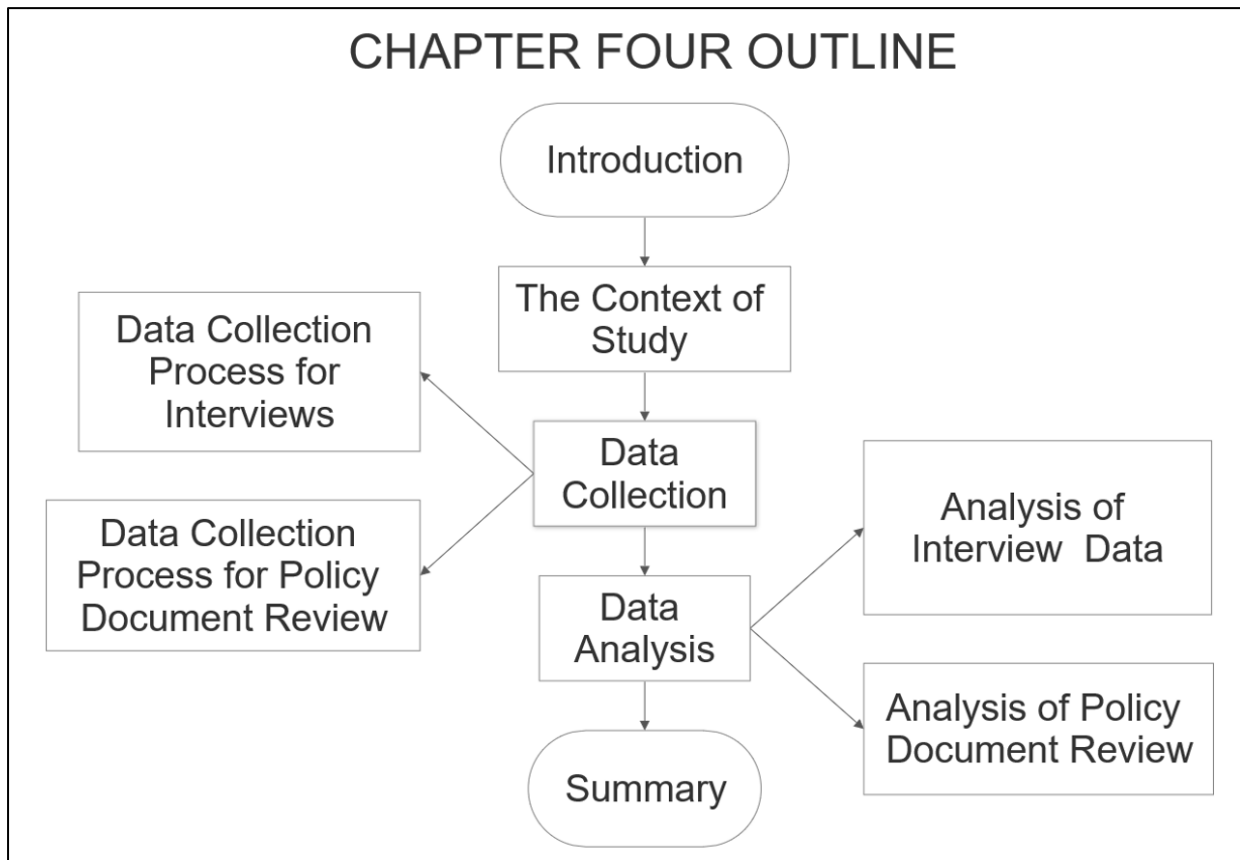


Figure 4.1: Chapter Four outline

4.1 Introduction

This chapter focuses on the analysis of the data obtained through semi-structured interviews of fifteen IoT-based organisations across four of the provinces in South Africa as well as the document analysis of updated data protection legislation across the following regions: Europe, North America, Asia-Pacific, Central and South America, the Caribbean, the Middle East and Africa.

Data obtained from the interviews and document analysis were subjected to a systematic thematic analysis process and emergent findings were presented in descriptive narrative format. This chapter is divided into four sections as displayed in Figure 4.1 and section 4.2 focuses on the context of the study. Section 4.3 describes the data collection process for the interview and policy documents, section 4.4 presents the data analysis of both the interviews and policy documents and the chapter concludes with the summary in section 4.5.

The problem statement, research questions, research objectives and research aim are repeated here for ease of reference.

4.1.1 Problem statement

There is no defined holistic framework of best practices and guidelines for the governance of data privacy in IoT environments in South Africa.

4.1.2 Research questions

RQ: How can data privacy governance be implemented in IoT environments in South Africa?

SQ1.1: What are the factors affecting data privacy regulation in IoT organisations in South Africa?

SQ1.2: How knowledgeable are South African organisations of existing local and international data privacy legislations in relation to IoT environments?

SQ1.3: What are the best practices for the governance of data privacy in IoT environments?

SQ1.4: How can a data privacy governance framework for IoT organisations in South Africa be developed?

4.1.3 Research objectives

The objectives of the research are:

- i. To determine the factors affecting data privacy regulation in IoT-based organisations in South Africa.
- ii. To establish the knowledge of South African organisations of local and international data privacy legislation in relation to IoT environments.
- iii. To determine existing best practices for the governance of data privacy in an IoT environment.
- iv. To develop a framework of guidelines for governing data privacy in IoT environments in South Africa.

4.1.4 Research aim

The aim of this study is to explore the factors for the governance of data privacy regulation and compliance for connected environments, with a view to develop a framework of guidelines and best practices for governing data privacy in IoT environments in South Africa.

4.2 The context of study

The research was conducted in South Africa, a country on the southern tip of Africa. The country is divided into nine provinces (North West, Western Cape, Northern Cape, Eastern

Cape, Mpumalanga, Gauteng, Free State, KwaZulu-Natal, Limpopo), each with its own Legislature, Premier and Executive Council (South African Government, 2021). There are three capitals in South Africa, namely Cape Town in the Western Cape, Bloemfontein in the Free State and Pretoria in Gauteng (South African Government, 2021). The third largest economy in Africa, South Africa has been characterised as having widely developed industries and infrastructure, as being technologically advanced and boasting a diversified economy (The Department of Trade and Industry, 2020; Varrella, 2021). South Africa has the continent's largest stock exchange, the Johannesburg Stock Exchange (JSE), is a large exporter of natural resources such as gold and platinum, and has established "financial, legal, communications, energy, and transport" industries (The Heritage Foundation, 2020:380). In comparison to the rest of Africa, South Africa has the largest information and communications technology (ICT) market, boasting sophisticated leadership security and mobile software, as well as electronic banking services (International Trade Administrator, 2021).

4.3 Data collection

For this study, the data collection process was divided into two parts which involved the collection of data through interviews and a review of policy documents. The initial part of the data collection process which involved the interviews is presented firstly and is subsequently followed by the data collection process for the policy documents.

4.3.1 Data collection process for interviews

This section covers the data collection process for the interviews and is divided into the case of the study and the participants of the study.

4.3.1.1 The case of the study

The participating organisations were distributed across four provinces, namely the Western Cape, Eastern Cape, KwaZulu-Natal and Gauteng. One of the organisations had operations in all four provinces and two had a presence in Canada and Australia, respectively. Two of the organisations operated mostly in a virtual capacity, but have head offices in Johannesburg. The distribution of organisations across the provinces in South Africa is illustrated in Figure 4.2.

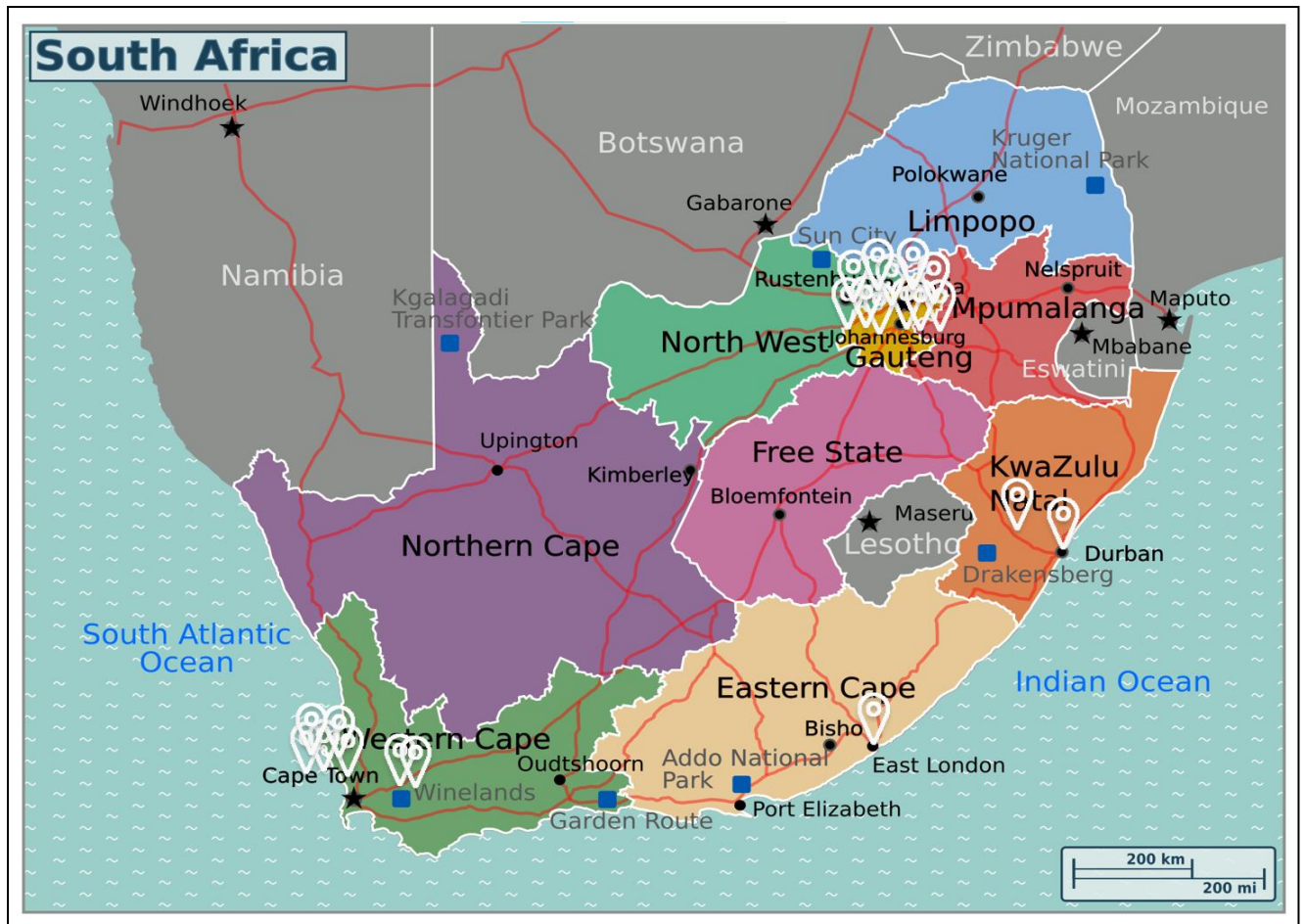


Figure 4.2: Distribution of IoT-based organisations across South Africa

The Western Cape included five participating organisations in the capital city of Cape Town and two were located in Stellenbosch. In the Eastern Cape, only one organisation had an operation in East London. KwaZulu-Natal comprised of one enterprise in Durban and one in Pietermaritzburg. However, the majority of the organisations had a presence in Johannesburg.

Seven of the fifteen organisations operated in the Information Technology and Service sector, two in the Telecommunications sector, two in Cyber Security and Risk Management, one in Computer Software, one in Tracking and Fleet Management, one in Renewables and Energy and one in Tracking, Design and Development. A brief overview of each organisation represented in the study can be found in Table 4.1. In adherence to privacy and to preserve anonymity, the names of the organisations have been replaced by a letter of the alphabet, e.g., Organisation A is presented as OA, etc. The business sector, number of years in operation, number of employees and how they facilitate the use of IoT are included, in the order specified, below:

Table 4.1: Brief overview of each organisation

Organisation	Overview
OA	- Information Technology and Services - Five years in operation - Two to ten employees - Facilitates the use of IoT through the building of information gathering systems in which key elements can be actioned back to the operation
OB	- Telecommunications - Five years in operation 22 employees - Facilitates the use of IoT by providing network access and coverage for IoT solutions and operators throughout South Africa
OC	- Telecommunications - Five years in operation 150 employees, of which seven are solely focused on IoT - Facilitates the use of IoT through the development of hardware, firmware and software, as well as providing turnkey solutions to end customers
OD	- Information Technology & Services - Twenty-four years in operation 30 employees - An enterprise IoT enablement organisation that facilitates companies in having IoT solutions
OE	- Information Technology & Services - Sixteen years in operation, but involved in IoT for five years 60 core employees - Facilitates the use of IoT through the creation of solutions such as track-and-trace, water metering and precision agriculture
OF	- Information Technology & Services - Six years in operation - Eight employees - Facilitates the use of IoT through utility management using smart devices such as energy and water meters
OG	- Information Technology & Services - Three years in operation 35 employees - Facilitates the use of IoT through the product lifecycle and the management of data flow in IoT solutions
OH	- Information Technology & Services - Fourteen years in operation 50–60 employees - Facilitates the use of IoT through systems integration and hardware development
OI	- Computer Software - Twelve years in operation 27 employees - Facilitates the use of IoT through data acquisition, analysis and dissemination
OJ	- Tracking, IoT Design & Development - Five years in operation - Four employees - Facilitates the use of IoT through the design and development of tracking devices
OK	- Renewables and Energy - Fourteen years in operation 10 employees - Facilitates the use of IoT through design, development and maintenance of systems
OL	- Cyber Security & Risk Assessment - Two years in operation - Contracted structure, no full-time employees - Security risk assessment and management for IoT environments and IT
OM	- Information Technology and Services - Three years in operation - Eight employees - Facilitates the use of IoT through data acquisition, analysis and dissemination
ON	- Tracking, Fleet Management & Utility Monitoring - Fourteen years in operation - Five employees

OO	▪ Utilises IoT for tracking and monitoring
	▪ Cyber Security & Risk Assessment ▪ Five years in operation ▪ Ten employees ▪ Security risk assessment and management for IoT environments and IT

In accordance with the classification of the South African government found in the National Small Enterprise Act, the size of the organisations ranged from micro to medium organisations, with a corresponding employment work force of 1–10 to 50–251 as indicated in Table 4.2 (Government Gazette, 2019).

4.3.1.2 The participants of the study

To answer the research questions posed by the study, fifteen participants were interviewed. The selected participants comprised of high-level executives from organisations based in four of the provinces in South Africa.

As per the information provided by the participants, the profiles of the participants were further expanded in relation to the organisations in Table 4.2 which contains the participants' roles and responsibilities, sector, size of the organisation and location. The names of the participants have been replaced by a number to maintain anonymity, for example, Participant 1 is presented as P1; etc. and P6 is represented as a joint interview with two participants.

Table 4.2: Participant classification

Organisation	Interview Participant Number	Roles	Responsibilities	Sector	Enterprise Size	Location
OA	P1	CEO and Co-Founder	Marketing, setting strategy, defining direction, and getting investment and funding	Information Technology and Services	1-10 (Micro)	Johannesburg
OB	P2	Executive: Solutions and Innovations	Assisting customers from the technical perspective to integrate into the network	Telecommunications	11-50 (Small)	Centurion
OC	P3	IoT Technology Consultant	Systems Integration	Telecommunications	51-200 (Medium)	Johannesburg, Canada
OD	P4	Internal Systems Co-Ordinator	Network management	Information Technology and Services	11-50 (Small)	Cape Town, Johannesburg

OE	P5	Chief Digital Officer	Designing and development of firmware, building of IoT platforms	Information Technology and Services	51-200 (Medium)	Johannesburg, Durban, East London, Cape Town
OF	P6: (Joint Interview)	Interim CEO	Involved in all aspects of business	Information Technology and Services	1-10 (Micro)	Stellenbosch
		Intern	Operations, finance and legal			
OG	P7	Platform Co-Ordinator	Value proposition for digital transformation for our AI system	Information Technology and Services	11-50 (Small)	Virtual Office, Gauteng
OH	P8	Production Director	Overseeing production and new technology	Information Technology and Services	11-50 (Small)	Cape Town, Johannesburg, Australia
OI	P9	Chief Technology Officer	Responsible for all the developers and technological direction	Computer Software	11-50 (Small)	Stellenbosch
OJ	P10	CEO	Prototype Designing	Tracking, IoT Design and Development	1-10 (Micro)	Pietermaritzburg
OK	P11	Founder and CEO	Involved in all aspects of business	Renewables and Energy	1-10 (Micro)	Johannesburg, Australia, USA
OL	P12	CFO and COO	Operations and finance	Cyber Security and Risk Assessment	Contracted Structure	Virtual, Johannesburg
OM	P13	Co-Founder and CEO	Sales, development and innovation	Information Technology and Services	1-10 (Micro)	Johannesburg
ON	P14	Founder	Sales and solution implementation	Tracking, Fleet Management & Utility Monitoring	1-10 (Micro)	Cape Town
OO	P15	Founder Member and Director	Product and software development , Strategic direction	Cyber Security and Risk Assessment	1-10 (Micro)	Cape Town, Gauteng, Canada

4.3.1.3 The interview process

The data were collected over a period of three months via semi-structured interviews of fifteen participants. Due to the global pandemic, Zoom (an online video conferencing application) was used to conduct the interviews which ranged from between 30 to 45 minutes. The interview schedule (Appendix E) consisted of three sections. The first two sections pertained to participant and company information and the third section contained the fifteen interview question and seven possible follow-up questions.

4.3.2 Data collection process for policy document review

The document analysis process employed a series of systematic steps geared towards collecting relevant and valid data. A reduction in irrelevant data collection and systematic document selection can be achieved by setting inclusionary criteria, such as a time frame or document age (Gross, 2018). Policy documents pertaining to data protection from countries that have updated their regulations between years 2018–2021 were selected and analysed using the thematic analysis technique. Following an internet search, a total of twenty-five countries with updated policies were found as listed in Table 4.3. The countries were grouped under the following regions: Europe, North America, Asia-Pacific, Central and South America, the Caribbean, the Middle East and Africa.

To ensure a systematic approach to final document sample selection, exclusionary criteria are essential for narrowing the list (Gross, 2018). For this study, policy documents from countries without an English version, at the time of the online search, specifically, policy documents from Serbia, Kosovo, China, Panama, Bahrain, Algeria, the Republic of Congo and Togo were excluded. The remaining seventeen documents were further filtered for the following reasons.

- The UK GDPR offered similar provisions as the EU's GDPR, with minimal modifications following the UK's withdrawal from the EU. In addition to that, the UK's Data Privacy Act 2018 only establishes the conditions for processing personal information for law enforcement and intelligence service as well as enforcement procedures.
- Israel's updated regulation only pertained to data security in databases.
- The Cayman Islands and Barbados were excluded as the Caribbean was already presented by the British Virgin Islands.
- Zambia, Uganda and Nigeria were excluded as Africa was already represented by Egypt, Kenya and South Africa that presented more comprehensive policy documents.

The policy documents from the subsequent ten countries, highlighted in Table 4.3, were selected for analysis. These are inclusive of the EU, San Marino, USA, South Korea, New Zealand, Brazil, British Virgin Islands, Egypt, Kenya and South Africa. Where reference is made to 'countries' in respect of the analysis within this section and subsequently in Chapter Five, it will be inclusive of the EU, unless otherwise specified. The responsibility for the protection of privacy in the USA is not as straightforward as an all-encompassing regulation due to the government structure, however various states have enacted privacy policies in relation to consumer privacy (Green, 2021). Therefore, in this study the USA was represented by the California Consumer Privacy Act (CCPA) which falls under the selection criteria of this study.

Table 4.3: List of countries with updated data protection legislation 2018–2021

Year	Country	Name of Legislation	Link	Notes
Europe				
2018	Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden	General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679	
2018	San Marino	Law No. 171 of 21 December 2018, Protection of Natural Persons with Regard to the Processing of Personal Data (the Law)	https://www.dataguidance.com/sites/default/files/law_21_december_2018_no._171_en.pdf	
2018	UK	United Kingdom General Data Protection Regulation (UK GDPR)	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/969514/20201102_-_GDPR_-_MASTER_Keeling_Schedule_with_changes_highlighted__V4.pdf	The UK GDPR offers similar provisions as the EU's GDPR, with minimal modifications and came into effect after Brexit.
2018		Data Protection Act 2018 (the Act)	https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf	The Act sets out the conditions for processing personal information for law enforcement and intelligence service, as well as enforcement procedures.
2018	Serbia	Law on Protection of Personal Data 2018 (the Law)		Unable to find English version
2019	Kosovo	Law No. 06/L-082 on Personal Data Protection (the Law)		Unable to find English version
North America				
2020	USA	California Consumer Privacy Act (CCPA)	https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375	

Asia-Pacific				
2020	South Korea	Personal Information Protection Act 2011 (as amended in 2020) (PIPA)	https://elaw.klri.re.kr/kor_service/lawView.do?hseq=53044&lang=ENG	Unofficial English translation; Included as it was extensively updated in 2020
2020	New Zealand	Privacy Act 2020 (the Act)	https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html#LMS23479	
2021	China	Personal Information Protection Law (PIPL)		Unable to find English version, effective as of 01/11/2021
Central & South America				
2020	Brazil	Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019) (LGPD)	https://www.dataguidance.com/sites/default/files/lgpd_translation.pdf	
2021	Panama	Law No. 81 on Personal Data Protection 2019 (the Law)		Unable to find English version
The Caribbean				
2021	British Virgin Islands (BVI)	Data Protection Act, 2021	https://eservices.gov.vg/gazette/sites/eservices.gov.vg.gazette/files/newattachments/Act%20No.%203%20of%202021-Data%20Protection%20Act,%202021.pdf	
2021	Cayman Islands	The Data Protection Act (2021 Revision) (the Act)	https://ombudsman.ky/images/pdf/laws_regs/Data_Protection_Act_2021_Rev.pdf	Included as it was extensively updated in 2020
2021	Barbados	Data Protection Act 2019 (the Act)	https://gisbarbados.gov.bb/download/data-protection-act-2019/	
The Middle East				
2018	Israel	Privacy Protection Regulations (Data Security), 5777-2017	https://iapp.org/media/pdf/resource_center/IS-PROTECTION-OF-PRIVACY-REGULATIONS.pdf	This update pertains to data security in databases
2019	Bahrain	Law No. 30 of 2018 with respect to Personal Data Protection (PDPL)		Unable to find English version

Africa				
2019	Kenya	The Data Protection Act, 2019 (the Act)	http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf	
2021	South Africa	The Protection of Personal Information Act 4 of 2013 (POPIA)	https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf	
2020	Egypt	Personal Data Protection Law No.151 of 2020 (the Law)	https://www.acc.com/sites/default/files/program-materials/upload/Data%20Protection%20Law%20-%20Egypt%20-%20EN%20-%20MBH.PDF	
2021	Zambia	Data Protection Act No. 3 of 2021 (Data Protection Act)	https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%203%20The%20Data%20Protection%20Act%202021_0.pdf	
2019	Uganda	Data Protection and Privacy Act, 2019 (Act)	https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf	
2019	Nigeria	Nigeria Data Protection Regulation 2019 (NDPR)	https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf	
2018	Algeria	Law No. 18-07 of 25 Ramadhan 1439 Corresponding to June 10, 2018, Relating to the Protection of Individuals in the Processing of Personal Data (the Law)		Unable to find English version
2019	Republic of Congo	Law 29-2019 on the Protection of Personal Data (the Law)		Unable to find English version
2019	Togo	Law No. 2019-014 Relating to the Protection of Personal Data		Unable to find English version

4.4 Data analysis

For this study, the data analysis was divided into two parts which involved the analysis of policy documents and interview transcripts. The initial part of the data analysis which involved the interviews is presented first and subsequently followed by the analysis of the policy documents.

The research followed the principles of thematic analysis which involves the six phase process shown in Table 4.4 for the identification, analysis and reporting on patterns or themes that emerged from the accumulated data (Braun & Clarke, 2006).

Table 4.4: The phases of thematic analysis (Braun & Clarke, 2006:87)

Phase	Description
1. Familiarizing yourself with your data	Transcribing data (if necessary), reading and re-reading the data, jotting down initial ideas. ▪ The step of transcribing data was applied only to the interview audio data, given that the policy documents were already in textual form. Both data sets were read multiple times to familiarise with the content.
2. Generating initial codes	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code. ▪ Following the upload of each transcript into ATLAS.ti, the coding process began by identifying and coding the key concepts descriptively.
3. Searching for themes	Collating codes into potential themes, gathering all data relevant to each potential theme. ▪ Next, all the identified codes were collated into categories by assessing the common thread in each code and grouping similar codes under one category and assigning a descriptive label.
4. Reviewing themes	Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic 'map' of the analysis. ▪ Following the initial identification of categories, several iterations of the process were completed to arrive at the final ten categories.
5. Defining and naming themes	Ongoing analysis to refine the specifics of each theme and the overall story the analysis tells, generating clear definitions and names for each theme. ▪ Using Microsoft Excel functions on the data, the categories and corresponding extracts were filtered and classified according to developing relationships and patterns, to produce the emergent themes.
6. Producing the report	Selection of vivid, compelling extract examples, final analysis of selected extracts, the relating back of the analysis to the research question and literature. ▪ The descriptive findings were presented based on the data analysed. The subsequent findings were presented in relation to the research sub questions and the interview questions. For the document analysis, the findings were presented under each of the emergent themes. The findings from both datasets were also mapped to the components of the activity theory.

4.4.1 Analysis of interview data

Following the collection of data from participants using semi-structured interviews, an automatic transcription tool called, Otter.ai was used to transcribe the audio files. Each of the interview transcriptions were reviewed by the researcher to ensure that responses were captured accurately and to obtain a thorough overview and understanding of the collected data. Once the researcher had corrected the few errors and was satisfied with the accuracy of the transcripts it was subsequently exported into a Microsoft Word document (MS doc).

4.4.1.1 Generating codes and categories

After the exportation of the transcribed data into a MS doc, the transcripts were uploaded into ATLAS.ti, a qualitative data analysis computer software package developed to manage the coding process (Paulus, 2018). Following the upload of each transcript, the coding process began by identifying and coding the key concepts descriptively as depicted in Figure 4.3 which is a snapshot from a participant's response. This identification and coding process was applied systematically for each participant's transcribed response which rendered seventy-seven codes.

Researcher Yeah. So starting with the first question, how would you describe the current situation of data breaches that are affecting South African organizations? Participant 2 Well, yeah, so I mean, there's a locally reported one recently. Well, I mean, every now and again you do hear of large companies losing, well databases being leaked, your high profile cases, both locally and globally. Yeah, data bre...so data security, I think, is something that's becoming more and more focus for the organization, on every level. So in terms of IoT, I think there's a large focus on the devices when it comes to data breaches. We have heard of, you know, things like thermometer in casinos are being used to hack into that casino's core network. So, there is a lot of responsibility on the part of the device makers to ensure their devices are secure. But still, I believe that the vast majority of data breaches are not on the device side. It comes through other avenues, there's the applications, there's the backend infrastructure, there's even the people within the organization who perhaps aren't trained correctly, don't have the correct email policies or the correct antivirus support for that organization. If you think of some of the big high profile breaches, it's been from people within the organization opening emails. There's a million IoT devices out there, but it just takes one person for that breach. So that's really the holistic kind of approach. I don't think anybody's got 100% right, but certainly, if your company isn't taking it seriously, then I think it's a matter of time before you do feel the effects of that the negative effects of that.	5:29... 5:13... db: upsurge in data breaches 5:14... ppi: increased focus on data se... 5:18 fo... iot: focus of data breaches in IoT 5:20 IQ2 Res... sec: responsibility for securing... 5:21 IQ2 Res... sv: vulnerable processes in org... 5:21 IQ2 Res... cspt: culpability within organisa...
---	--

Figure 4.3: Example of initial codes generated

The next step involved collating all the identified codes into categories. This was done by assessing the common thread in each code and grouping similar codes under one category and assigning a descriptive label, for example, "Challenges of Securing Personal Information (CSPI)". Once the categorisation process was complete, all the codes in the category were colour-coded and assigned a prefix (for use in ATLAS.ti) as displayed in Figure 4.4. Following the initial identification of categories, several iterations of the process were completed to arrive at the final ten categories, also shown in Figure 4.4.

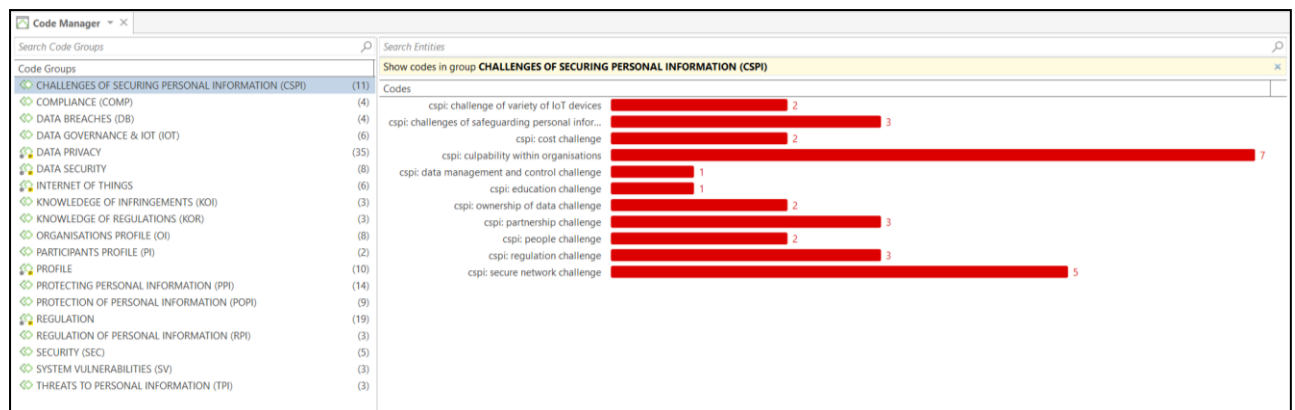


Figure 4.4: Example of generating categories and potential themes

Subsequently the codes, categories and relating extracts from the responses were exported into Microsoft Excel in order to further explore the common relationships and patterns leading to the development of the themes.

4.4.1.2 Generating themes

The application of Microsoft Excel functions to the data, visible in Figure 4.5, allowed for the categories and corresponding extracts to be filtered and classified according to developing relationships and patterns to produce the emergent themes. Following a similar iterative process to that of identification, coding and categorisation, the categories were further grouped into five overarching themes.

Interview Question (IQ)	Participant	Response	Comment	Codes	Categories	Themes
Company Info: Q5_Response	Participant 9	I am the CTO, Chief Technology Officer. I'm responsible for all the developers and technological direction given the choices.		participant's role and responsibilities	Participant Profile	PROFILE
IQ2_Response	Participant 2	I believe that the vast majority of data breaches are not on the device side. It comes through other avenues, there's the applications, there's the backend infrastructure, there's even the		vulnerable processes in organisations	System Vulnerabilities	DATA SECURITY
IQ1_Follow-up Q_Response	Participant 9	I can see that there could be strategic advantage for some companies to try to breach security on South African companies		reason for data breaches	Data Breaches	DATA PRIVACY
Company Info: Q5_Response	Participant 6	I do a little bit of everything, whether it be putting ads up, or creating the social media profile to signing commercial contracts, or		participant's role and responsibilities	Participant Profile	PROFILE
IQ11_Response	Participant 9	the weakest part of all your systems will always be social engineering, where some employee somewhere gets convinced to let somebody in		people challenge	Challenges of Securing Personal Information	DATA PRIVACY
IQ4_Response	Participant 10	I don't know a[obscene language] lot about I'm going to be honest		knowledge of SA data privacy regulation	Protection of Personal Information	REGULATION
IQ15_Response	Participant 10	I don't know to be perfectly honest. All I can say there needs to be a framework because we've got more Google assistants. Sir's. And home automation, smart locks		establishing compliance of data privacy and regulatory laws	Compliance	REGULATION
IQ14_Response	Participant 8	I don't think it does. And I don't think it should, I think it should be all on the same level, you have one standard base that you work off, which just makes it more simpler for everybody		data privacy differentiation between IoT and conventional systems	Data Governance & IoT	INTERNET OF THINGS (IOT)
IQ11_Response	Participant 5	there will be a cost associated with compliance		cost challenge	Challenges of Securing Personal Information	DATA PRIVACY
Q5_Response	Participant 5	I don't think the PoPI Act clearly defines IoT devices yet because		PoPI and IoT	Data Governance &	INTERNET OF

Figure 4.5: Example of themes generated

The generated codes, categories and themes that emerged from the analysis of the interview data are presented in Table 4.5. The seventy-seven codes generated from the data analysis were grouped into ten categories and classified into five themes.

Table 4.5: Summary of generated codes, categories and themes

Codes	Categories	Themes
data breach insurance	Data breaches	DATA PRIVACY
reason for data breaches		
upsurge in data breaches		
using technologies to combat data breaches	Experience of infringements	
infringements experienced by organisation		
knowledge of infringements		
personal experience of infringements		
challenge of variety of IoT devices	Challenges of securing personal information	
challenges of safeguarding personal information		
cost challenge		
culpability within organisations		
data management and control challenge		
education challenge		
ownership of data challenge		
partnership challenge		
people challenge		
regulation challenge		
secure network challenge		
establishing compliance of data privacy and regulatory laws		Knowledge of regulations
GDPR compliance		
regulatory processes adopted from parent company		
SA data privacy compliance		
opinion of GDPR		
opinion of POPI		
opinion of global data privacy regulation	Regulation of personal information	
acceptance of POPI		
knowledge of SA data privacy regulation		
mechanism/protocols to fulfil POPI requirements		
POPI Act grey area		
POPI comparison to global privacy regulations		
POPI compliance training		
reaction to POPI Act		
reason for not collection unique identifiers		
remedying POPI Act in relation to IoT		
impact of global regulations		
impact of POPI on organisation		
approach for safeguarding personal information		
architectural oversight		
development of data transfer protocol		
end-to-end control		

honest about use of data	Security in IoT environments	DATA SECURITY
increased focus on data security		
layered protocol approach		
limited access to, and control of data		
mitigating threats to personal information		
no digital transfer of valuable information		
non-digital transfer of security keys		
ownership of data generation		
protocol/mechanisms for protecting personal information		
safeguarding public/security keys		
types of vulnerabilities to safeguard		
uncertainty of criminal intent		
willingness to share information		
adopt partner's network security protocols		
determinant of level of security		
responsibility for securing devices		
responsibility of securing customer data		
stronger security capabilities		
organisations lack understanding and knowledge	System vulnerabilities	INTERNET OF THINGS (IOT)
vulnerable processes in organisations		
vulnerable types of organisations		
data privacy differentiation between IoT and conventional systems	Data governance and IoT	
focus of data breaches in IoT		
open source element of IoT		
POPI and IoT		
regulation and data management in IoT		
types of data stored on IoT network		

The analysis of the participants' profile data was separated as it did not form part of informative data on the subject of investigation, but rather served as a contextual information of the study. Table 4.6 below represents the data collected on the profile of the participants.

Table 4.6: Summary of generated codes, categories and themes for participants' profile

Codes	Categories	Themes
length organisation in operation	Organisation profile	PROFILE
organisation experience and background		
organisation structure		
organisation's area of operation		
organisation's location		
organisation's network coverage and partnerships		
organisation's role in terms of facilitating IoT		
size of organisation		
participant's experience and background	Participant profile	
participant's roles and responsibilities		

In the next section, the descriptive findings will be presented based on the afore-mentioned data analysis process where relevant representative data from participants' responses are presented to inform insightful deductions from answers to the each of the questions posed.

4.4.1.3 Descriptive presentation of findings

This section of the chapter focuses on the presentation of findings drawn from the interview responses of the participants following the systematic thematic analysis process outlined in the previous section. The research sub-questions (SQ) and the corresponding interview questions (IQ) are used to present the responses of the participants and subsequent emergent findings deduced from the meaning and understanding derived from the responses.

4.4.1.3.1 Sub-Question 1.1

SQ1.1: What are the factors affecting data privacy regulation in IoT organisations in South Africa?

IQ1: How would you describe the current situation of data breaches affecting South African organisations?

The purpose of this question was to ascertain the participants' general knowledge of data breaches in organisations in South Africa. **P4**, **P5** and **P10** described the situation in South Africa as "bad" and "scary". Similarly, **P14** and **P15** referred to the upsurge in data breaches as: "quite worrying" and "a very huge concern". **P11** opined that the situation was "problematic and growing", whilst **P12** commented: "It's critical and significant." and "...the biggest risk facing the sustainability of organisations." **P9** believed that in terms of data breaches, South Africa is not unique in the world, nonetheless **P13** was of the impression that South Africa is seen as a soft, easy target whose government is unable to respond adequately. Somewhat alarmingly, **P15** asserted that South Africa is headed for one of the biggest attacks in the near future and it will involve IoT.

Numerous participants were of the opinion that only high profile infringements were reported, arguing that the number of breaches that actually occur were much higher. **P2** stated: "Every now and again you do hear of large companies losing, well databases being leaked, your high profile cases, both locally and globally". **P6** agreed with the above statement, asserting: "Much of what we hear in the news is very large-scale hacks and ransomware attacks". At the time of the research, Transnet, South Africa's state-owned ports and freight-rail enterprise, fell victim to a ransomware attack as mentioned by **P7**: "Transnet's sort of terror was quite publicised a few days ago, and there may be quite a few of these things [data breaches] that we don't know about", which is in agreement with **P2** and **P6**. Additionally, **P7** expressed the

opinion that there may be a considerable amount of data breaches that are unreported, a view shared by **P10** and **P13**, who respectively stated: “There's a lot more data breaches than we are aware of” and “We only see, your Liberty's, and your big cases being reported”.

It was obvious that data breaches worldwide were on the increase and prominent South African organisations have been targeted and had fallen prey to frequent attacks in recent years, however the numbers reported cannot be verified as accurate. This might also be linked to the lack of visible regulation and compliance as seen in South Africa until recently.

Finding: 1: There were deep-rooted concern and consternation about the upsurge in data breaches in South Africa, with a prediction that one of the biggest attacks in the near future would involve the IoT environment.

Finding 2: It was established that the actual number of incidents of data breaches were considerably higher than the high profile infringements that were generally reported.

IQ2: Can you describe the difficulties IoT-based organisations face in terms of the protection of data privacy?

The protection of data privacy has been a keenly debated topic in recent years, therefore it was important to determine what some of the difficulties IoT-based organisations might face in this regard. Participants were in general agreement that people posed the biggest risk when it comes to protecting data privacy. **P6** commented: “We're actually working with a lot of real people as well, who potentially, do have access to a lot of personal information, and could potentially do, not that much with it, but I mean there's always the risk”, **P2** listed various obstacles and agreed: “People within the organisation who perhaps aren't trained correctly”. In accordance with that, **P8** commented that data issues are as a result of inadequacy: “It's the people that don't know what they're doing”. Whilst **P5** was of the opinion: “For most breaches, a person is at fault, usually they're the weakest point”. **P14** highlighted the fact that even though the POPI Act is now in place, it seems that data is still being shared, and thus wondered if it is “someone from within the organisation?”

Additionally, participants cited unsecured devices and networks as sources of threat, **P2** mentioned: “In terms of IoT, I think there's a large focus on the devices”, **P10** in an example mentioned hackers gaining access through unsecured cameras, but **P5** painted the grimmest picture in his assertion: “You can literally take over millions of devices and create a bot army that you can point at any possible site you want to hack”. In addition to that, two of the participants highlighted not having a secure network as a threat. **P3** asserted: “If you can get

access to the network layer, you've got undetectable visibility of the data flowing through that network", and **P4** emphasised: "One of the difficulties for organizations is to get everything on a secure locked down network". Another issue raised by **P8** is the fact that people use their work laptops outside of the office and "connect to some weird sites", a point **P10** concurred with stating: "People using their laptops at Wimpy's [fast food restaurant] and things like that because it's free data and that Wi-Fi is so easily hackable".

Of note was the fact that, **P8** was the only participant who listed POPI as an obstruction to the protection of data privacy for their organisation. The participant argued that it could be due to the fact that "with [the] service systems part of the company, we have to scrub all the data that we get in".

The participants signified that they had a number of processes in place to manage the above-mentioned difficulties, some of these included assigning different levels of access to different users, employing server mirroring, having end-to-end control of the data, and using technologies, such as Sigfox (a French global communications provider) which according to **P3**: "Inherently does not really have any data breaches, when it comes from the physical layer to the application layer".

One can surmise that the difficulties in terms of the protection of data privacy in IoT-based organisations were numerous and aspects relating to people, devices and networks and its implication on data privacy were of significant concern.

Finding 3: There was consensus that the human risk factor and their associated actions presented the biggest danger to IoT-based organisations in terms of the data privacy protection.

Finding 4: In relation to protecting against data breaches, it was reported that unsecured devices and networks posed a high risk to IoT-based organisations.

IQ3: As an IoT-based organisation, what are the types of data privacy infringements your organisation has experienced?

This question was posed to determine if the organisations had experienced any specific type of violations in relation to data privacy. The participants reported that they had no real encounters of infringements in their organisations, as evidenced by responses from **P4**: "We've never had a breach, nor have we had any experience with it", **P11**: "Luckily, to date,

none” and **P14**: “To date, we haven't had any”. Nonetheless, there are a number of possible exposures that organisations are safeguarding against.

P1 was of the opinion that because the intentions of violators were unknown, it was probably good practice to have safeguards in place for every possible eventuality and that this could be achieved by watching global trends. A few examples were given by **P5**, but there were too many threats to mention: “There's ransomware, there's Trojans, there's spyware, there's a whole array of different cyber-attacks that's happening at the moment”. Whilst on the other hand, **P9**, referred to defending against: “man-in-middle attacks” and “social engineering” of employees. For **P4** it was ensuring that there was not a network failure and for **P11** it was defending against “the corruption of the data and a third party collecting that data”.

Furthermore, the participants had varying schools of thought on how to mitigate threats to data privacy, **P15** argued: “Each day, new malware is being developed and without doing continuous, ongoing cyber risk assessments, you can never mitigate against it”. Participants agreed that security should be a key focus. **P1** noted: “Management, “end-to-end control” and “data security for the customer becomes crucial”. **P5** maintained that devices and firmware should have some level of security, along with the back-end systems having “intrusion detection” and “firewalls”. In addition to that, **P5** stated that as an organisation they are applying “cybersecurity based on artificial intelligence” for the recognition of patterns or of anything that was out of the ordinary. There was also a need to start running “secure servers”, that were managed by outside parties, asserted **P10**. There were three aspects of security noted by **P13**, including: “securing the device”, secure transmission and communication, and a “secured [Cloud] environment without any unauthorised access”.

Even though participants had limited experience of actual infringements, proactively safeguarding against potential threats was seen as common practice to ensure that data were secured.

Finding 5: Responses implied that the IoT-based organisations had no real experience of data privacy infringement incidents.

Finding 6: There was an understanding that establishing comprehensive security measures were vital to mitigating threats to data privacy in IoT environments.

4.4.1.3.1.1 Summary of findings

The summarised findings for SQ1.1 can be found in Table 4.7. The sub-question is listed below for ease of reference:

SQ1.1: What are the factors affecting data privacy regulation within IoT organisations in South Africa?

Table 4.7: Summary of findings for SQ1.1

Finding 1	There were deep-rooted concern and consternation about the upsurge in data breaches in South Africa, with a prediction that one of the biggest attacks in the near future would involve IoT environment.
Finding 2	It was established that the actual number of incidents of data breaches were considerably higher than the high-profile infringements that were generally reported.
Finding 3	There was consensus that the human factor and associated actions presented the biggest risk to IoT-based organisations in terms of the data privacy protection.
Finding 4	In relation to protecting against data breaches, it was reported that unsecured devices and networks posed a high risk to IoT-based organisations.
Finding 5	Responses implied that the IoT-based organisations had no real experience of data privacy infringement incidents.
Finding 6	There was an understanding that establishing comprehensive security measures was vital to mitigating threats to data privacy in IoT environments.

4.4.1.3.2 Sub-Question 1.2

SQ1.2: How aware are South African organisations of existing international or cross-border data privacy and regulatory legislations in relation to IoT environments?

IQ4: Can you share your knowledge of South African data privacy and regulatory laws?

The Protection of Personal Information Act, 2013 (Act 4 of 2013), also known as the POPI Act was signed into law in November 2013 (Baloyi & Kotzé, 2018). In February 2017, the Information Regulator was introduced and following several deferments, the Act finally came into effect on the 1st of July 2021 (Roux, 2021). The aim of this question was to establish the participants' general understanding of data privacy and regulatory laws in South Africa.

P10 confirmed: "I don't know a lot about it if I'm going to be honest". Even though the interview question did not explicitly mention the POPI Act, the majority of the participants referred to it in their answer. **P2** asserted: "Every organization now must be POPI compliant". **P5** declared: "We have to adhere to POPI", while **P1** stated: "We've been expecting it [POPI], we support it". **P13** claimed to have very limited knowledge, but mentioned the POPI Act. **P14** specified: "We've got this POPI Act, and that's come in recently" and **P15** asserted: "I have a very good understanding of POPIA". **P11** admitted having limited knowledge, but was aware of the POPI Act and **P12** stated: "We have the POPI Act that has been promulgated and implemented".

Some of the participants however, voiced concerns about the efficacy and application of the POPI Act, **P7** believed that POPI is wonderful, but wondered why it hasn't taken on Facebook? **P6** argued: "It's so hard and so complicated to comply fully with the regulation of POPI". **P9** termed POPI as: "A popular catchphrase at the moment" since organisations are required to comply with the provisions of the Act within a stipulated time period and many are just following the tide. While **P8** was of the opinion that POPI was "overboard" and that "there's lots of flaws in it".

In addition to this point of view, **P7** observed: "The State [government] cannot regulate fast enough" and suggested: "They're [government] probably behind I'd say, probably six, seven years behind in terms of being able to legislate what's actually going on". Furthermore, **P8** acknowledged that due to the changing nature of technology, the POPI Act will continuously have to be adapted to remain applicable.

Conversely, participants believed that even though the legislation has been passed, it will not succeed due to certain challenges faced by the South African government in relation to the implementation and enforcement of the Act. **P13** observed: "Like every other piece of legislation in South Africa, we have very good laws, I think it's the enforcement of the laws where we have the biggest challenge. And there's no accountability", **P14** concurred: "We've got this POPI Act, and that's come in recently, but even with that you're still seeing breaches of security". Whilst **P15** contended: "I don't believe that government has any clue on how to implement and manage POPIA" and "They [government] don't have the skills to police the POPIA legislation". In addition, **P12** pointed out: "The weakness is not so much in the Act as much as it is in the ability to impose sanction and to prosecute".

Limited knowledge around data privacy and regulatory laws in South Africa was evidenced, nevertheless participants were aware of the POPI Act and recognised the challenges it brings in terms of regulation and application by the governing body.

Finding 7: Predominantly, participants demonstrated some knowledge of the POPI Act. However, it did not depict in-depth knowledge and comprehensive understanding of data privacy law in South Africa.

Finding 8: Responses indicated that legislation was behind in terms of technological developments and advancements and that the POPI Act was bound to fail due to implementation and enforcement challenges.

Finding 9: Participants acknowledged that the POPI Act needed to be continuously updated in line with advancing technologies, global trends and developments.

IQ5: How well do you think the POPI Act addresses the uniqueness of managing data within IoT environments?

The POPI Act is South Africa's legislation that aims to provide its citizens with more control over the processing and disclosure of personal information (McKane, 2020). The goal of this question was to determine the participants' perception of the POPI Act in relation to IoT environments. The majority of the participants remarked that the POPI Act does not adequately provide for data management within IoT. **P1** surmised that the POPI Act relates to personal private data and glosses over machine-to-machine (M2M) or IoT data. Yet, the participant believed that POPI is a good enough standard to follow for personal information. **P2** commented that although the POPI Act does not specifically mention IoT, the principles of the Act will fundamentally apply to IoT. **P4** was of the opinion that the POPI Act has not taken IoT into consideration and it does not address privacy in an IoT environment.

Similar to the opinions expressed above, **P5** observed that the POPI Act pertains to information of people, rather than data obtained through IoT devices and therefore, it has not addressed it fully. **P6** corroborated that POPI addresses the management of data "terribly, the reason being is no one knows what POPI says". **P8** was of the impression: "In a perfect world, I think it [POPI] addresses it, but in an imperfect world, I don't think it's spot on". **P10** also thought the Act was inadequate stating: "It's giving lip service". In similar vein, **P13** stressed that the POPI Act, "doesn't do a very good job" and that "there's lots of interpretation issues". While **P15** argued: "It [POPI Act] doesn't address the management of data in IoT" because "the people who drafted POPIA never even heard of IoT, don't even know what IoT is, so nowhere in POPIA, does it really address IoT".

To remedy the above-mentioned adverse opinions on the applicability of the POPI Act in IoT environments, **P6** suggested that people with more technical knowledge and experience should be involved. **P15** also agreed with the point of view and emphasised that there was a need for skilled and technically specialised individuals to assist with the POPI Act. Additionally, **P8** opined that the POPI Act will need to "morph" to a point where it addresses the situation.

With regard to regulation, data obtained from IoT environments may perhaps require further clarification in terms of its classification as personal information.

Finding 10: The majority of participants were in agreement that the POPI Act did not adequately address the uniqueness of managing data in IoT environments.

Finding 11: It was suggested that data privacy regulation, relating to technologies such as IoT should involve input from people with requisite technical expertise.

IQ6: What does the POPI Act mean to your organisation's business processes?

This question was asked to verify the impact of the POPI Act on organisations' operational processes. Participants mentioned that the consequence of the Act was largely administrative and involved communicating the changes with their customers, partners and vendors. **P4** noted that it involved "updating our forms and email policy" and having "less people we can send emails out of the blue". **P6** concurred and expressed that it involved, "lots of agreements, lots of footwork, lots of kind of internal policy things". For **P7** the process involved getting all parties to "agree to an information to share template", while **P8** enquired via email if customers would like to have their details removed. **P5** claimed that the effect on their organisation was two-fold: "There is an administrative impact and a cost impact".

However, a number of participants claimed that due to the type of information collected in their IoT environments, the effect of the Act was minimal. **P1** was under the impression that because they "don't play in the consumer space", the POPI Act had less of an effect on their organisation. **P4** claimed that on the IoT-side, the effect was far less due to the information the organisation needed. A sentiment shared by **P9**: "Very little of our IoT endeavours fall under the POPI Act, because it doesn't contain any personal information". **P11** stated that because they use a third-party, the POPI Act "hasn't really affected us at all". Similarly, **P13** indicated that the POPI Act has meant "very little at this stage" to their organisation.

From the responses it can be gathered that POPI Act impacted organisations in varying ways, the extent of which depended on the organisations collection, utilisation and processing of personal information.

Finding 12: Participants largely claimed that the impact of the POPI Act was administrative, with no evidence of enforcement of compliance and standards.

Finding 13: It was established that the impact of the POPI Act on IoT-based organisations, was dependent on the nature and type of data being collected from the users.

IQ7: You may be aware, the deadline for POPI Act compliance was the 1st of July 2021, **what mechanisms or protocols has your organisation put in place to fulfil the requirements set out by the Act?**

After assessing the impact of the POPI Act, this researcher felt that it was important to enquire about any additional protocols or mechanisms organisations had to put in place to meet the conditions of the Act. Participants described varying practices that were required for their organisation to comply with the POPI Act conditions. **P1** implemented a de-linking process, where information of a person (username) was removed from an operation (GPS location), as well as stored separately. In addition to updating their documents and email policy, **P4** employed an Information Officer to ensure compliance, as did **P12** and **P14**. **P8** used a technique called “scrubbing” which involved customers informing the organisation of their preference to have the organisation store or dispose of their details. If a customer opted for the latter, their information was removed from every system; the organisation performed this “scrubbing” process daily. **P13** utilised “air gapping” (not connected to any network) and “a secure MQTT broker solution” (messaging protocol used for IoT).

Participants also used the processes dictated by other organisations, **P2** as part of a larger organisation, followed the direction of their parent company. On the other hand, **P3** utilised the service of a third-party who “took care of the POPI compliance and the security thereof”. Likewise, for **P11** who claimed: “Our third-party supplier is covering that for us”.

Contrastingly, **P6** claimed that they did not collect what the POPI Act refers to as “unique identifiers”.

Organisations were obligated to apply the appropriate security protocols and mechanisms in order to accomplish compliance with the POPI Act.

Finding 14: Most organisations have put in place distinctly diverse measures to accomplish the conditions stipulated by the POPI Act for data governance, in line with adhering to personal information protection, while a few depended on third-party suppliers to ensure compliance.

IQ8: What is your knowledge of the evolving nature of data privacy regulation and laws globally?

In order to stimulate business, it was imperative for South Africa to establish personal information privacy regulation in harmony with international legislation (Botha & Grobler, 2017). The purpose of this question was to discover the participants’ knowledge and interpretations of global laws relating to data privacy. When asked the question, participants

mentioned GDPR. **P1** declared: “We've always been following GDPR as a global standard because we've got global customers”. **P2** thought that they were in a fortunate position because their data flow was performed by Sigfox, “and they are already GDPR compliant”. **P5** was in agreement and asserted: “If I want to deal with a company in Europe, I have to be GDPR compliant”. **P6** believed that the POPI Act was modelled on GDPR and stated: “POPI is a mirror image of GDPR with a few exceptions”. **P13** indicated: “There is a massive, sort of overlap between GDPR compliance and POPIA”.

The following sentiment was shared by **P15**: “If you look closely at the GDPR and you look at POPIA, you'll see that they've actually taken a lot of the GDPR legislation and just fine-tuned it for South African use”.

P9 was of the impression: “If we conform to our POPI Act we should be able to operate on an international footing, equally”.

Interestingly, participants referred to the main difference between GDPR and the POPI Act. **P6** asserted: “The one difference being that where, GDPR is only concerned with the personal information of natural persons, POPI expands that to juristic persons as well. So not only are people protected, but company's personal information”. A notion **P9** concurred with: “Our POPI Act specifically classifies companies as persons. So, storing personal information about companies, is regulated by the POPI Act, where in general in the international scene, it is not”. **P8** made mention of Australia and America, claiming that they are behind South Africa in terms of “using data for the right outputs”.

Besides the POPI Act and GDPR, there were updates from other countries, including Brazil's Lei Geral de Proteção de Dados Pessoais (LGPD) and in the US, the California Consumer Privacy Act (CCPA), in response to the growing proliferation of data within the digital space.

Finding 15: There was a perception that GDPR was relatively close to the POPI Act, with minor differences in the application, while the definition of an entity's protection of personal information extended to juristic persons in the POPI Act.

Finding 16: A good number of participants displayed knowledge of the GDPR, because of the need to comply with international laws while dealing with global partners within their perspective marketplaces.

4.4.1.3.2.1 Summary of findings

The summary of findings for interview questions relating to SQ1.2 is presented in Table 4.8, and the sub-question is listed below for ease of reference:

SQ1.2: How aware are South African organisations of existing international or cross-border data privacy and regulatory legislations in relation to IoT environments?

Table 4. 8: Summary of findings for SQ1.2

Finding 7	Predominantly, participants demonstrated some knowledge of the POPI Act, however, it did not depict in-depth knowledge and comprehensive understanding of data privacy law in South Africa.
Finding 8	Responses indicated that legislation was behind in terms of technological developments and advancements, and the POPI Act was bound to fail due to implementation and enforcement challenges.
Finding 9	Participants acknowledged that the POPI Act needed to be continuously updated in line with advancing technologies, global trends and developments.
Finding 10	The participants were mainly in agreement that the POPI Act did not adequately address the uniqueness of managing data within IoT environments.
Finding 11	It was suggested that data privacy regulation, relating to technologies such as IoT should involve input from people with requisite technical expertise.
Finding 12	Participants largely claimed that the impact of the POPI Act was administrative, with no evidence of enforcement of compliance and standards.
Finding 13	It was established that the impact of the POPI Act on IoT-based organisations was dependent on the nature and type of data being collected from the users.
Finding 14	Most organisations have put in place distinctly diverse measures to accomplish the conditions stipulated by the POPI Act for data governance, in line with adhering to personal information protection, while a few depended on third-party suppliers to ensure compliance.
Finding 15	There was a perception that GDPR was relatively close to the POPI Act, with minor differences in the application, while the definition of an entity's protection of personal information extended to juristic persons in the POPI Act.
Finding 16	The majority of participants displayed knowledge of GDPR, because of the need to comply with international laws while dealing with global partners within their perspective marketplaces.

4.4.1.3.3 Sub-Question 1.3

SQ1.3: What are the best practices for the governance of data privacy within IoT environments?

IQ9: How do these data privacy regulations and laws inform the management of data, specifically those obtained through IoT environments?

The transfer of personal information to non-EU countries with insufficient privacy protections became almost impossible (Schwartz & Peifer, 2017). The question was intended to assess how recent updated privacy laws influenced data management with respect to IoT environments. In essence, only **P8** thought that it aided in making an educated decision about the handling of data rather than playing a guessing game.

Participants believed that the regulations limited the flow of information and forced organisations to decentralise their databases. **P5** maintained that for IoT devices connecting to the Cloud in other parts of the world, the organisation needed to ensure that identifiable personal information could not be distinctly identified, i.e., “sending personal data across

borders is a no-no". In addition to that, the participant speculated that this was a primary reason companies such as Amazon were relocating their head office to places like Cape Town. **P6** was of the opinion that the regulations were "discretizing the whole world into smaller parts and making it very hard to flow information across those virtual borders". Thus, the participant said that to operate in the EU, the organisation would either have to move their infrastructure there or duplicate it. Similarly, **P9** had the experience of dealing with a European client, where regulatory requirement, requested that their data to be hosted in Europe.

Although updates to privacy laws provided guidance, as per **P8**, it also placed restrictions on the undeterred movement of information across virtual borders. It was evident that the heterogeneity in the standards applicable to data governance by different countries was an inhibitor to the cross-border operations in the business process.

Finding 17: The implementation of diverse country-specific data regulations forced organisations to decentralise their databases which limited the flow of information as a compliance for cross-border business operations.

IQ10: Given the universal nature and the amount of data generated by connected devices, **how can organisations facilitate the protection of personal information? (In an ideal world)**

The number of IoT connected devices for 2021 were assessed to be in the region of 13 billion, a nine percent rise from the previous year (Sinha, 2021). Moreover, this figure has been forecasted to reach 50 billion in the next ten years (Vailshery, 2021). The growth of IoT devices correlated with increased volumes of data, therefore it was essential to determine how organisations enabled personal information protection of data generated from IoT devices. Participants cited applying security measures such as encryption and having secure storage were essential. **P3** mentioned utilising encryption on the devices and the network layer, while **P5** noted: "Encryption, using encrypted tunnels to transport data" and **P9** advised: "Encryption of the data in transit", as well as "encrypting the data in storage". **P13** corroborated the previous assertions, saying: "Good current encryption" was essential. Additional methods were also stated, such as "a lockdown network, uninterrupted transfer of data and a secure place to store it" as reported by **P4**. "Stronger firewalls, stronger places that you store it," was suggested by **P8**. In addition to that, **P13** stated: "We tokenise and keep all of the data completely separate".

On the other hand, **P6** contended that the protection of personal information should not make it more difficult to process information, but should entail making it more challenging to access personal information.

The growing number of connected devices and the volume of data produced by these devices necessitated an increased focus on the protection of personal information.

Finding 18: To facilitate the protection of personal information, measures such as encryption and providing secure data storage were applied.

IQ11: What are the challenges or complexities surrounding the protection of personal information within IoT environments?

Discovering the obstacles and difficulties in IoT environments in relation to the protection of personal information was necessary in order to determine best practices for data governance. The biggest challenge participants perceived within the IoT environments was the linked devices. **P10** presented the argument that IoT devices such as security cameras were perfect entry points for hackers as there was seldom security on these devices. Voicing similar concerns, **P5** asserted that there was no certification or security checks for device creators. In addition, **P7** was of the opinion that having so many devices to contend with became too complicated. While **P12** advanced: “Every device becomes an entry point for a hacker”.

P1 and **P5** declared that cost was a challenge, they respectively stated: “Splitting environments means that you've got an added fee on your structure”, and “there will be a cost associated with compliance”. **P15** warned that due to the fact that IoT was relatively new and evolving daily, it made it difficult to understand and therefore challenging to obtain a budget to protect it.

Participants also had varying ideas about other challenges faced in IoT environments which involved **P1**, **P2**, **P3**, **P6**, **P9** and **P13**, respectively identifying “the management of the data and the end-to-end control component”, “education”, “normal problems of TCP/IP and general web security”, “companies like us can't own the whole value chain”, “social engineering” of individuals and “maintenance of the data”.

Thus, the challenges for IoT in relation to the protection of personal information were numerous and diverse. For example, unsecured devices could provide a perfect entry point for the individual's intent on illegally gaining access to personal information and secured data.

Finding 19: It was established that the security of connected devices in IoT environments posed the biggest challenge when it came to the protection of personal information, with other constraints such as cost and maintenance voiced as well.

IQ12: Can you describe the protocols that guide the protection and use of personal information within IoT environments in your organisation?

This question was asked to assess the common protocols employed by IoT-based organisations for the protection and use of personal information. Participants remarked that they used external companies such as Sigfox, AWS, Microsoft Azure and Google Cloud for their network and Cloud infrastructures. These third parties utilised technologies that inherently had stringent security protocols in place for data transmission and storage. **P2** explained that the telecommunications infrastructure was operated by their organisation which in turn leveraged Sigfox technology for Cloud communication. In addition to that, **P2** added: “When you are using something like Sigfox, because the protocol is done for you, a lot of the really dangerous security flaws are taken care of for you”. **P6** declared: “To a large extent, Internet of Things companies are dependent on other suppliers for their data privacy”, while **P13** affirmed: “We're relying heavily on Microsoft and what Microsoft are doing to secure their Cloud infrastructure environment”.

To ensure accountability in the management of client data, **P3** insisted that their IoT-based organisation whose existence largely depended on security, thoroughly evaluated and tested third party providers to ensure they adhered to all the required security parameters.

On the other hand, **P1** claimed that their own security protocol provided about eighty percent of the security for their solution and consisted of several security elements, such as AES (Advanced Encryption Standard) and authentication. Although **P8** did not give details of their own protocols, the participant alluded to utilising their in-house solution rather than trusting external third parties.

The participants' responses did not render any distinct list of protocols, but rather indicated a tendency for IoT-based organisations to rely on external providers or those deemed experts in the field for the secure management of their data through varying customised technologies.

Finding 20: Responses indicated that the majority of IoT-based organisations depended on third party organisations to provide security protocols for the protection and use of client's personal information.

Finding 21: The third party customised technology used for securing data from IoT devices included Sigfox, AWS, Microsoft Azure and Google Cloud for their network and Cloud infrastructures, with in-house solutions like AES also being utilised.

IQ13: Can you share a situation you have experienced or know of where there was unauthorised access and use of personal data?

IQ13b: What measures were applied or could have been applied to mitigate and resolve such a situation?

This is a two-part question which, firstly seeks to establish the participants' knowledge of unauthorised access and use of personal data, and secondly, to determine how these situations could have been mitigated or resolved. In general, most of the participants had some knowledge or experience of unauthorised access and use of personal information. **P1** mentioned the notorious hacking of a fish tank at a US casino through the temperature meter. **P2** referred to a PlayStation hack in which the hacker obtained user credentials as well as getting daily unsolicited emails and messages. **P5** provided the following examples: "Employees stealing customer databases", "a company that tried to crack into another company's customer database" and turning electricity meters into a bot army and attacking a server so that it was unable to perform designated tasks.

P9 described a situation in which someone was able to reuse a voucher on an airtime purchasing application. Commenting on the spate of unauthorised use of personal information, **P10** expressed knowledge of a server farm that was the target of a ransomware attack. **P14** mentioned the number of call centres that contacted people on a daily basis. **P12** agreed: "One sees it just in terms of scam calls and emails that just are unabated".

Resolutions to some of these issues were suggested by **P8**, **P9**, **P10** and **P12**, respectively as: "It should be a certain level of management that has access", "As soon as there are money values involved architectural oversight becomes a requirement", "Do a mirror image of the server every day" and "It's just a plethora of controls that one has to put in place to try and protect one's information assets".

It was important to understand the plethora of possibilities that could result in the breach of data beyond the commonly reported hacks in order to put in adequate measures and security protocols. Incidents like unauthorised access and use of personal data could include practices as simple as spam emails and text messages with serious consequences to more nefarious acts such as hacking and ransomware.

Finding 22: Instances of threats to personal data included hacking into smart devices, employee action, corporate espionage, ransomware attacks, as well as scam calls and emails.

Finding 23: Suggested solutions to mitigate unauthorised access and use of personal data included management level access, preventative and protection controls, architectural oversight for monetary transactions and daily server mirroring.

4.4.1.3.3.1 Summary of findings

The summarised findings from the interview questions relating to SQ1.3 are presented in Table 4.9, and the sub-question is listed below for ease of reference:

SQ1.3: What are the best practices for the governance of data privacy within IoT environments?

Table 4.9: Summary of findings for SQ1.3

Finding 17	The implementation of diverse country-specific data regulations forced organisations to decentralise their databases which limited the flow of information as a compliance for cross-border business operations.
Finding 18	To facilitate the protection of personal information, measures such as encryption and providing secure data storage were applied.
Finding 19	It was established that the security of connected devices within IoT environments posed the biggest challenge when it came to the protection of personal information, with other constraints such as cost, and maintenance voiced as well.
Finding 20	Responses indicated that the majority of IoT-based organisations depended on third party organisations to provide security protocols for the protection and use of client's personal information.
Finding 21	The third party customised technology used for securing data from IoT devices included Sigfox, AWS, Microsoft Azure and Google Cloud for their network and Cloud infrastructures, with in-house solutions like AES also being utilised.
Finding 22	Instances of threats to personal data included hacking into smart devices, employee action, corporate espionage, ransomware attacks, as well as scam calls and emails.
Finding 23	Suggested solutions to mitigate unauthorised access and use of personal data included management level access, preventative and protection controls, architectural oversight for monetary transactions and daily server mirroring.

4.4.1.3.4 Sub-Question 1.4

SQ1.4: How can a data privacy governance framework for IoT organisations in South Africa be developed?

IQ14: In your opinion, how does data privacy and protection differ between IoT environments and conventional systems?

The purpose of the question was to discover if there is a differentiation between IoT environments and conventional systems when it concerns data privacy and protection. **P1** was of the impression that in IoT environments there was less focus on personal information than in general IT environments. Conversely, **P2** believed that security issues and processes for conventional systems and IoT environments were inherently similar, but with the added

physical component for IoT. **P3** was also in agreement, but cited the long range networks used by IoT for communication as a variant. **P4** noted: “The vulnerability about an IoT environment is the fact that you have so many endpoints”, while **P5** was of the opinion that it’s more difficult to secure and have control in IoT environments because of the widespread nature of the networks.

P7 commented that although IoT environments provided accurate “real-time dynamic information”, privacy might be an issue when compared to an ERP (Electronic Resource Planning) system. **P9** opined that compromising information in an IoT environment was more difficult than with conventional systems that involved people, however this did not include IoT devices connected to a person. **P12** did not think that there was much variation, as well as **P14** who noted: “It should be more or less the same”. Similarly, **P15** argued that there was no difference and stated: “You’ve got to protect it [data] wherever it is”.

Due to the nature of data access and processing, distinctions in relation to data privacy and protection for conventional systems and IoT environments did exist, nevertheless similarities were prominent in the application of regulations and categorisation of data privacy requirements.

Finding 24: There was a perception that conventional IT systems focused more on people and personal information than IoT environments, where the focus was more on securing and controlling access due to the interconnectivity aspect of IoT environments.

Finding 25: It was believed that the security risks and procedures for conventional systems and IoT environments were similar, however for IoT there were added components such as the devices, the widespread nature of the networks and the vulnerability of having various endpoints.

IQ15: And lastly, how would you suggest organisations operating within IoT environments go about ensuring compliance for data privacy and regulatory laws?

Compliance to data privacy and regulatory laws are imperative or organisations run the risk of not only being fined, but also suffering reputational damage. Participants recommended engaging with experts in compliance and security. **P2** proposed getting legal advice and making certain service providers were compliant as well. **P4** agreed that gaining knowledge through hired specialists or an Information Officer was encouraged and emphasised, closely following the advice they provided. **P7** was also adamant that hiring a good consultant was

key to understanding digitalisation, as well as using and protecting data. From a security perspective, **P5** suggested meeting compliance through security and possibly appointing penetration experts “to probe and test” systems. **P9** strongly warned against the development of in-house security systems and advocated contracting authorities in security.

Relatively speaking, **P11** advised to obtain “good advice from third parties or advisors”. Similarly, **P15** recommended: “They need to employ suitably qualified specialists”. **P8** asserted: “There needs to be more education around what the actual Act is, and what you're allowed to and what you're not allowed to do”.

Finding 26: To comply with data privacy and regulatory laws in IoT environments, participants recommended utilising compliance experts and security specialists to ensure that the required standardised process and approach were followed.

For South Africa, compliance to the POPI Act was mandatory, therefore it was imperative that organisations were knowledgeable about the requirements of the Act. Particular focus was on the understanding and application of data privacy regulations in IoT environments in South Africa which provided rich insights and exposition of the research phenomenon.

4.4.1.3.4.1 Summary of findings

The summary of findings for interview questions relating to SQ1.4 is presented in Table 4.10, and the sub-question is listed below for ease of reference:

SQ1.4: How can a data privacy governance framework for IoT organisations in South Africa be developed?

Table 4.10: Summary of findings for SQ1.4

Finding 24	There was a perception that conventional IT systems focused more on people and personal information than IoT environments, where the focus was more on securing and controlling access due to the interconnectivity aspect of IoT environments.
Finding 25	It was believed that the security risks and procedures for conventional systems and IoT environments were similar, however for IoT there were added components such as the devices, the widespread nature of the networks and the vulnerability of having various endpoints.
Finding 26	To comply with data privacy and regulatory laws within IoT environments, participants recommended utilising compliance experts and security specialists to ensure that the required standardised process and approach were followed.

4.4.1.4 Summary of findings and theme development

A summary of all the findings, the related categories and themes grouped under each sub-question can be found in Table 4.11.

Table 4.11: Findings, categories and themes

Findings	Categories	Themes
SQ1.1: What are the factors affecting data privacy regulation within IoT organisations in South Africa?		
Finding 1: There were deep-rooted concern and consternation about the upsurge in data breaches in South Africa, with a prediction that one of the biggest attacks in the near future would involve IoT environment.	Data breaches	DATA PRIVACY
Finding 2: It was established that the actual number of incidents of data breaches were considerably higher than the high-profile infringements that were generally reported.		
Finding 3: There was a consensus that the human-factor and their associated actions presented the biggest risk to IoT-based organisations in terms of the data privacy protection.	Challenges of securing personal information	
Finding 4: In relation to protecting against data breaches, it was reported that unsecured devices and networks posed a high risk to IoT-based organisations.		
Finding 5: Responses implied that the IoT-based organisations had no real experience of data privacy infringement incidents.		
Finding 6: There was an understanding that establishing comprehensive security measures were vital to mitigating threats to data privacy in IoT environments.		
SQ1.2: How aware are South African organisations of existing international/cross-border data privacy and regulatory legislations for IoT environments?		
Finding 7: Predominantly, participants demonstrated some knowledge of the POPI Act, however, it did not depict in-depth and comprehensive understanding of data privacy law in South Africa.	Knowledge of regulations	REGULATION
Finding 8: Responses indicated that legislation was behind in terms of technological developments and advancements, and the POPI Act was bound to fail due to implementation and enforcement challenges.		
Finding 9: Participants acknowledged that the POPI Act needed to be continuously updated in line with advancing technologies, global trends and developments.		
Finding 10: The participants were mainly in agreement that the POPI Act did not adequately address the uniqueness of managing data in IoT environments.	Data governance and IoT	
Finding 11: It was suggested that data privacy regulation, relating to technologies such as IoT should involve input from people with requisite technical expertise.		
Finding 12: Participants largely claimed that the impact of the POPI Act was administrative, with no evidence of enforcement of compliance and standards.	Regulation of personal information	
Finding 13: It was established that the impact of the POPI Act on IoT-based organisations, was dependent on the nature and type of data being collected from the users.		
Finding 14: Most organisations have put in place distinctly diverse measures to accomplish the conditions stipulated by the POPI Act for data governance, in line with adhering to personal information protection, while a few depended on third-party suppliers to ensure compliance.		

Finding 15: There was a perception that GDPR was relatively close to the POPI Act, with minor differences in the application, while the definition of an entity's protection of personal information extended to juristic persons in the POPI Act.	Knowledge of regulations	
Finding 16: A good number of participants displayed knowledge of GDPR, because of the need to comply with international laws while dealing with global partners within their respective marketplaces.		
SQ1.3: What are the best practices for the governance of data privacy within IoT environments?		
Finding 17: The implementation of diverse country- specific data regulations forced organisations to decentralise their databases, which limited the flow of information as a compliance for cross-border business operations.	Security in IoT environments	DATA SECURITY
Finding 18: To facilitate the protection of personal information, measures such as encryption and providing secure data storage were applied.		
Finding 19: It was established that the security of connected devices within IoT environments posed the biggest challenge when it came to the protection of personal information, with other constraints such as cost and maintenance voiced as well.		
Finding 20: Responses indicated that the majority of IoT-based organisations depended on third-party organisations to provide security protocols for the protection and use of client's personal information.		
Finding 21: The third party customised technology used for securing data from IoT devices included Sigfox, AWS, Microsoft Azure and Google Cloud for their network and Cloud infrastructures, with in-house solutions like AES also being utilised.	System vulnerabilities	
Finding 22: Instances of threats to personal data included hacking into smart devices, employee action, corporate espionage, ransomware attacks, as well as scam calls and emails.		
Finding 23: Suggested solutions to mitigate unauthorised access and use of personal data included management level access, preventative and protection controls, architectural oversight for monetary transactions and daily server mirroring.		
SQ1.4: How can a data privacy governance framework for IoT organisations in South Africa be developed?		
Finding 24: There was a perception that conventional IT systems focused more on people and personal information than IoT environments, where the focus was more on securing and controlling access due to the interconnectivity aspect of IoT environments.	Data governance and IoT	INTERNET OF THINGS (IOT)
Finding 25: It was believed that the security risks and procedures for conventional systems and IoT environments were similar, however for IoT there were added components such as the devices, the widespread nature of the networks and the vulnerability of having various endpoints.		
Finding 26: To comply with data privacy and regulatory laws within IoT environments, participants recommended utilising compliance experts and security specialists to ensure the required standardised process and approach were followed.		

The following section presents the analysis of data from policy documents and emergent findings.

4.4.2 Analysis of policy document review

The review and evaluation of printed and electronic documents involving a systematic procedure can be termed document analysis (Bowen, 2009). Impartial and consistent analysis of policies are facilitated by applying document analysis according to Wach (2013), in order to “elicit meaning, gain understanding, and develop empirical knowledge” (Bowen, 2009:27). This section of the chapter describes the analysis and presents the findings obtained from the analysis of data protection policies from selected countries using a judgmental sampling technique. The criteria for selecting the policies were based on documents that were updated recently, following the implementation of the EU's GDPR in the year 2018 which was necessitated by the advancements in technologies that facilitated the collection, aggregation, dissemination and storage of personal information. The primary focus of the document analysis was to extract the relevant data and themes that made provision for the protection of personal information pertaining to the use of technology within legislative policies. The analysis of the policy documents was necessary to assess the commonalities and disparities in terms of the protection of personal information based on the perspective of a region or country.

The thematic analysis of the ten selected policy documents are presented and discussed in the next section. Applying the steps of thematic analysis is outlined in Table 4.4 which encompasses familiarisation with text or data, producing codes and initial themes and revising, defining and identifying themes, relevant data and emergent patterns within the policy documents were identified.

4.4.2.1 Generating codes and categories

Following the selection of policy documents from the ten countries as discussed in the previous section, the documents were uploaded into ATLAS.ti. The word frequency identified within the policy documents is depicted in Figure 4.6.

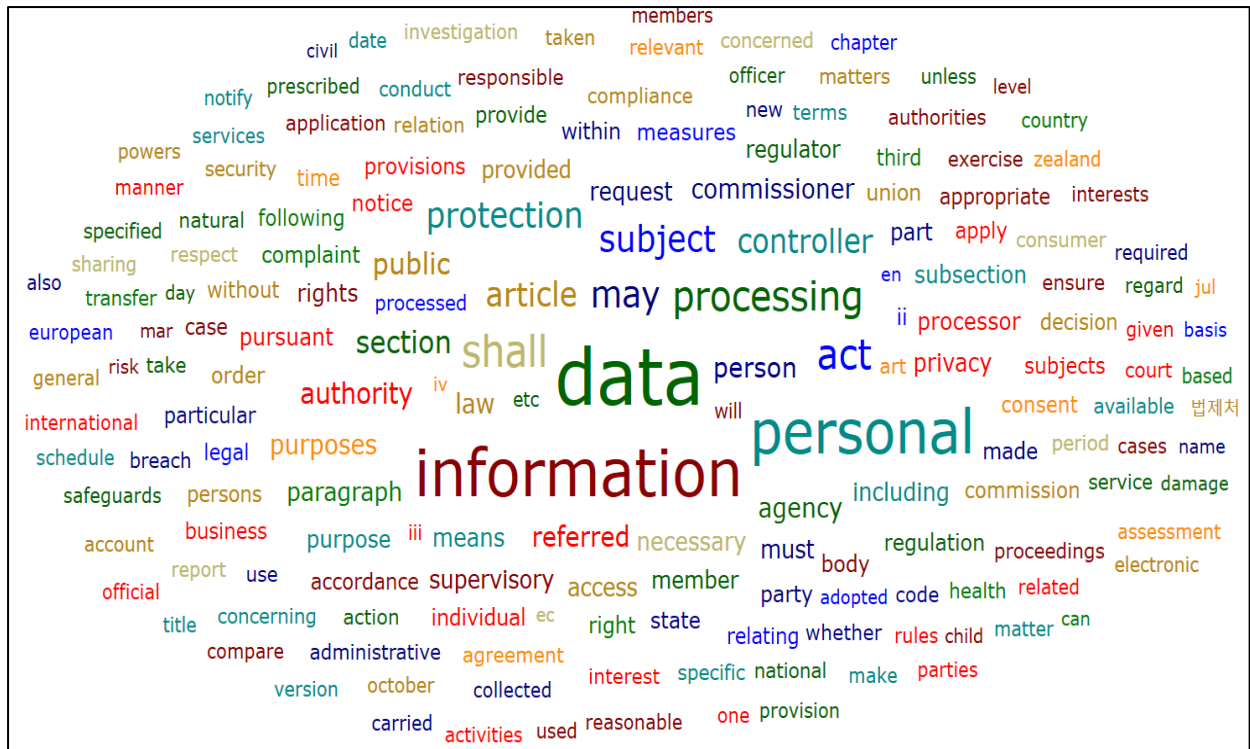


Figure 4.6: Representation of word frequency in policy documents

When conducting a document analysis, an inductive or deductive approach can be used to identify the initial codes for the analysis of the documents (Gross, 2018). The initial coding process involved reading through the policy documents to gain an understanding of the structure and concepts. Utilising an inductive approach, the policy documents were analysed and open coding was applied to establish the initial codes. An example of the codes generated from the analysis of the policy documents is shown in Figure 4.7. Following this, the preliminary identified codes were exported into Excel, where the final codes were grouped under the relevant descriptive categories as portrayed in Table 4.12.

L 119/36 EN Official Journal of the European Union 4.5.2016	
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (storage limitation); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality). 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').	1:31 Article... ◇ principle: storage limitation 1:3... ◇ principle: integrity and confide... ... ◇ principle: accountability
Article 6 Lawfulness of processing 1. Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks. 2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.	1:52 Article 6: Lawfulness of Processing ◇ lawful processing: applicable 1... ◇ lawful processing: not applicable 1:54... ◇ lawful processing: applicable (s...

Figure 4.7: Example of generating initial codes

4.4.2.2 Generating themes

An iterative process was followed to identify the emerging patterns in the data, shown in Table 4.12, from the extraction and categorisation of data into sub-themes and subsequently the overarching theme.

Table 4.12: Categories and themes generated from codes

Categories	Sub-themes	Theme
Defining Personal Information or Personal Data	Personal information / personal data definition	REGULATION
Conditions for Consent	Processing personal information	
Consent Pertaining to Children		
Obtaining Consent		
Lawful Processing		
Principles		
Processing		
Rights of Data Subject	Individual rights	
Rights of the Consumer		
Controller Obligations		
Processor Obligations		

Information Officer Obligation	Responsible parties, operators and supervision	
Information Regulator Obligation		
Cross-Border Transfers	International transfers of personal information	
Personal Data Breaches	Breaches of personal information	DATA PRIVACY

4.4.2.3 Presentation of the findings

This section provides a discussion on the findings from the themes that emerged following the analysis of the selected policy documents. The findings are presented based on two themes, namely regulation and data privacy.

4.4.2.3.1 Theme: Regulation

4.4.2.3.1.1 Personal information or personal data definition

To gain an understanding of the importance of the protection of personal information or personal data, it was imperative to ascertain the meaning of personal information or personal data as defined by the policy documents. The use of the terms, *personal information* or *personal data* depends on the origins of the policy document. Six of the countries used and defined the term, *personal data* and four of the countries defined and used the term, *personal information* as outlined in Table 4.13. Furthermore, four of the countries also differentiated between *sensitive personal data* and *sensitive data*. In relation to data generated by automated devices, like those found in IoT environments, there were no explicit definitions regarding the direct or indirect use of data.

However, the EU's GDPR defined personal information as "...an identifiable natural person is one who can be identified, directly or indirectly". Egypt also made reference to indirect identification, thus implying personal data collected from autonomous devices. The USA and South Africa which shared similar definitions had no statement on indirect or autonomous data collection. Still, they made relatable reference to personal information as "online identifier or other particular assignment to the person". Only the British Virgin Islands defined personal data in relation to that which was obtained indirectly from autonomous sources as information that "is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose". Similarly South Korea made reference to unique information that can be indirectly rendered by the use of technology:

Information which, even if it by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual. In such cases, whether or not there is ease of combination shall be determined by reasonably

considering the time, cost, technology, etc. used to identify the individual such as likelihood that the other information can be procured.

On the other hand, Brazil, Kenya and New Zealand had no explicit provisions for data sourced indirectly by means of technology in their documents. For the purpose of this study and in the context of South Africa, the term, *personal information* was adopted to represent personal data.

Table 4.13: Definitions for Personal Data or Personal Information

Country	Term	Definition
EU (GDPR)	Personal Data	“any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.
San Marino		“any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.
Brazil		“information regarding an identified or identifiable natural person”.
British Virgin Islands		“any information in respect of commercial transactions, which (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information, or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject”.
Kenya		“any information relating to an identified or identifiable natural person”.
Egypt		“any data relating to an identified natural person, or one who is identifiable, directly or indirectly, by reference to such data and to other data such as a name, a voice, a photograph, an identification number, an online identity identifier, or any data referring to the person’s psychological, medical, economic, cultural or social identity”.
USA (CCPA)	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, color, 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”.

South Korea		“any of the following information relating to a living individual: (a) Information that identifies a particular individual by his or her full name, resident registration number, image, etc.; (b) Information which, even if it by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual. In such cases, whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as likelihood that the other information can be procured; (c) Information under items (a) or (b) above that is pseudonymized in accordance with subparagraph 1-2 and thereby becomes incapable of identifying a particular individual without the use or combination of information for restoration to the original state”.
New Zealand		“(a) means information about an identifiable individual; and (b) includes information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages, and Relationships Registration Act 1995 or any former Act (as defined in section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995)”.
South Africa (POPIA)		“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”.
Brazil	Personal Sensitive Data	“personal data concerning racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical or political organization membership, data concerning health or sex life, genetic or biometric data, when related to a natural person”.
British Virgin Islands		“means any personal data about a data subject’s (a) physical or mental health; (b) sexual orientation; (c) political opinions; (d) religious beliefs or other beliefs of a similar nature; (e) criminal convictions, the commission or alleged commission, of any offence; or (f) any other personal data that the Minister may by Order prescribe”.
Kenya		“data revealing the natural person’s race, health status, ethnic social origin conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person’s children, parents, spouse or spouses, sex or the sexual orientation of the data subject”.
Egypt	Sensitive Data	“data disclosing psychological, mental, physiological, or genetic health, biometric or financial data, religious beliefs, political opinions, or security standing and, in all cases, data relating to children is considered to be sensitive data”.

Finding 27: In relation to data generated by automated devices, like those found in IoT environments, there was no explicit definition regarding what constituted direct or indirect data.

4.4.2.3.1.2 Processing personal information

The policy documents incorporated definitions and principles or conditions for the lawful processing of personal information. Nine of the ten countries defined the term, *processing* and for the purpose of this study the definition for South Africa was employed:

any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including — (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information.

▪ Principles for processing of personal information

Although the number of principles or conditions specified for each country varied, commonalities existed within the stipulations as observed in Table 4.14. The legislations directed that parties (for example, controllers and processors) responsible for the processing of personal information must ensure that the principles are upheld and compliance is established.

Table 4.14: Principles related to the processing of personal information

Country	No. of Principles	Principles / Conditions
EU (GDPR)	6	1. Lawfulness, fairness & transparency 2. Purpose limitation 3. Data minimisation 4. Accuracy 5. Storage limitation 6. Integrity & confidentiality
San Marino		
South Korea	8	1. Lawfulness, fairness and transparency 2. Purpose limitation 3. Accuracy & Data minimisation 4. Integrity and confidentiality 5. Openness 6. Minimise possibility of infringements 7. Apply anonymisation / pseudonymisation 8. Trustfulness
New Zealand	13	1. Purpose of collection of personal information 2. Source of personal information 3. Collection of information from subject 4. Manner of collection of personal information 5. Storage and security of personal information 6. Access to personal information 7. Correction of personal information 8. Accuracy, etc., of personal information to be checked before use or disclosure 9. Agency not to keep personal information for longer than necessary 10. Limits on use of personal information 11. Limits on disclosure of personal information 12. Disclosure of personal information outside New Zealand 13. Unique identifiers
Brazil	10	1. Purpose 2. Suitability 3. Necessity 4. Free access 5. Quality of the data 6. Transparency 7. Security 8. Prevention 9. Non-discrimination 10. Accountability
British Virgin Islands	7	1. General 2. Notice & choice 3. Disclosure 4. Security 5. Retention 6. Data integrity 7. Access
Egypt	4	1. Lawfulness, fairness & transparency 2. Accuracy 3. Purpose limitation 4. Storage limitation
Kenya	8	1. Right of privacy adherence 2. Lawfulness, fairness & transparency 3. Purpose limitation 4. Data minimisation 5. Family & private affairs 6. Accuracy 7. Storage limitation 8. Adequate safeguards for cross-border transfers
South Africa (POPIA)	8	1. Accountability 2. Processing limitation 3. Purpose specification 4. Further processing limitation 5. Information quality 6. Openness 7. Security safeguards 8. Data subject participation

Based on the frequency of the principles in Table 4.14, eight shared principles were identified and Figure 4.8 illustrates the principles visually and a description of each is proposed below.

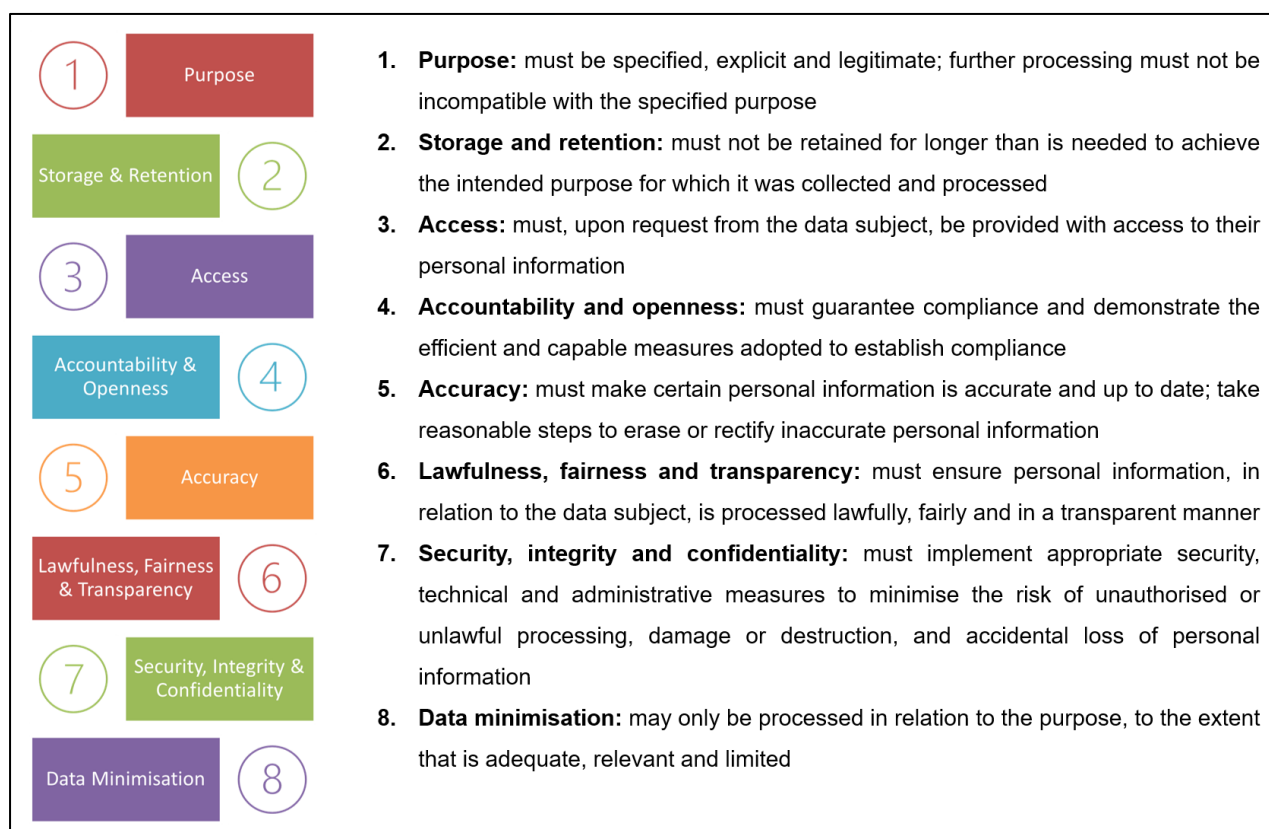


Figure 4.8: Proposed principles

From a legal perspective, the proposed principles provide a neat package within which to wrap the legal requirements for processing personal information. However, given the scope and diversity, the application to an array of disciplines, as well as the constant advancement of IoT and evolving technologies, continuous revision of the principles may be required.

Additionally, in order to process personal information lawfully, a number of conditions have been outlined by the majority of countries, as indicated in Table 4.15.

Table 4.15: Lawful processing of personal information

Country	Conditions
EU (GDPR)	"Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in
San Marino	

	the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”.
South Korea	“A personal information controller may collect personal information in any of the following circumstances, and use it with the scope of the purpose of collection: 1. Where consent is obtained from a data subject; 2. Where special provisions exist in laws or it is inevitable to observe legal obligations; 3. Where it is inevitable for a public institution’s performance of its duties under its jurisdiction as prescribed by statutes, etc.; 4. Where it is inevitably necessary to execute and perform a contract with a data subject; 5. Where it is deemed manifestly necessary for the protection of life, bodily or property interests of the data subject or third party from imminent danger where the data subject or his or her legal representative is not in a position to express intention, or prior consent cannot be obtained owing to unknown addresses, etc.; 6. Where it is necessary to attain the justifiable interest of a personal information controller, which such interest is manifestly superior to the rights of the data subject. In such cases, processing shall be allowed only to the extent the processing is substantially related to the justifiable interest of the personal information controller and does not go beyond a reasonable scope”.
Brazil	“Processing of personal data shall only be carried out under the following circumstances: I – with the consent of the data subject; II – for compliance with a legal or regulatory obligation by the controller; III – by the public administration, for the processing and shared use of data which are necessary for the execution of public policies provided in laws or regulations, or based on contracts, agreements or similar instruments, subject to the provisions of Chapter IV of this Law; IV – for carrying out studies by research entities, ensuring, whenever possible, the anonymization of personal data; V – when necessary for the execution of a contract or preliminary procedures related to a contract of which the data subject is a party, at the request of the data subject; VI – for the regular exercise of rights in judicial, administrative or arbitration procedures, the last pursuant to Law No. 9,307, of September 23, 1996 (the “Brazilian Arbitration Law”); VII – for the protection of life or physical safety of the data subject or a third party; VIII – to protect health, in a procedure carried out by health professionals or by health entities; IX – when necessary to fulfil the legitimate interests of the controller or a third party, except when the data subject’s fundamental rights and liberties which require personal data protection prevail; or X – for the protection of credit, including as provided in the pertinent legislation”.
British Virgin Islands	“(1) A data controller shall not (a) in the case of personal data other than sensitive personal data, process personal data about a data subject unless the data subject has given his or her express consent to the processing of the personal data; (b) in the case of sensitive personal data, process sensitive personal data about a data subject except in accordance with section 20; or (c) transfer personal data outside the Virgin Islands, unless there is proof of adequate data protection safeguards or consent from the data subject. (2) Notwithstanding subsection (1)(a) and subject to subsection (3), a data controller may process personal data about a data subject if the processing is necessary (a) for the performance of a contract to which the data subject is a party; (b) for the taking of steps at the request of the data subject with a view to entering into a contract; (c) for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by a contract; (d) in order to protect the vital interests of the data subject; (e) for the administration of justice; or (f) for the exercise of any functions conferred on a person by or under any law. (3) Personal data shall not be processed unless (a) the personal data is processed for a lawful purpose directly related to an activity of the data controller; (b) the processing of the personal data is necessary for, or directly related to that purpose; and (c) the personal data is adequate but not excessive in relation to that purpose”.
Egypt	“Electronic Processing shall be considered legitimate and legal in the following cases: 1. If the Data Subject consents to the Processing for the achievement of one or more specific purpose(s). 2. If the Processing is necessary and essential for the performance of a contractual obligation, a legal action, the execution of an agreement for the benefit of the Data Subject or the undertaking of any procedure with respect to claiming or defending the Data Subject’s legal rights. 3. Performing an obligation regulated by the law or an order issued by the competent investigation authorities or based upon a court judgement. 4. Allowing the Controller to perform his obligations or any relevant person to practice his legitimate rights unless such matter contradicts the basic rights and freedoms of the Data Subject”.
Kenya	“A data controller or data processor shall not process personal data, unless — (a) the data subject consents to the processing for one or more specified purposes; or (b) the processing is necessary — (i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract; (ii) for compliance with any legal obligation to which the controller is subject; (iii)

	in order to protect the vital interests of the data subject or another natural person; (iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (v) the performance of any task carried out by a public authority; (vi) for the exercise, by any person in the public interest, of any other functions of a public nature; (vii) for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or (viii) for the purpose of historical, statistical, journalistic, literature and art or scientific research”.
South Africa (POPIA)	“Personal information may only be processed if — (a) the data subject or a competent person where the data subject is a child consents to the processing; (b) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party; (c) processing complies with an obligation imposed by law on the responsible party; (d) processing protects a legitimate interest of the data subject; (e) processing is necessary for the proper performance of a public law duty by a public body; or (f) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied”.

Predominantly the countries stipulated consent as the first requirement for processing personal information, however other situations under which personal information can be processed were also provided. These related to self-explanatory circumstances such as contractual and legal obligations, safeguarding the interests of the data subject, etc. The next section expands on two of the circumstances stipulated for the majority of countries, namely consent and for the pursuance of the legitimate interests of the responsible party (controller or data controller) or in some cases a third party.

▪ Consent

Although obtaining consent was not the only circumstance under which personal information can be lawfully processed, it was a preferred method for most organisations. Specifications on obtaining consent from users were conspicuously missing from the documents, yet the responsibility for acquiring consent should rest with the entities that collect, process or store the information. The definitions for consent, as reflected in Table 4.16, specify that consent must be given freely or voluntarily and be specific and informed.

With regard to smart devices and IoT environments, more often than not, if a user did not consent to the processing of their personal information, they might not be able to use the device or application. Therefore, the notion of consenting freely and voluntarily became questionable and one could argue that consent in IoT environments was rarely given freely or voluntarily.

Similarly, by giving consent, a smart device user or IoT client generally agreed to blanket terms and conditions that covered the device makers, app developers and in some cases even third parties, thus it could be argued that consent in IoT environments was rarely explicit or informed.

Table 4.16: Countries with definitions for consent

Country	Definition of consent
EU (GDPR)	"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".
Brazil	"free, informed and unambiguous manifestation whereby the data subject agrees to her/his processing of personal data for a given purpose".
Kenya	"any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject".
San Marino	"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".
South Africa (POPIA)	"any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information".

Interestingly, the British Virgin Islands and South Korea did not define the term, however provisions were made for consent within the legislations. With the exception of South Africa, where the legal age was stipulated as 18, the overall age of consent varied from 13 – 16 years. However, a parent or legal guardian can consent on behalf of a minor.

▪ Legitimate interests

The majority of the policy documents, with the exception of the USA and New Zealand, included a condition under which a responsible party, data controller or even a third party may process personal information for legitimate interests. Thus, any form of processing may, technically, be carried out for any acceptable purpose. The specific condition is presented below for each corresponding country:

EU: *"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".*

South Korea: *"where it is necessary to attain the justifiable interest of a personal information controller, which such interest is manifestly superior to the rights of the data subject. In such cases, processing shall be allowed only to the extent the processing is substantially related to the justifiable interest of the personal information controller and does not go beyond a reasonable scope".*

Brazil: *"when necessary to fulfil the legitimate interests of the controller or a third party, except when the data subject's fundamental rights and liberties which require personal data protection prevail".*

British Virgin Islands: *“(a) the personal data is [are] processed for a lawful purpose directly related to an activity of the data controller; (b) the processing of the personal data is necessary for, or directly related to that purpose; and (c) the personal data is [are] adequate but not excessive in relation to that purpose”.*

Egypt: *“allowing the controller to perform his obligations or any relevant person to practice his legitimate rights, unless such matter contradicts the basic rights and freedoms of the data subject”.*

Kenya: *“for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is [are] disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject”.*

South Africa: *“processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied”.*

With the exception of South Africa, the countries specified that the legitimate interest of the responsible party, data controller or third party should not outweigh the rights of the data subject within the extracts. However, South Africa made this provision in clause 9 of the POPI Act: “personal information must be processed — (a) lawfully; and (b) in a reasonable manner that does not infringe the privacy of the data subject”.

In terms of lawful processing, legitimate interests as a reason could be interpreted and applied flexibly and the necessity of processing was left open to the interpretation of the responsible party, data controller or third party.

Finding 28: Continuous revision of the principles for processing personal information was required, given the pervasive nature of advancing technologies and changing areas of its application.

Finding 29: The utilisation of smart devices and IoT environments was contingent on consent for use of data which did not allow for expressive and informed user consent.

Finding 30: Conditions were specified for the basis of lawful processing of personal information without the expressed consent of the data subject which might jeopardise the subject's data privacy control and permission rights.

4.4.2.3.1.3 Individual rights

In addition to the principles discussed in the above section, the policy documents also specified the rights of data subjects pertaining to the protection of their personal information. Similarities and differences for the provision of the rights of data subjects existed across the policy documents. The rights of the data subjects and the descriptions, depicted by Table 4.17, were simplified for this study. The definitions for each of the specified rights are similar and, in some cases, self-explanatory, for instance the right to: access, rectification, erasure, object, consent and revoke consent. The individual's rights in relation to restriction of processing, data portability, no profiling or automated decision-making, to know and be informed are expanded below.

- The right to restriction of processing, allowed individuals to limit the processing of their personal information, however storage of the information was allowed. The circumstances under which an individual can restrict processing included:
 - The data accuracy was in doubt.
 - The data were unlawfully processed instead of requesting for it to be erased.
 - The data subject requested the restriction.
 - The data were no longer needed by the data controller.
 - An objection has been logged by the data subject.
- Under the right to data portability, individuals were permitted to receive and move the personal information they have provided to another controller and across environments without jeopardising the security and usability of the information.
- The right to no profiling or automated decision-making, covered aspects related to decisions made, without human intervention, on the eligibility of an individual for certain services such as online bank loans. Furthermore, an individual had the right to not be profiled based on automated methods pertaining to their digital activity.
- The right to know or be informed were similar rights, but termed differently in the policy documents. Effectively, this right allowed an individual to have knowledge about the collection and utilisation of their personal information, thus fulfilling the transparency requirement of the majority of the policy documents.

Table 4.17: Right of the data subject in relation to the processing of personal information

Rights	Description
Europe (GDPR)	
1. Right to be informed	Individuals have the right to be informed about the collection and use of their personal data.
2. Right of access	Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
3. Right to rectification	Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.
4. Right to erasure	Individuals have the right to have their personal data erased.
5. Right to restriction of processing	Individuals have the right to request the restriction or suppression of their personal data.
6. Right to data portability	Allows individuals to obtain and reuse their personal data for their own purposes across different services.
7. Right to object	The right to object to the processing of their personal data in certain circumstances.
8. Right to no profiling / no automated decision-making	Individuals have the right to not be profiled or decisions made concerning them based solely by automated means
San Marino	
1. Right to be informed	Individuals have the right to be informed about the collection and use of their personal data.
2. Right of access	Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
3. Right to rectification	Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.
4. Right to erasure	Individuals have the right to have their personal data erased.
5. Right to restriction of processing	Individuals have the right to request the restriction or suppression of their personal data.
6. Right to data portability	Allows individuals to obtain and reuse their personal data for their own purposes across different services.
7. Right to object	The right to object to the processing of their personal data in certain circumstances.
8. Right to no profiling / no automated decision-making	Individuals have the right to not be profiled or decisions made concerning them based solely by automated means
South Korea	
1. Right to be informed	Individuals have the right to be informed about the collection and use of their personal data.
2. Right to consent	The right to determine whether or not to consent and the scope of consent regarding the processing of such personal information.
3. Right to access	Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
4. Right to object	The right to object to the processing of their personal data in certain circumstances.
5. Right to rectification	Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.
New Zealand	
1. Right to access	Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
2. Right to correction	An individual may request the correction of personal information held
Brazil	
1. Right to be informed	Individuals have the right to be informed about the collection and use of their personal data.
2. Right of access	Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
3. Right to rectification	Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.
4. Right to restriction of direct marketing	Individuals have the right to not have personal information processed for purposes of direct marketing by means of unsolicited electronic communications.

5. Right to data portability	Allows individuals to obtain and reuse their personal data for their own purposes across different services.
6. Right to erasure	Individuals have the right to have their personal data erased.
7. Right to revoke consent	Individuals have the right to revoke consent previous given.
British Virgin Islands	
1. Right of access	Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
2. Right to rectification	Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.
3. Right to know	Individuals have the right to know about the personal information a business collects about them and how it is used and shared.
4. Right to restriction of direct marketing	Individuals have the right to not have personal information processed for purposes of direct marketing by means of unsolicited electronic communications.
Egypt	
1. Right of access	Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
2. Right to revoke consent	Individuals have the right to revoke consent previous given.
3. Right to rectification	Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.
4. Right to restriction	Individuals have the right to limit the scope of processing.
5. Right to know	Individuals have the right to know about the personal information a business collects about them and how it is used and shared.
6. Right to object	The right to object to the processing of their personal data in certain circumstances.
Kenya	
1. Right to be informed	Individuals have the right to be informed about the collection and use of their personal data.
2. Right of access	Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
3. Right to object	The right to object to the processing of their personal data in certain circumstances.
4. Right to rectification	Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.
5. Right to erasure	Individuals have the right to have their personal data erased.
USA	
1. Right to know	Consumers have the right to know about the personal information a business collects about them and how it is used and shared
2. Right to deletion	Consumers have the right to delete personal information collected from them (with some exceptions)
3. Right to opt-out	Consumers have the right to opt-out of the sale of their personal information.
4. Right of access	Consumers have the right to access and receive a copy of their personal data, and other supplementary information.
5. Right to non-discrimination	Consumers have the right to non-discrimination for exercising their CCPA rights.
South Africa	
1. Right to be informed	Individuals have the right to be informed about the collection and use of their personal data.
2. Right of access	Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
3. Right to rectification	Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.
4. Right to object	The right to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information
5. Right to restriction of direct marketing	Individuals have the right to not have personal information processed for purposes of direct marketing by means of unsolicited electronic communications.

6. Right to no profiling / no automated decision-making	Individuals have the right to not be profiled or decisions made concerning them based solely by automated means.
7. Right to erasure	Individuals have the right to have their personal data erased.
8. Right to lodge a complaint	Individuals have the right to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information.
9. Right to institute civil action	The right to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information.

Finding 31: The provision of rights for individuals should underpin the actions of responsible parties (controllers and processors) in terms of their obligations towards the data subjects.

4.4.2.3.1.4 Responsible parties, operators and supervision

The obligation of upholding the principles and observing the rights of the data subjects fell to data custodians that the majority of the countries defined as controllers and processors. Other terms used in the description of the data custodians were *personal information controllers* in South Korea, *data controllers* and *data processors* in Kenya and the British Virgin Islands. New Zealand extensively used the term, *agency*, but did not define it in terms of data custodians. South Africa employed the terms, *responsible parties* and *operators* which have been adopted by this study. Table 4.18 illustrates the terms and the definitions per country.

A clear distinction between controllers and processors were made by the majority of the countries. A controller could be seen as the entity that determined the purpose and means of processing personal data, whereas the processor was the entity that processed the personal data on behalf of the controller. The onus rests with the controller to assess the competency of the processor to process personal information, as well as ensuring the compliance of both entities.

South Korea's personal information controller related to the entity that, directly or indirectly, processed personal information. A service provider as defined by the USA related to the entity that processed information on behalf of a business.

For South Africa, the term, *responsible party* referred to the entity that established processing purpose and means; *operator* has been defined as the entity that, on behalf of the responsible party, processed personal information. It was the duty of the responsible party to contractually ensure that the operator employed reasonable measures for securing the integrity and confidentiality of personal information, and ultimately assuring compliance.

Table 4.18 Definitions for the responsible parties and operators

Country	Term	Definition	Term	Definition
EU (GDPR)	Controller	“means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law”.	Processor	“means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.
San Marino	Controller	“means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law”.	Processor	“means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.
Brazil	Controller	“natural person or legal entity, of public or private law, that has competence to make the decisions regarding the processing of personal data”.	Processor	“natural person or legal entity, of public or private law, that processes personal data in the name of the controller”.
British Virgin Islands	Data Controller	“means a person who either alone or jointly or in common with other persons processes any personal data, or has control over, or authorises the processing of any personal data, but does not include a data processor”.	Data Processor	“means a person who, processes data on behalf of a data controller, but does not include an employee of the data controller”.
Kenya	Data Controller	“means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data”.	Data Processor	“means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller”.
Egypt	Controller	“any natural or juristic person who has - by virtue of the nature of his activities - the right to obtain Personal Data and to specify the method and criteria of retaining, processing or controlling such data according to a specific purpose or to his activities”.	Processor	“any competent natural or juristic person by virtue of the nature of his work, to process Personal Data for his benefit or for the benefit of the Controller by way of an agreement with the Controller and in accordance with his instructions”.
South Africa (POPIA)	Responsible Party	“means 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”.	Operator	“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”.
South Korea	Personal Information Controller	“means a public institution, legal person, organization, individual, etc. that processes personal information directly or indirectly to operate the personal information files as part of its activities”.		

USA (CCPA)	Service Provider	“means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business”.
------------	------------------	--

Other roles in terms of the supervision of the stipulations specified by South Africa’s POPI Act included the establishment of the Information Regulator and the designation of information officers. In terms of the governance of data privacy, it was the duty of the Information Regulator to “monitor and enforce compliance” in relation to the POPI Act, as well as to deal with complaints “about alleged violations of the protection of personal information of data subjects”. Organisations were required to appoint an information officer to guarantee compliance with the Act and function as a liaison between the organisation and the Information Regulator. The responsibilities for the Information Regulator and information officer are shown in Table 4.19.

Table 4.19: Responsibilities of Information Regulator and information officers in South Africa

Roles	Responsibilities
Information Regulator	“(1) The powers, duties and functions of the Regulator in terms of this Act are— (a) to provide education by — (i) promoting an understanding and acceptance of the conditions for the lawful processing of personal information and of the objects of those conditions; (ii) undertaking educational programmes, for the purpose of promoting the protection of personal information, on the Regulator’s own behalf or in co-operation with other persons or authorities acting on behalf of the Regulator; (iii) making public statements in relation to any matter affecting the protection of the personal information of a data subject or of any class of data subjects; (iv) giving advice to data subjects in the exercise of their rights; and (v) providing advice, upon request or on its own initiative, to a Minister or a public or private body on their obligations under the provisions, and generally on any matter relevant to the operation, of this Act; (b) to monitor and enforce compliance by — (i) public and private bodies with the provisions of this Act; (ii) undertaking research into, and monitoring developments in, information processing and computer technology to ensure that any adverse effects of such developments on the protection of the personal information of data subjects are minimised, and reporting to the Minister the results of such research and monitoring; (iii) examining any proposed legislation, including subordinate legislation, or proposed policy of the Government that the Regulator considers may affect the protection of the personal information of data subjects, and reporting to the Minister the results of that examination; (iv) reporting upon request or on its own accord, to Parliament from time to time on any policy matter affecting the protection of the personal information of a data subject, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the personal information of a data subject; (v) submitting a report to Parliament, within five months of the end of its financial year, on all its activities in terms of this Act during that financial year; (vi) conducting an assessment, on its own initiative or when requested to do so, of a public or private body, in respect of the processing of personal information by that body for the purpose of ascertaining whether or not the information is processed according to the conditions for the lawful processing

	of personal information; (vii) monitoring the use of unique identifiers of data subjects, and reporting to Parliament from time to time on the results of that monitoring, including any recommendation relating to the need of, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the personal information of a data subject; (viii) maintaining, publishing and making available and providing copies of such registers as are prescribed in this Act; and (ix) examining any proposed legislation that makes provision for the— (aa) collection of personal information by any public or private body; or (bb) disclosure of personal information by one public or private body to any other public or private body, or both, to have particular regard, in the course of that examination, to the matters set out in section 44(2), in any case where the Regulator considers that the information might be used for the purposes of an information matching programme, and reporting to the Minister and Parliament the results of that examination; (c) to consult with interested parties by — (i) receiving and inviting representations from members of the public on any matter affecting the personal information of a data subject; (ii) co-operating on a national and international basis with other persons and bodies concerned with the protection of personal information; and (iii) acting as mediator between opposing parties on any matter that concerns the need for, or the desirability of, action by a responsible party in the interests of the protection of the personal information of a data subject; (d) to handle complaints by — (i) receiving and investigating complaints about alleged violations of the protection of personal information of data subjects and reporting to complainants in respect of such complaints; (ii) gathering such information as in the Regulator's opinion will assist the Regulator in discharging the duties and carrying out the Regulator's functions under this Act; (iii) attempting to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation; and (iv) serving any notices in terms of this Act and further promoting the resolution of disputes in accordance with the prescripts of this Act; (e) to conduct research and to report to Parliament — (i) from time to time on the desirability of the acceptance, by South Africa, of any international instrument relating to the protection of the personal information of a data subject; and (ii) on any other matter, including necessary legislative amendments, relating to protection of personal information that, in the Regulator's opinion, should be drawn to Parliament's attention; (f) in respect of codes of conduct to — (i) issue, from time to time, codes of conduct, amend codes and to revoke codes of conduct; (ii) make guidelines to assist bodies to develop codes of conduct or to apply codes of conduct; and (iii) consider afresh, upon application, determinations by adjudicators under approved codes of conduct; (g) to facilitate cross-border cooperation in the enforcement of privacy laws by participating in any initiative that is aimed at such cooperation; (h) in general to — (i) do anything incidental or conducive to the performance of any of the preceding functions; (ii) exercise and perform such other functions, powers, and duties as are conferred or imposed on the Regulator by or under this Act or any other legislation; (iii) require the responsible party to disclose to any person affected by a compromise to the integrity or confidentiality of personal information, such compromise in accordance with section 22; and (iv) exercise the powers conferred upon the Regulator by this Act in matters relating to the access of information as provided by the Promotion of Access to Information Act".
Information Officer	"An information officer's responsibilities include — (a) the encouragement of compliance, by the body, with the conditions for the lawful processing of personal information; (b) dealing with requests made to the body pursuant to this Act; (c) working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to the body; (d) otherwise ensuring compliance by the body with the provisions of this Act; and (e) as may be prescribed".

Finding 32: Definitive roles were specified for the responsibilities of processing personal information which ranged from country to country.

Finding 33: *Responsible party* referred to the entity that established processing purpose and means; whereas *operator* was defined as the entity that, on behalf of the responsible party, processed personal information.

Finding 34: Organisations were required to appoint an information officer to ensure compliance with the Act and function as a liaison between the organisation and the Information Regulator.

Finding 35: The duty of the Information Regulator was to monitor and enforce compliance in relation to the POPI Act, as well as to deal with complaints about suspected violations of the protection of personal information.

4.4.2.3.1.5 International transfers of personal information

The international transfer or cross-border flow of personal information referred to moving personal data from one country, across its international borders, to another country. Predominantly the countries prohibited the transfer of personal information to foreign countries or international organisations, with the following exceptions.

- The data subject consented to the transfer.
- A governing body decided that the country or international organisation provided adequate protection.
- The country or international organisation can provide similar provisions for the protection of personal information as those set out by the originating country's policy document.
- The country or international organisation can prove adequate protection of personal information.
- The country or international organisation can provide proof of appropriate security safeguards and the protection of personal information.

The European Court of Justice, in July 2020, ruled that the USA did not provide adequate protection for personal information (Fefer & Archick, 2021). Consequently, it was also limiting the international transfer of personal information between South Africa and the USA. Furthermore, a decision by the European Commission on the adequacy of the POPI Act was not in place, meaning that the transfer of personal information between the EU and South Africa based on adequate protection, was not possible at that moment. The implication of such restrictions impacted on the ability of South African organisations, especially data-driven

businesses to participate in global markets. Consequently, the lost revenue opportunities had a negative effect on the economy.

Finding 36: The restrictions on the international transfer of personal information impacted on the ability of South African organisations to participate in the global market, especially data-driven cross-border organisations like those operating in the IoT environment.

4.4.2.3.2 Theme: Data privacy

4.4.2.3.2.1 Breaches of personal information

Four of the policy documents defined the term, *personal data breach*, the EU, San Marino and Kenya provided the following definition:

a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

On the other hand, Egypt defined a personal data breach as:

any unauthorized or illegal access to personal data, or any other illegitimate operation to reproduce, transmit, distribute, exchange, transfer, or circulate which aims to expose or disclose such personal data, or damage or edit it while it is being stored, transferred or processed.

Although the majority of the countries did not define the term, personal data breach, they provided stipulations for notification should a data breach occur. The overall requirement was for written notice to the responsible authority in each country and the data subject after becoming aware of the breach, generally within 72 hours. However, notification to data subjects might be delayed if, in doing so, the investigation into the breach was compromised or it violated national security or infringed on the rights of others.

South Korea and South Africa did not specify a particular time frame for notification, but required the notice to be “without delay” and “as soon as reasonably possible” following knowledge of the breach. In the case of South Africa, the absence of a definition for a personal information breach, as well as the vague requirement for the notification of a breach in the POPI Act might have adverse implications on compliance. Consequently, in relation to a personal information breach incident, compliance was left to the interpretation of the responsible party.

Finding 37: In relation to the POPI Act, notification of a personal information breach incident and consequently compliance was left to the interpretation of the responsible party which contradicted the objectives of transparency and accountability.

4.4.2.4 Summary of findings

A summary of the findings for the document analysis, the related sub-themes and themes can be found in Table 4.20.

Table 4.20: Findings, sub-themes and themes

Findings	Sub-Themes	Themes
Finding 27: In relation to data generated by automated devices, like those found in IoT environments, there was no explicit definition regarding what constitute direct or indirect data.	Personal information or personal data definition	REGULATION
Finding 28: Continuous revision of the principles for processing personal information was required given the pervasive nature of advancing technologies and changing areas of its application.	Processing personal information	
Finding 29: The utilisation of smart devices and IoT environments was contingent on consent for use of data, which did not allow for expressive and informed user consent.		
Finding 30: Conditions were specified for the basis of lawful processing of personal information without the expressed consent of the data subject, which might jeopardise the subject's data privacy control and permission rights.		
Finding 31: The provision of rights for individuals should underpin the actions of responsible parties (controllers and processors) in terms of their obligations towards the data subjects.	Individual rights	
Finding 32: Definitive roles were specified for the responsibilities of processing personal information which ranged from country to country.	Responsible parties, operators and supervision	
Finding 33: <i>Responsible party</i> referred to the entity that established processing purpose and means, whereas <i>operator</i> was defined as the entity that, on behalf of the responsible party, processed personal information.		
Finding 34: Organisations were required to appoint an information officer to ensure compliance with the Act and function as a liaison between the organisation and the Information Regulator.		
Finding 35: The duty of the Information Regulator was to monitor and enforce compliance in relation to the POPI Act, as well as to deal with complaints about suspected violations of the protection of personal information.		
Finding 36: The restrictions on the international transfer of personal information impacted on the ability of South African organisations to participate in the global market, especially data-driven cross-border organisations like those operating in the IoT environment.	International transfers of personal information	
Finding 37: In relation to the POPI Act, notification of a personal information breach incident and consequently compliance was left to the interpretation of the responsible party which contradicted the objective of transparency and accountability.	Breaches of personal information	DATA PRIVACY

4.5 Summary

In this chapter, a detailed discussion on the analysis and findings was presented, commencing with an introduction of the focus of the chapter, followed by the context, the case, and the participants of the study.

Fifteen IoT-based organisations, ranging from micro (1-10) to large (251-500) enterprises, spread across four provinces (Western Cape, Eastern Cape, KwaZulu-Natal and Gauteng) in South Africa contributed to the study. The participants included high-level executives within the organisations and data were collected via semi-structured interviews.

Data collection also involved a document review or analysis of countries that have updated their data protection policies between 2018–2021. Following an internet search, twenty-five countries with updated policies were identified from Europe, North America, Asia-Pacific, Central and South America, the Caribbean, the Middle-East and Africa. Exclusionary criteria, such as countries without an English version of their policies were employed and ten countries (EU, San Marino, USA, South Korea, New Zealand, Brazil, British Virgin Islands, Egypt, Kenya and South Africa) were selected.

A thematic analysis was employed for both the interview data and the document analysis. The process involved the six phase approach that included: familiarizing yourself with your data; generating initial codes; searching for themes; reviewing themes; defining and naming themes; and producing a report. Following an iteration of the six phases of thematic analysis, the interview data generated seventy-seven codes, ten categories and five overarching themes. In addition to that, the document analysis generated thirteen categories and six sub-themes which were grouped under two of the five themes identified during the interview data analysis.

The findings from the interview data analysis were presented in relation to the sub-questions and corresponding interview questions, as well as the summary of findings for the four sub-questions. A summary of all the twenty-seven headline findings, the related categories and themes and the corresponding sub-questions were also illustrated. The chapter concludes with the headline findings from the document analysis presented in relation to the sub-themes and the overarching themes.

CHAPTER FIVE: INTERPRETATION OF FINDINGS

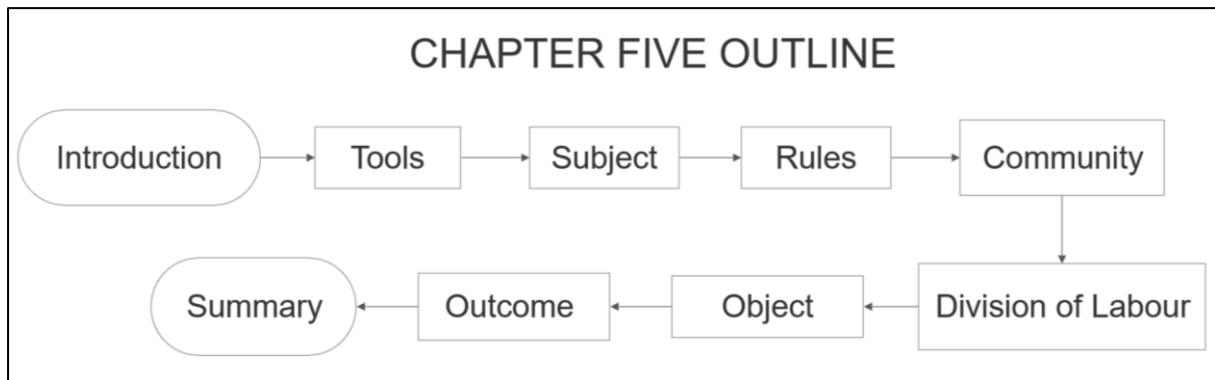


Figure 5.1: Chapter Five outline

5.1 Introduction

Activity Theory (AT), according to Nardi (1995:4) “offers a set of perspectives on human activity and a set of concepts for describing that activity” by providing a data analysis framework for understanding use and usability issues that affect systems and the comprehension of user behaviour. This research utilised the components of the activity system as a theoretical lens to study and analyse the interactions and data patterns from the study. The AT was applied to provide a deeper insight in the context of the network of activities involved in the process of fulfilling a specific outcome related to the objectives of the study. Therefore, the components of the theory were used to explain the findings in relation to each set of interlocking activities and the roles played towards fulfilment of the outcome of effective data privacy governance in IoT environments in South Africa.

The chapter is divided into nine sections as displayed in Figure 5.1 above. Section 5.2 describes the subject component in their utilisation of smart devices, applications and IoT environments. The focus of section 5.3 is on the tools component in the activity system which facilitates the processing and governance of data by the subjects towards fulfilling the object in the activity system. In section 5.4 the rules component is presented in relation to the POPI Act that sets out the stipulations for the protection of personal information. Section 5.5 identifies the members of the community component which included the users of smart devices, applications and IoT environments, the responsible parties and operators, the information officers and the Information Regulator. In section 5.6, the roles and responsibilities of the community in relation to the object are highlighted. Sections 5.7 and 5.8 show the interplay of the various components in relation to achieving the goal and the outcome. The chapter concludes with a summary of the chapter in section 5.9.

A brief description of each component in the AT is presented in Table 5.1, as well as the applicable context in relation to the study.

Table 5.1: Components of an activity system, description and context

Components	Description	Context of the study
Tools	A variety of tools or artefacts are contained in an activity in a mediating role (Kuutti, 1995).	Smart devices, applications and IoT environments. Security measures and protocols, Regulatory compliance measures
Subject	The source of activity is always the subject and its interaction in the world (Roos, 2012).	Users of smart devices, applications and IoT environments. Responsible parties and operators (aka data controllers and processors), Information officers, Information Regulator
Rules	These are norms and rules that govern subjects' activity in a community (Allen et al., 2011).	Data Privacy or Protection Regulation, Compliance Contracts / Agreements
Community	This involves subjects performing their activities, individually or in groups and their interactions with other subjects who utilise a similar object (Kuutti, 1995).	Users of smart devices, applications and IoT environments. Responsible parties and operators (aka data controllers and processors), Information Regulator
Division of Labour	This represents the administration of a community, i.e. the roles and responsibilities of the subjects (Kuutti, 1995).	Roles and responsibilities of the subjects in the community
Object	An object can be material in nature or less physical, for instance a plan or an idea (ibid, 1996).	The establishment of guidelines and best practices for the governance data privacy in IoT environments in South Africa
Outcome	This involves the transformation of the object based on activities of the subject (ibidi, 1996).	The effective governance of data privacy in IoT environments in South Africa

Depicted in Figure 5.2 are the components of Engeström's activity system in relation to the study, each of which are discussed in this section.

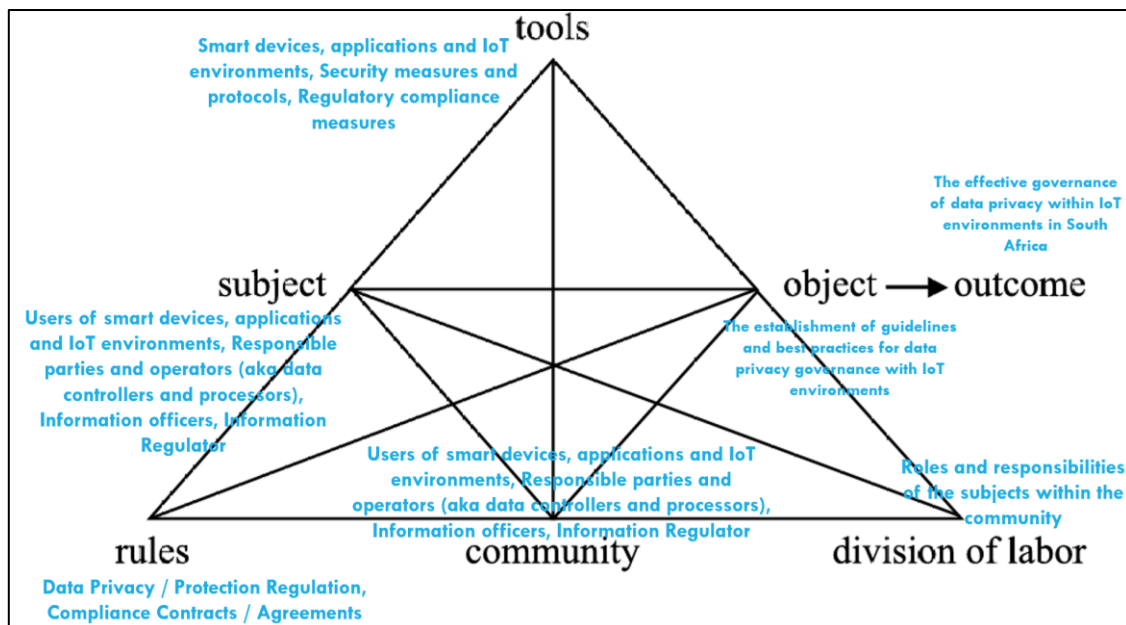


Figure 5.2: Mapping of study's finding to activity system, adapted from (Engeström, 1987, cited in Allen et al., 2011:781)

In the next section, the components of the AT are used to explain the corresponding findings through the lens of the theory. The application of the theory is presented descriptively to better understand the attributed meanings and relationships that exist in the network of activities which inform effective data privacy governance in IoT environments in South Africa.

5.2 Subject

The subject in an activity system refers to the source or undertaker of an activity (Roos, 2012). In terms of the activity system for data privacy governance, the subject can be classified under two main categories: a) knowledge of subjects on data privacy regulation; b) actions of subjects in the governance of data privacy. The activities of the subjects in the system facilitate the provision of data and the transformation process of data. Therefore, the subjects play a pivotal role in the activity system of data privacy governance through the interaction with the tools to produce data. This action subsequently leads to the processing of data by appointed subjects (responsible parties and operators, who must act in accordance with defined rules. The findings describing the knowledge of subjects on data privacy regulation and the actions of subjects in the activity of data privacy governance in IoT environments are presented below.

▪ Knowledge of subjects on data privacy regulation

The findings suggested that knowledge of regulation that governed the protection of personal information existed amongst the community, however, “in-depth and comprehensive understanding” was lacking (**Finding 7**). In addition to that, **Finding 16** exhibited a knowledge of the EU’s GDPR due to compliance with international regulations. Comparatively, participants acknowledged that there were similarities between the POPI Act and GDPR, with one key exception in the fact that the POPI Act extended the protection of personal information to juristic persons (**Finding 15**). The knowledge of data privacy regulations that dealt with personal information was an important aspect for facilitating users’ consent for use of their data. Although users did not form part of this study, the activity system of data privacy governance started at the point of users’ data being collected or generated from services rendered. For the user subjects, the utilisation of smart devices and IoT environments was frequently contingent on blanket consent for the collection and processing of their data (**Finding 29**). Thus, in terms of the stipulations related to consent in the POPI Act and the governance of data privacy in IoT environments, it can be deduced that consent was often not freely given, nor was it specific or informed.

▪ Actions of subjects in the governance of data privacy

The way in which subjects use smart devices and IoT environments and the actions of responsible parties (controllers and processors) have a bearing on the governance of data

privacy. **Finding 3** stated that “the human factor and their associated actions presented the biggest risk to IoT-based organisations” and consequently the governance of data privacy. As a result, the majority of IoT-based organisations relied on the security protocols of third-party vendors to protect their client’s personal information (**Finding 20**). In relation to legislation, the findings determined that “definitive roles were specified for the responsibilities of processing personal information” (**Finding 32**). Furthermore, **Finding 31** concluded: “The provision of rights for individuals should underpin the actions of responsible parties (controllers and processors) in terms of the legislation”. Therefore, the actions of subjects served as the triggering effect on the activities in the system, through the interaction with the tools towards fulfilling the object of the activity.

The major activity in terms of the governance of data privacy in IoT environments (object) centres around the users (subject) of smart devices and responsible parties’ (controllers and processors) management of user data in IoT environments.

The related findings in terms of the subjects are portrayed in Table 5.2.

Table 5.2: Findings related to Subject

Findings	Categories	Themes
Finding 3: There was consensus that the human factor and the associated actions presented the biggest risk to IoT-based organisations in terms of the data privacy protection.	Challenges of securing personal information	DATA PRIVACY
Finding 7: Predominantly, participants demonstrated some knowledge of the POPI Act, however, it did not depict in-depth and comprehensive understanding of data privacy law in South Africa.	Knowledge of regulations	REGULATION
Finding 15: There was a perception that GDPR was relatively close to the POPI Act, with minor differences in the application, while the definition of an entity’s protection of personal information extended to juristic persons in the POPI Act.		
Finding 16: The majority of participants displayed knowledge of the GDPR, because of the need to comply with international laws while dealing with global parties in their perspective marketplaces.		
Finding 20: Responses indicated that the majority of IoT-based organisations depended on third-party organisations to provide security protocols for the protection and use of client’s personal information.	Security in IoT Environments	DATA SECURITY
Finding 29: The utilisation of smart devices and IoT environments were contingent on consent for use of data which did not allow for expressive and informed user consent.	Processing personal information	REGULATION
Finding 31: The provision of rights for individuals should underpin the actions of responsible parties (controllers and processors) in terms of their obligations towards the data subjects.	Individual rights	
Finding 32: Definitive roles were specified for the responsibilities of processing personal information.	Responsible parties, operators and supervision	

5.3 Tools

The subject-object relationship is transformed by the tool and can include tangible and intangible tools (Kuutti, 1995). Through the findings, this study identified tools utilised by the subjects for the processing of data and the actualisation of the object in terms of established protocols, process and standards for compliance with regulatory requirements. Smart devices and IoT environments were primarily utilised by users, who had to provide consent, to perform tasks or actions. **Finding 29** determined that the use of smart devices and IoT environments were often contingent on blanket consent from users for the collection and processing of their data. Thus, it can be argued that consent was rarely given freely, nor was it specific and informed. It was difficult to guarantee the transparency of activities that resulted in data privacy governance, if the privacy of the users were compromised at the start of the service, due to restrictive conditions and uninformed permissions for the collection and processing of their data. The findings underlined a requirement for effective measures (tools) that enabled users (subject) to utilise smart devices in IoT environments (tools) without compromising their personal information (object).

To mitigate threats to data privacy in IoT environments, there must be established standards and protocols in place as well as contingency plans in the event of breaches. **Finding 6** concluded that the establishment of “comprehensive security measures was (sic) vital”. Policies have been created to ensure that a system was in place to uphold standards when dealing with users’ data. It was reported in **Finding 14** that most organisations have put in place distinctly diverse measures to accomplish the conditions stipulated by the POPI Act for data governance. Some of the measures were captured in **Finding 23 and 18** which included “management level access, preventative and protection controls, architectural oversight for monetary transactions and daily server mirroring” and “encryption and providing secure data storage”. The establishment of measures and the adoption of protocols or standards set the tone for establishing best practices and guidelines towards regulatory compliance in the activity system of data privacy governance.

In terms of the governance of data privacy in IoT environments, the findings also established that unsecured devices and networks posed a high risk (**Finding 4**). Security of devices in the networked IoT environment was imperative, because of the level and impact of vulnerabilities and exposure connected devices might pose to users’ data. It was established that the security of connected devices in IoT environments posed the biggest challenge when it came to the protection of personal information (**Finding 19**). Furthermore, it was determined that in IoT environments, the emphasis was on securing and controlling access due to the interconnectivity of devices, as well as the widespread nature of the networks and the

vulnerability of having various endpoints (**Finding 24 and 25**). The nature of the interconnectivity of devices and the associated risk to data privacy presented a serious threat in the activity system and the actualisation of the outcome. Thus, these challenges could derail the effective governance of data privacy in IoT environments if proper security and contingency measures were not put in place.

Moreover, the findings indicated that the majority of IoT-based organisations depended on third-party organisations to provide security protocols for the protection and use of client's personal information (**Finding 20**). Responses highlighted a reliance on third party suppliers, such as Sigfox, AWS, Microsoft Azure and Google Cloud for the application of security protocols in terms of the protection of personal information from **Finding 21**. The security of user data was an obligation placed on the responsible parties by the users and legislation, therefore appropriate tools had to be deployed to fulfil this duty. Securing user data in line with the best practices and regulations was a key activity in the system which enabled the governance of data privacy in a manner that ensured transparency and compliance.

In summary, the related findings conveyed the understanding of the relationships facilitated by the tools employed in an IoT environment. The findings revealed the network of the relationship between the components resulting from the subjects' use of the tools to facilitate data and the establishment of guidelines and best practices towards the effective governance of data privacy.

The related findings in terms of the tools component of AT are portrayed in Table 5.3.

Table 5.3: Findings related to Tools

Findings	Categories	Themes
Finding 4: In relation to protecting against data breaches, it was reported that unsecured devices and networks posed a high risk to IoT-based organisations.	Challenges of securing personal information	DATA PRIVACY
Finding 6: There was an understanding that establishing comprehensive security measures was vital to mitigating threats to data privacy in IoT environments.	Protecting personal information	
Finding 14: Most organisations have put in place distinctly diverse measures to accomplish the conditions stipulated by the POPI Act for data governance, in line with adhering to personal information protection, while a few depended on third-party suppliers to ensure compliance.	Regulation of personal information	REGULATION
Finding 18: To facilitate the protection of personal information, measures such as encryption and providing secure data storage were applied.		
Finding 19: It was established that the security of connected devices in IoT environments posed the		

biggest challenge when it came to the protection of personal information, with other constraints such as cost, and maintenance voiced as well.	Security in IoT environments	DATA SECURITY
Finding 20: Responses indicated that the majority of IoT-based organisations depended on third-party organisations to provide security protocols for the protection and use of client's personal information.		
Finding 21: The third-party customised technology used for securing data from IoT devices included Sigfox, AWS, Microsoft Azure and Google Cloud for their network and Cloud infrastructures, with in-house solutions like AES also being utilised.		
Finding 23: Suggested solutions to mitigate unauthorised access and use of personal data included management level access, preventative and protection controls, architectural oversight for monetary transactions and daily server mirroring.	System vulnerabilities	
Finding 24: There was a perception that conventional IT systems focused more on people and personal information than IoT environments, where the focus was more on securing and controlling access due to the interconnectivity aspect of IoT environments.	Data governance and IoT	INTERNET OF THINGS (IOT)
Finding 25: It was believed that the security risks and procedures for conventional systems and IoT environments were similar, however for IoT there were added components such as the devices, the widespread nature of the networks and the vulnerability of having various endpoints.		
Finding 29: The utilisation of smart devices and IoT environments was contingent on consent for use of data which did not allow for expressive and informed user consent.	Processing personal information	REGULATION

5.4 Rules

The rules relate to the interaction and action restrictions inclusive of conventions, norms and regulations (Ditsa, 2003). In South Africa, the POPI Act sets out the stipulations for the protection of personal information. The establishment of regulations and standards to address the growing threat of data privacy in the digital space was the basis for the recent upgrades of privacy protection policy documents in many countries. These policies (rules) play an important role in the governance of data privacy by providing the conditions and stipulations under which user data is managed. **Finding 30** determined that conditions existed in the regulations for lawful processing of personal information without the consent of the data subject. In addition to that, the global implementation of data protection regulations, specifically conditions related to the international transfer of personal information, “force organisations to decentralise their databases which limit the flow of information as a compliance for cross-border business operations” (**Findings 17 and 36**).

Finding 27 established that “in relation to data generated by automated devices, like those found in IoT environments, there were no explicit definitions regarding the direct or indirect use of data”. Moreover, the findings indicated that in terms of technological developments and advancements, legislation was playing catch up and thus required continuous updates in line

with emerging technology trends (**Findings 8, 9 and 28**). The advancement in technology and its impact on data privacy had to be monitored continuously and appropriate steps had to be taken to mitigate the threats posed to data privacy governance. Based on the findings, the current situation created a gap in the activity system where the rules were not in tandem with the dynamic nature of data privacy governance in IoT environments. This had serious implications for the effect and applicability of compliance.

With regard to managing data in IoT environments, the findings determined that “the POPI Act does not adequately address” the requirements for data management (**Finding 10**). Participants were of the opinion that the POPI Act lacked clarity in terms of the management of data in IoT environments. Furthermore, participants felt that a lot of the stipulations in the Act were left open to interpretation. Additionally, legislation pertaining to technologies such as IoT should employ the expertise of knowledgeable people in the field (**Finding 11**). It was believed that the persons involved in drafting the POPI Act had no technical background and thus had not heard of IoT, nor had any real experience in the management of data in IoT environments. Therefore, it could be established that by not employing technology experts in determining stipulations that primarily provided guidelines for the processing of personal data, was an oversight with serious implications for the governance of data privacy.

Thus, the establishment of best practices and guidelines for the governance of data privacy in IoT environments (object) required specific legislation (rules) that addressed the uniqueness of IoT environments through the involvement of knowledgeable individuals (community) in determining the rules of data privacy governance.

The related findings in terms of the rules are portrayed in Table 5.4.

Table 5.4: Findings related to Rules

Findings	Categories	Themes
Finding 8: Responses indicated that legislation was behind in terms of technological developments and advancements, and the POPI Act was bound to fail due to implementation and enforcement challenges.	Knowledge of regulations	REGULATION
Finding 9: Participants acknowledged that the POPI Act needed to be updated continuously in line with advancing technologies, global trends and developments.		
Finding 10: The participants were mainly in agreement that the POPI Act did not adequately address the uniqueness of managing data in IoT environments.	Data governance and IoT	
Finding 11: It was suggested that data privacy regulation relating to technologies such as IoT had to		

involve input from people with requisite technical expertise.		
Finding 17: The implementation of diverse country specific data regulations forced organisations to decentralise their databases which limited the flow of information as a compliance for cross-border business operations.	Security in IoT environments	DATA SECURITY
Finding 27: In relation to data generated by automated devices, like those found in IoT environments, there were no explicit definitions regarding the direct or indirect use of data.	Personal information or personal data definition	REGULATION
Finding 28: Continuous revision of the principles for processing personal information was required, given the pervasive nature of advancing technologies.	Processing personal information	
Finding 30: Conditions were specified for the lawful basis of processing personal information without the consent of the data subject.		
Finding 35: The restrictions on the international transfer of personal information impacted the ability of South African organisations to participate in the global market, especially data-driven cross-border organisations like those operating in the IoT environment.	International transfers of personal information	

5.5 Community

The community involves those persons performing the activities, individually or in groups and their interactions with other subjects who utilise a similar object (Kuutti, 1995). The activity of data privacy governance in the community commences with the users' utilisation of a smart device, operating in an application area of an IoT environment where user data is generated by the connected devices. Subsequently, the data is then processed and transformed by the responsible parties (controllers and processors) for operational purpose according to internal protocols and processes. Afterwards the use of the data then becomes subjected to a process of standards and oversight by the information officer, in compliance with the regulations administered by the Information Regulator. Each member of the community has a relative effect on the other, through the roles they play, towards actualisation of the object and realisation of the outcome. Thus, it has been established that the effective governance of data privacy in IoT environments was contingent on the community's roles and actions, which dictated the level of interaction in the activity system.

The POPI Act identified specific actors in the community and their definitive roles and responsibilities (**Findings 32**). The *responsible party* referred to the entity that established processing purpose and means, whereas the *operator* was defined as the entity that, on behalf of the responsible party, processed personal information (**Finding 33**). As per **Finding 34**, stipulations were made in the POPI Act for the designation of an information officer in organisations to ensure compliance. In addition, the information officer was required to act as a liaison between organisations and the Information Regulator who in turn was responsible for

monitoring and enforcing compliance as well as contended with suspected violations of the protection of personal information (**Finding 35**).

In the context of this study, responsible parties and operators, information officers and the Information Regulator, played prominent roles in the community in the activity system. Findings illustrated that although responsible parties, in the form of IoT-based organisations, lack “in-depth and comprehensive understanding” of the POPI Act, a basic understanding of the regulation in terms of the governance of data privacy was demonstrated (**Finding 7**). **Finding 5** implied that IoT-based organisations “had no real experience of data privacy infringement incidents”. However, **Finding 3** established responsible parties’ concern over the “human factor” and actions of community members presenting a major threat to protecting data privacy. This concern could be exacerbated by the responsible parties’ reliance on third party vendors, such as Sigfox, AWS, Microsoft Azure and Google Cloud to secure data, networks and infrastructures, thus presenting another layer of risk to user data (**Findings 20 and 21**).

The knowledge and expertise of the various actors in the community worked in unison to achieve the governance of data privacy in IoT environments (object).

The related findings in terms of the community are portrayed in Table 5.5.

Table 5.5: Findings related to Community

Findings	Categories	Themes
Finding 3: There was consensus that the human factor and the associated actions presented the biggest risk to IoT-based organisations in terms of the data privacy protection.	Challenges of securing personal information	DATA PRIVACY
Finding 5: Responses implied that the IoT-based organisations had no real experience of data privacy infringement incidents.	Knowledge of infringements	
Finding 7: Predominantly, participants demonstrated some knowledge of the POPI Act, however, it did not depict in-depth and comprehensive understanding of data privacy law in South Africa.	Knowledge of regulations	REGULATION
Finding 20: Responses indicated that the majority of IoT-based organisations depended on third-party organisations to provide security protocols for the protection and use of client’s personal information.	Security in IoT environments	DATA SECURITY
Finding 21: The third-party customised technology used for securing data from IoT devices included Sigfox, AWS, Microsoft Azure and Google Cloud for their network and Cloud infrastructures, with in-house solutions like AES also being utilised.		
Finding 31: The provision of rights for individuals should underpin the actions of responsible parties (controllers and processors) in terms of their obligations towards the data subjects.	Individual rights	

Finding 32: Definitive roles were specified for the responsibilities of processing personal information.	Responsible parties, operators and supervision	REGULATION
Finding 33: <i>Responsible party</i> referred to the entity that established processing purpose and means, whereas <i>operator</i> was defined as the entity that, on behalf of the responsible party, processed personal information.		
Finding 34: Organisations were required to appoint an information officer to ensure compliance with the Act and function as a liaison between the organisation and the Information Regulator.		
Finding 35: The duty of the Information Regulator was to monitor and enforce compliance in relation to the POPI Act as well as deal with complaints about suspected violations of the protection of personal information.		

5.6 Division of labour

Division of labour pertains to the distributions of the roles and responsibilities of the members of the community (Ditsa, 2003). In reference to the study, the findings concluded that the impact of the POPI Act on organisations was dependent on the nature and type of data being collected from the users as reported by **Finding 13**. Hence, the division of labour was between the responsible parties and operators' adherence to standards and best practices in compliance with regulations and the Information Regulator's enforcement of compliance. In the context of this study, findings relating to the division of labour distinctly addressed the roles and responsibilities of IoT-based organisations as responsible parties (data controllers), the appointed third parties as operators (data processors), information officers as compliance deputies in the organisations and the Information Regulator as the compliance officiator.

In relation to the POPI Act, **Finding 33** showed that the responsibilities for the lawful processing of personal information rested with the responsible parties and operators. In the event of a data breach, **Finding 37** established that "notification of a personal information breach incident and consequently compliance, was left to the interpretation of the responsible party". The information officer was required to ensure that the responsible parties and operators processed information in a lawful and compliant manner as stipulated by the POPI Act (**Finding 34**). As well as function as a liaison between the responsible parties, operators and the Information Regulator, the information officer was responsible for monitoring and enforcing compliance with the POPI Act and investigated alleged infringements (**Finding 35**).

Regarding the responsible party for the processing of users' personal information, it was reported in **Finding 20** that IoT-based organisations largely depended on third-party vendors to provide security protocols for the protection and use of the client's personal information. **Finding 21** highlighted third-party customised technology used for securing data from IoT devices such as Sigfox, AWS, Microsoft Azure and Google Cloud. The third-party data processors played a prominent role in the security and safeguarding of users' data in the

activity system to ensure effective data privacy governance. **Finding 11** suggested that data privacy regulation, relating to technologies such as IoT, should involve input from people with requisite technical expertise. Stipulations were made in the POPI Act as part of the Information Regulator's duty "to consult with interested parties". Thus, not consulting technical experts in terms of data privacy regulation in IoT environments, could be seen as a dereliction of duty on the part of the Information Regulator.

Participants largely claimed that the impact of the POPI Act was administrative, with no evidence of enforcement of compliance and standards as indicated by **Finding 12**. In terms of POPI Act implementation, participants performed tasks such as "updating our forms and email policy", "lots of agreements, lots of footwork, lots of kind of internal policy things", getting all parties to "agree to an information to share template". Participants' opinions were reflective of the lack of visible engagement from the Information Regulator's office and the perceived generic requirement of the Act as being administrative in nature.

The findings suggested that the activity system required a symbiotic relationship of several actors (community) performing their designated roles and responsibilities (division of labour) towards achieving the object, in line with the stipulations (rules) necessary to ensure effective governance of data privacy (outcome).

The related findings in terms of the division of labour are portrayed in Table 5.6.

Table 5.6: Findings related to division of labour

Findings	Categories	Themes
Finding 11: It was suggested that data privacy regulation, relating to technologies such as IoT, should involve input from people with requisite technical expertise.	Data governance and IoT	REGULATION
Finding 12: Participants largely claimed that the impact of the POPI Act was administrative, with no evidence of enforcement of compliance and standards.	Regulation of personal information	REGULATION
Finding 13: It was established that the impact of the POPI Act on IoT-based organisations, was dependent on the nature and type of data being collected from the users.		
Finding 20: Responses indicated that the majority of IoT-based organisations depended on third-party organisations to provide security protocols for the protection and use of client's personal information.	Security within IoT environments	DATA SECURITY
Finding 21: The third -party customised technology used for securing data from IoT devices included Sigfox, AWS, Microsoft Azure and Google Cloud for their network and Cloud infrastructures, with in-house solutions like AES also being utilised.		

Finding 32: Definitive roles were specified for the responsibilities of processing personal information.	Responsible parties, operators and supervision	REGULATION
Finding 33: <i>Responsible party</i> referred to the entity that established processing purpose and means, whereas <i>operator</i> was defined as the entity that, on behalf of the responsible party, processed personal information.		
Finding 34: Organisations were required to appoint an information officer to ensure compliance with the Act and function as a liaison between the organisation and the Information Regulator.		
Finding 35: The duty of the Information Regulator was to monitor and enforce compliance in relation to the POPI Act as well as deal with complaints about suspected violations of the protection of personal information.		
Finding 37: In relation to the POPI Act, notification of a personal information breach incident and consequently compliance was left to the interpretation of the responsible party which contradicted the objective of transparency and accountability.	Breaches of personal information	DATA PRIVACY

5.7 Object

The object relates to that at which the activity is directed (Hashim & Jones, 2007). The object, in terms of this study was the establishment of best practices and guidelines for the governance of data privacy in IoT environments. The activities of the subject, mediated by the tools, governed by a set of rules applied in a community with distinct division of labour culminates in the actualisation of the object. The findings revealed that there were a number of challenges pertaining to the governance of data privacy in IoT environments. As earlier indicated, these challenges included the rise in data breaches (**Findings 1 and 2**) which was a cause for concern for the subjects, along with the knowledge expressed in regard to data privacy regulations. However, the greatest challenge in securing personal information related to human beings who, inadvertently or deliberately, exposed organisations to threat actors (**Finding 3**). Instances included employee action (social engineering), corporate espionage, ransomware attacks as well as scam calls and emails (**Finding 22**). The actions of subjects being the focal point of the activity system, initiated and dictated the level of interaction and inter-related activities in the system in actualising the object.

Threats such as hacking of smart devices (tools) posed a risk to personal information (**Finding 22**). As previously stated, the establishment of comprehensive security measures was vital to mitigating threats to data privacy in IoT environments (**Finding 6**). These measures included encryption, secure data storage and the mitigation of unauthorised access and use of personal data through “management level access, preventative and protection controls, architectural oversight for monetary transactions and daily server mirroring” (**Findings 18 and 23**). The security of connected devices in IoT environments posed the biggest challenge when it related to the protection of personal information (**Finding 19**). It was also established that IoT-based

organisations relied on the services of third-party vendors like Sigfox, AWS, Microsoft Azure and Google Cloud for data, network and infrastructure security (**Findings 20 and 21**).

As earlier discussed, the stipulations for the protection of personal information were set out by the POPI Act in South Africa. **Finding 2** suggested that actual incidents of data breaches were much higher than what was actually reported and participants agreed that the POPI Act did not adequately address the uniqueness of managing data in IoT environments (**Finding 10**). Thus, the effectiveness of the POPI Act as a deterrent to infringements was brought into question. **Finding 28** determined that the pervasive nature of advancing technologies, such as IoT, necessitated the continuous revision of the principles of processing personal information as well as the contributions of technical experts towards the establishment of best practices for the governance of data privacy in relation to IoT environments (**Finding 11**).

The afore-mentioned activities of community members pursuant to the establishment of guidelines and best practices for the governance of data privacy required clear specification and understanding. According to **Finding 32**, definitive roles were specified in the POPI Act for the responsibilities of processing personal information. These included responsible parties, operators, information officers and the Information Regulator. In terms of the governance of data privacy in IoT environments, the responsible party should determine the purpose and means of processing, whereas the operator was the entity that processed the personal information on behalf of the responsible party (**Finding 33**). The information officer should ensure compliance with the POPI Act and maintain adequate record keeping that needed to be provided as proof of compliance in the event of a breach (**Finding 34**). The duties of the Information Regulator included the monitoring and enforcement of compliance with the POPI Act as well as the investigation of alleged violations or breaches (**Finding 35**). The role of the Information Regulator was geared towards the object of establishing best practices and compliance within the activity system.

The establishment of best practices and guidelines (object) was necessitated by the increased number of data breaches affecting IoT environments (tools) and consequent infringements pertaining to the data privacy of users (subject). Also, the Information Regulator as a subject in the community played the important role of ensuring that the object was actualised through the established rules that governed the interrelated activities in the system.

The related findings in terms of the object are depicted in Table 5.7.

Table 5.7: Findings related to Object

Findings	Categories	Themes
Finding 1: There were deep-rooted concern and consternation about the upsurge in data breaches in South Africa, with a prediction that one of the biggest attacks in the near future would involve the IoT environment.	Data breaches	DATA PRIVACY
Finding 2: It was established that the actual number of incidents of data breaches were considerably higher than the high-profile infringements that were generally reported.		
Finding 3: There was consensus that the human factor and the associated actions presented the biggest risk to IoT-based organisations in terms of the data privacy protection.	Challenges of securing personal information	
Finding 6: There was an understanding that establishing comprehensive security measures were vital to mitigating threats to data privacy in IoT environments.		
Finding 10: The participants were mainly in agreement that the POPI Act did not adequately address the uniqueness of managing data in IoT environments	Data governance and IoT	REGULATION
Finding 11: It was suggested that data privacy regulation, relating to technologies such as IoT should involve input from people with requisite technical expertise.		
Finding 18: To facilitate the protection of personal information, measures such as encryption and providing secure data storage were applied.	Security within IoT environments	DATA SECURITY
Finding 19: It was established that the security of connected devices in IoT environments posed the biggest challenge when it related to the protection of personal information, with other constraints such as cost and maintenance voiced as well.		
Finding 20: Responses indicated that the majority of IoT-based organisations depended on third-party organisations to provide security protocols for the protection and use of client's personal information.		
Finding 21: The third-party customised technology used for securing data from IoT devices included Sigfox, AWS, Microsoft Azure and Google Cloud for their network and Cloud infrastructures, with in-house solutions like AES also being utilised.		
Finding 22: Instances of threats to personal data included hacking into smart devices, employee action, corporate espionage, ransomware attacks, as well as scam calls and emails.	System vulnerabilities	
Finding 23: Suggested solutions to mitigate unauthorised access and use of personal data included management level access, preventative and protection controls, architectural oversight for monetary transactions and daily server mirroring.		
Finding 28: Continuous revision of the principles for processing personal information was required given the pervasive nature of advancing technologies.	Processing personal information	REGULATION
Finding 32: Definitive roles were specified for the responsibilities of processing personal information which ranged from country to country.	Responsible parties, operators and supervision	
Finding 33: <i>Responsible party</i> referred to the entity that established processing purpose and means, whereas <i>operator</i> was defined as the entity that, on behalf of the responsible party, processed personal information.		
Finding 34: Organisations were required to appoint an information officer to ensure compliance with the Act and function as a liaison between the organisation and the Information Regulator.		

Finding 35: The duty of the Information Regulator was to monitor and enforce compliance in relation to the POPI Act, as well as deal with complaints about suspected violations of the protection of personal information.		
---	--	--

5.8 Outcome

The outcome involves the transformation of the object based on the activities of the subject (Kuutti, 1995). The outcome pertains to the effective governance of data privacy in IoT environments in South Africa. Findings concerning all components of the activity system indicated that all the activities work collectively towards the realisation of data privacy governance in IoT environments in South Africa. As previously shown, **Finding 7** indicated that an “in-depth and comprehensive understanding” in regard to the regulations that governed the protection of personal information was lacking. However, due to the compliance with international regulations, participants exhibited some knowledge of the EU's GDPR due to trade activities (**Finding 16**). The knowledge and actions of subjects, including users, of data privacy laws, were necessary, as it played a crucial role in the activities system towards the realisation of the outcome of effective data privacy governance.

To realise the effective data governance in IoT environments, **Finding 24** determined that due to the interconnectivity of IoT environments, the focus should be on securing and controlling access to devices (endpoints) and networks (**Finding 25**). Therefore, in IoT environments the establishment of comprehensive security measures was vital for the effective governance of data privacy (**Findings 6, 14 and 18**). Furthermore, the use of compliance experts and security specialists was recommended as assurance that the required standardised processes and approaches were followed (**Finding 26**). The findings conveyed the understanding of the relationships facilitated by the tools employed in an IoT environment. It was also revealed that the network of activities between the components, required the subjects' use of the tools to facilitate data and the establishment of guidelines and best practices for the effective governance of data privacy.

As previously acknowledged, the findings determined that “the POPI Act does not adequately address” the requirements for data management in IoT environments (**Finding 10**). The opinion of participants, in terms of the management of data in IoT environments, was that the POPI Act lacked clarity and stipulations were left open to interpretation. Therefore, to determine the best practices and guidelines for data privacy in IoT environments and the effective governance thereof, “input from people with requisite technical expertise” was required (**Finding 11**). This should better inform the requirements for effective governance of data privacy in IoT environments. The responsibilities of processing personal information, as

previously stated, were specified in the POPI Act (**Finding 32**). These roles included responsible parties and operators, information officers and the Information Regulator. Thus, as previously mentioned, the division of labour in the activity system required a symbiotic relationship of several actors (community) performing their designated roles and responsibilities (division of labour) towards achieving the object, in line with the stipulations (rules) necessary to ensure effective governance of data privacy (outcome).

To ensure the effective governance of data privacy in IoT environments, the responsibility of each member of the community was geared towards ensuring that the individual's personal data were processed in a lawful manner (responsible parties and operators) in compliance with the POPI Act (information officers and Information Regulator). **Finding 5** implied that IoT-based organisations “had no real experience of data privacy infringement incidents”. However, **Finding 3** established responsible parties' concern over the “human factor” and actions of community members presenting the biggest threat to protecting data privacy. The establishment of best practices and guidelines to inform the effective governance of data privacy in IoT environments, required the participation of all members of the community. Each member of the community interacted and connected, through the roles they played, towards actualisation of the object and realisation of the outcome. Thus, it was established that the effective governance of data privacy in IoT environments, was contingent on the community's roles and actions which dictated the level of interaction in the activity system.

The establishment of best practices and guidelines (object) was necessitated by the increased number of data breaches affecting IoT environments (tools) and consequent infringements pertaining to the data privacy of users (subject). As mentioned earlier, the findings reported that participants were mainly in agreement that the POPI Act did not adequately address the uniqueness of managing data in IoT environments (**Finding 10**). Therefore, to achieve the effective governance of data privacy in IoT environments, the use of technical experts to advise on legislative aspects pertaining to technology, was recommended (**Finding 11**). In addition to that, the establishment of comprehensive security measures was contingent on relevant and applicable rules that were vital to mitigating threats to data privacy in IoT environments. Similarly, the Information Regulator played the important role of ensuring that the object was actualised through the established rules that governed the system. The duty of the Information Regulator was to monitor and enforce compliance in relation to the POPI Act as well as deal with complaints about suspected violations of the protection of personal information.

In summary, the trigger of activity in terms of the effective governance of data privacy in IoT environments (outcome) centred around the users' (subject) of smart devices and responsible parties' (controllers and processors) management of user data in IoT environments. Relatively, the role of tools in the activity system centred around the subjects' use of the tools to collect and facilitate data that informed the establishment of guidelines and best practices towards the effective governance of data privacy (object). Focal to the activity system, there was the requirement of meeting stipulated legislation (rules) that addressed the compliance of data privacy governance in IoT environments. Each member of community played a role towards actualisation of the object and realisation of the outcome which dictated the level of interaction in the activity system.

The activity system required a symbiotic relationship of several actors (community) performing their designated roles and responsibilities (division of labour) within the boundaries of the law (rules) to achieve the object. The culmination of the interactions and relationships of activities informed the object that ultimately translated into the outcome of effective governance of data privacy in IoT environments in South Africa.

The related findings in terms of the outcome are shown in Table 5.8.

Table 5.8: Findings related to Outcome

Findings	Categories	Themes
Finding 3: There was consensus that the human factor and the associated actions presented the biggest risk to IoT-based organisations in terms of the data privacy protection.	Challenges of securing personal information	DATA PRIVACY
Finding 6: There was an understanding that establishing comprehensive security measures was vital to mitigating threats to data privacy in IoT environments.		
Finding 7: Predominantly, participants demonstrated some knowledge of the POPI Act, however, it did not depict in-depth and comprehensive understanding of data privacy law in South Africa.	Knowledge of regulations	REGULATION
Finding 10: The participants were mainly in agreement that the POPI Act did not adequately address the uniqueness of managing data in IoT environments.	Data governance and IoT	
Finding 11: It was suggested that data privacy regulation, relating to technologies such as IoT should involve input from people with requisite technical expertise.		
Finding 14: Most organisations have put in place distinctly diverse measures to accomplish the conditions stipulated by the POPI Act for data governance, in line with adhering to personal information protection, while a few depended on third-party suppliers to ensure compliance.	Regulation of personal information	
Finding 16: The majority of participants displayed knowledge of GDPR, because of the need to comply with international laws, while dealing with global parties within their respective marketplaces.	Knowledge of regulations	

Finding 18: To facilitate the protection of personal information, measures such as encryption and providing secure data storage were applied.	Security in IoT environments	DATA SECURITY
Finding 22: Instances of threats to personal data included hacking into smart devices, employee action, corporate espionage, ransomware attacks as well as scam calls and emails.	System vulnerabilities	
Finding 24: There was a perception that conventional IT systems focused more on people and personal information than IoT environments, where the focus was more on securing and controlling access due to the interconnectivity aspect of IoT environments.	Data governance and IoT	INTERNET OF THINGS (IOT)
Finding 25: It was believed that the security risks and procedures for conventional systems and IoT environments were similar, however for IoT there were added components such as the devices, the widespread nature of the networks and the vulnerability of having various endpoints.		
Finding 26: To comply with data privacy and regulatory laws in IoT environments, participants recommended utilising compliance experts and security specialists to ensure the required standardised process and approach were followed.		
Finding 32: Definitive roles were specified for the responsibilities of processing personal information which ranged from country to country.	Responsible parties, operators and supervision	REGULATION

5.9 Summary

This chapter provided explanations of the findings through the application of components of the activity theory. The subject component included users of smart devices, applications and IoT environments, responsible parties and operators (aka data controllers and processors), information officers and the Information Regulator. It was established that the biggest risk in terms of the governance of data privacy in IoT environments (outcome) centred around the users (subject) of smart devices and IoT environments (tools). Subjects, being the source of data, processor and regulator, laid the foundation and played a vital role in the network of the activity system towards the outcome.

The components for tools pertained to smart devices, applications and IoT environments, security measures and protocols and regulatory compliance measures. The findings pointed to the requirement for effective measures (tools) that enabled users (subject) to utilise smart devices and IoT environments (tools) without compromising their personal information. The interaction of the subjects with the tools helped to facilitate the object of establishing best practices and compliance.

The component for rules related to data privacy or protection regulation and compliance contracts or agreements. The rules governed the activities in the system, however, it was reported that the current nature of the POPI Act was inadequate to deal with the uniqueness of managing data in IoT environments. Thus, the establishment of best practices and guidelines for the governance of data privacy in IoT environments (object) required the

involvement of knowledgeable individuals (community) in determining the applicable legislation (rules) that applied to the system.

The community component involved users of smart devices, applications and IoT environments, responsible parties and operators (aka data controllers and processors), information officers and the Information Regulator. In the activity system there was a co-dependence between community members for the actualisation of the object and realisation of the outcome. Therefore, the governance of data privacy in IoT environments was contingent on the community's roles and actions which dictated the level of interaction in the activity system.

The division of labour component specified the roles and responsibilities of the subjects in the community. The activity system required a symbiotic relationship of several actors performing their designated responsibilities (division of labour) towards achieving the object and with the collaborations necessary to ensure effective governance of data privacy (outcome).

The object referred to the establishment of guidelines and best practices for the compliance of data privacy in IoT environments. The object was necessitated by the increased number of data breaches affecting IoT environments (tools) and consequent infringements pertaining to the data privacy of users (subject). Thus, the Information Regulator's responsibility was to ensure that the object was actualised through the established rules that governed the network of activities in the system and towards realising the outcome.

To achieve the effective governance of data privacy in IoT environments in South Africa (outcome) required the actualisation of the object and the collaboration of community members in line with their respective responsibilities.

CHAPTER SIX: DISCUSSION

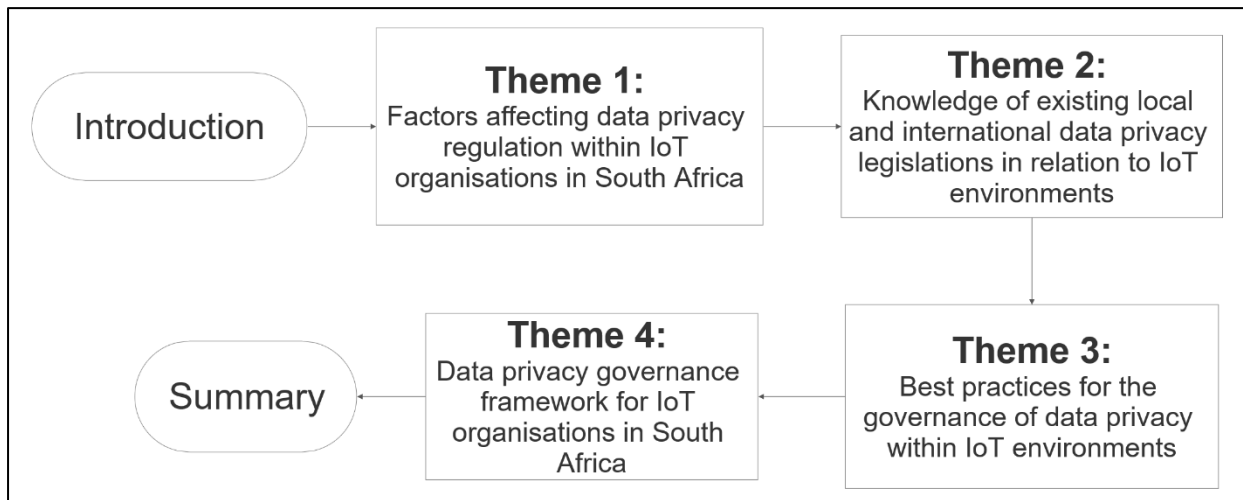


Figure 6.1: Chapter Six outline

6.1 Introduction

This chapter presents a detailed discussion of the findings of the analysis of the case study on the governance of data privacy in IoT-based organisations. The findings emanating from the analysis of data and the emergent themes identified across the interview and documents review are subsequently discussed, in relation to the relevant literature.

The aim of this research was to explore the factors for the governance of data privacy regulation and compliance for connected environments, with a view to develop a framework of guidelines and best practices for governing data privacy in IoT environments in South Africa.

The chapter is divided into six sections as displayed in Figure 6.1. Section 6.2 presents a discussion of the factors affecting data privacy regulation in IoT-based organisations in South Africa under the overarching data privacy theme. In section 6.3 the knowledge of South African organisations of local and international data privacy legislation in relation to IoT environments is discussed under the regulation theme. Section 6.4 offers a discussion on the best practices for the governance of data privacy in IoT environments as determined under the data security theme. Section 6.5 puts forward a discussion on the development of a data privacy governance framework for IoT organisations in South Africa under the IoT theme. The chapter concludes with the summary in section 6.6.

The discussion of the findings is presented under the umbrella of the research objectives, under corresponding themes such as data privacy, regulation, data security and IoT.

6.2 Theme 1: Factors affecting data privacy regulation in IoT organisations in South Africa

The objective was to determine the factors that affect data privacy regulation in IoT-based organisations in South Africa. From the analysis of data, these factors were captured under the theme, *data privacy* and the categories included data breaches, challenges of securing personal information and experience of infringements. The subsequent sub-sections present the discussion under the data privacy theme and related categories.

6.2.1 Data privacy

The novel methods of data collection for IoT lead to complex data privacy challenges, such as consent, user control, customisation and choice in what data to share as well as data use limited to the purposes stated (Naeini et al., 2017; Anand & Sharma, 2020). In addition, Fazeldehkordi et al. (2019) asserted that from a security and privacy point of view the vulnerabilities presented by the capabilities of data collection and processing in IoT environments were worrisome. The significant points of discussion of factors affecting data privacy regulation in IoT organisations in South Africa are expanded below, together with contrasting and complementary literature.

6.2.1.1 Data breaches

Greve et al. (2020:1280) described a data breach as “a security incident where data are intentionally or unintentionally exposed to an unauthorized third party”. Comparably, Sobers (2021) established that an incident in which private, confidential or sensitive information was accessed without authorisation can be defined as a data breach. Data protection policy documents from the EU, San Marino and Kenya offer the following definition for a personal data breach:

“a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

Egypt defines a personal data breach as:

“any unauthorized or illegal access to personal data, or any other illegitimate operation to reproduce, transmit, distribute, exchange, transfer, or circulate which aims to expose or disclose such personal data, or damage or edit it while it is being stored, transferred or processed”.

Taking into account the above-mentioned definitions, it can be concluded that a data breach essentially involves any incident of unauthorised access (accidental or illegal) and action to an individual's personal information.

According to SonicWall (2021), a total of 440 million records were affected by the largest breach in 2020. Check Point Software Technologies (2021) reported that the increased number of data breaches worldwide continue to be a significant threat to organisations, thus putting the personal information of individuals at risk. Regrettably, South Africa has not gone unscathed by this global occurrence and well-known organisations and state-owned enterprises (SOEs) have fallen prey to the nefarious actions of threat actors (Moyo, 2021b). In describing the current situation in relation to data breaches in South Africa, participants in the interviews employed terms such as “bad”, “scary”, “quite worrying”, “a very huge concern” and “problematic and growing” (**P4, P5, P10, P14, P15, P11 and P12**). Additionally, **P12** stated that data breaches are “the biggest risk facing the sustainability of organisations”. According to IBM Security (2021), South African organisations saw a 50% increase in the average overall cost (R46 million) involving data breaches between 2020 and 2021. A survey conducted by Liquid Cyber Security (2021) reported that 79% of the South African organisations which participated, have experienced a threat in 2020 as a result of remote operations of employees due to the COVID-19 pandemic.

Mohapi (2020) asserted that it is very likely that South African organisations are not disclosing data breaches. Likewise, several participants contended that the number of data breaches that actually occurred were much higher than what was disclosed. **P7** believed that a significant number of data breaches go unreported. This is an opinion shared by **P10**: “There's a lot more data breaches than we are aware of” and **P13**: “We only see, your Libertys, and your big cases being reported”. Amongst the reasons cited for non-disclosure are the risks of reputational damage, lack of experience of the Chief Information Officer (CIO) or the failure to detect malware in networks (Makridis, 2021; Prevailion, 2021; Smith et al., 2021).

With regard to the data protection documents analysed, the majority of the countries did not define the term, *personal data breach*. However, they provided stipulations for notification should a data breach occur. The overall requirement was for written notice to the responsible authority in each country and the data subject after becoming aware of the breach, generally within 72 hours. However, notification to data subjects might be delayed if the investigation into the breach was compromised, or it violated national security, or infringed on the rights of others. Interestingly, South Korea and South Africa did not specify a particular time frame for

notification, but required the notice to be “without delay” and “as soon as reasonably possible” after becoming aware of the breach.

In the case of South Africa, the absence of a definition for a personal information breach as well as the vague requirement for the notification of a breach in the POPI Act might have adverse implications on compliance. Consequently, in relation to a personal information breach incident, compliance to the POPI Act was left to the interpretation of the responsible party.

6.2.1.2 Challenges of securing personal information

The challenges of securing personal information by IoT-based organisations were numerous, as highlighted by the findings. Therefore, particular concerns to participants, which were the human risk factor, unsecured devices and networks and their implication on data privacy, are elaborated upon as follows:

- **The human risk factor**

IBM Security (2020) reported that human error accounted for 26% of the root causes of a data breach in South Africa. Chong et al. (2019) contended that any high-tech security system could be rendered ineffective by the human element of the system. Many incidents, leaks and data breaches have been the result of human error and the information security systems of many organisations were crippled by the mistakes of individuals (Luyt, 2019). There was consensus amongst the participants that individuals and their actions presented the biggest risk to IoT-based organisations, when it came to the protection of data privacy. **P6** commented: “We’re actually working with a lot of real people as well, who potentially do have access to a lot of personal information, and could potentially do, not that much with it, but I mean there’s always the risk”. **P2** agreed and stated: “People within the organisation who perhaps aren’t trained correctly” present a threat. In accordance with that, **P8** emphasised that data issues are as a result of inadequacy: “It’s the people that don’t know what they’re doing”. Furthermore, **P5** was of the opinion: “For most breaches, a person is at fault, usually they’re the weakest point”.

P14 highlighted the fact that data were still being shared post-implementation of the POPI Act and wondered if it is: “Someone from within the organisation?” Belanger and Crossler (2019) asserted that organisations were increasingly exposed by employees using their smart devices within the parameters of the office. The authors maintain that infected devices connecting to an organisation’s network could insert viruses and malware as well as expose confidential information. In addition to that, Hughes-Lartey et al. (2021:2) agreed that

employees were frequently the “Achilles’ heel” of an organisation and most often breaches could be linked back to some action (accidental or otherwise) on the part of an individual.

Taking into account the above revelations, it can be surmised that overcoming the human risk factor in the protection of data privacy would involve educating employees on the potential dangers and the organisations’ security procedures and compliance policies. In terms of IoT, the actions of users when using smart devices or lack of action in relation to securing devices, may inadvertently lead to the exploitation of vulnerabilities in an IoT environment.

▪ **Unsecured devices and networks**

The other risk factor identified by the participants related to unsecured devices and networks. **P2** mentioned: “In terms of IoT, I think there's a large focus on the devices”, **P10** in an example mentioned hackers gaining access through unsecured cameras, but **P5** painted the grimmest picture in his assertion: “You can literally take over millions of devices and create a bot army that you can point at any possible site you want to hack”. According to Vailshery (2021), the global number of interconnected devices are predicted to reach a staggering 50 billion by 2030. Seventy percent of IoT devices are unsecured and exposed to possible threats (Yaqoob et al., 2020). Moreover, Hameed et al. (2019) asserted that the number of devices and the absence of anti-virus or anti-malware software made devices in an IoT network susceptible to abuse. Atlam and Wills (2020) concurred that every vulnerable device in an IoT network could jeopardise an entire network's security and resilience.

Participants agreed and also highlighted not having a secure network as a threat. **P3** asserted: “If you can get access to the network layer, you've got undetectable visibility of the data flowing through that network”, and **P4** emphasised: “One of the difficulties for organizations is to get everything on a secure locked- down network”. Therefore, securing an entire IoT network should involve securing each and every device on the network as a priority (Ivankova et al., 2020).

A common practice for the participants was to proactively safeguard against potential threats to ensure that data were secured. **P1** commented that, because the intentions of perpetrators were unknown, it was probably good practice to have safeguards in place for every possible eventuality. **P15** concurred: “Each day, new malware is being developed and without doing continuous, ongoing cyber risk assessments, you can never mitigate against it”. Similarly, Liquid Cyber Security (2021:17) recommended the implementation of a framework that “evolves with the dynamic nature of cyber risks” and “ensures the effective management of those risks continuously”.

Thus, in relation to IoT environments, securing smart devices and educating people on security measures can be seen as integral to curbing security violations, ensuring network integrity and ultimately protecting the data privacy of its users.

6.2.1.3 Experience of infringements

In 2021 organisations across Europe, the Middle East and Africa (EMEA) saw a 36% increase in the average number of attacks per week (Check Point Software Technologies, 2021). Yet, participants claimed that they had not experienced data privacy infringements in their organisations, evident by the responses from **P4**: “We’ve never had a breach, nor have we had any experience with it”; **P11**: “Luckily, to date, none” and **P14**: “To date, we haven’t had any”. However, SonicWall (2021) reported a year-on-year increase in IoT malware attacks with the number of attacks for 2019 equalling 34.3 million, whereas 2020 recorded 56.9 million attacks.

Although the participants did not experience any data privacy infringements in their organisations, they did have some knowledge of infringements, as discussed under the data security section of this chapter.

6.3 Theme 2: Knowledge of existing local and international data privacy legislations in relation to IoT environments

The objective was to establish the knowledge of South African organisations of local and international data privacy legislation in relation to IoT environments. The related findings from the interviews and document analysis were captured broadly under the theme, *regulation* with categories that included knowledge of regulation, data governance and IoT and regulation of personal information. The following sub-section presents the discussion of the major points under the theme, regulation as it relates to the literature.

6.3.1 Regulation

The collection and processing of an individual's data became commonplace and many organisations built their business models on these practices (Gruschka et al., 2019). Furthermore, advances in technology aided the aggressive collection and indiscriminate use of personal information (Rudo & Reagan, 2021). User concern and the increased number of data breaches can be correlated with the global promulgation of data protection legislation (Baik, 2020). The purpose thereof being to give users more authority over the gathering and processing of their personal information and striking a balance between proper use and an individual's privacy rights (Alginahi & Kabir, 2019; Carson, 2021). In order to be seen as acting

lawfully and compliant, it is imperative for organisations to meet the requirements set out by these regulations.

6.3.1.1 Knowledge of regulations

As previously mentioned, South Africa's POPI Act came into effect on the 1st of July, 2021 (Moyo, 2021a). The POPI Act aims to provide citizens with more control over the processing and disclosure of personal information (McKane, 2020). Participants exhibited limited knowledge of data privacy and regulatory laws in South Africa, yet they were aware of the POPI Act. **P10** confirmed: "I don't know a lot about it if I'm going to be honest". **P2** asserted: "Every organization now must be POPI compliant"; **P5** declared: "We have to adhere to POPI"; **P1** stated: "We've been expecting it [POPI], we support it" and **P13** claimed to have very limited knowledge, but mentioned the POPI Act. **P14** specified: "We've got this POPI Act, and that's come in recently" and **P15** asserted: "I have a very good understanding of POPIA". **P11** admitted having limited knowledge, but was aware of the POPI Act and **P12** stated: "We have the POPI Act that has been promulgated and implemented".

According to Tsegaye and Flowerday (2019), the POPI Act stipulates that there is an obligation on the part of the responsible parties and operators to protect personal information. However, it does not specify what practices to follow for compliance. Along the same vein, **P6** maintained: "It's so hard and so complicated to comply fully with the regulation of POPI". Additionally, some participants voiced concerns about the efficacy and application of the POPI Act and **P7** believed that POPI is wonderful, but wondered why it had not taken on Facebook. **P9** termed POPI as: "A popular catchphrase at the moment". **P8** was of the opinion that POPI was: "overboard" and: "There's lots of flaws in it".

Moreover, responses indicated that legislation was behind in terms of technological developments and advancements. **P7** observed: "The State [government] cannot regulate fast enough" and suggested: "They're [government] probably behind I'd say, probably six, seven years behind in terms of being able to legislate what's actually going on". Furthermore, **P8** acknowledged that due to the changing nature of technology, the POPI Act will continuously have to be adapted to remain applicable. The findings corresponded with Mohlameane and Ruxwana (2020) who determined that, due to technological advancements and a lack of policy revisions, existing South African regulations were continuously playing catch-up. Conversely, participants believed that the POPI Act would not succeed due to the enforcement and accountability challenges faced by the South African government.

P13 observed: “Like every other piece of legislation in South Africa, we have very good laws, (but)I think it's the enforcement of the laws where we have the biggest challenge and there's no accountability”. **P14** concurred: “We've got this POPI Act, and that's come in recently, but even with that you're still seeing breaches of security”. **P15** contended: “I don't believe that government has any clue on how to implement and manage POPIA” and “They [government] don't have the skills to police the POPIA legislation”. In addition to that, **P12** pointed out: “The weakness is not so much in the Act as much as it is in the ability to impose sanction and to prosecute”. South Africa's POPI Act took eight years from the drafting of the Bill in 2013 to full implementation in July 2021 (Moyo, 2021a). Prior to implementation South African organisations suffered several high profile breaches in which millions of citizens' personal information was leaked (Mohapi, 2020). According to law firm Centurion (2021), the delay in the implementation of the POPI Act meant that citizens affected by breaches before the implementation of the Act had no legal recourse, as the stipulations could not be applied retrospectively. Although the South African government took positive steps towards the protection of personal information with the enactment of the POPI Act, the delay in its implementation, a lack of clear processes for compliance and government perception might prove challenging in its enforcement.

In addition to South African regulation, it was also important to assess local organisations' knowledge and interpretations of global data privacy laws. The majority of the participants made reference to the EU's GDPR which came into effect in 2018 (Reinwarth, 2019). **P1** declared: “We've always been following GDPR as a global standard because we've got global customers”. In accordance with that, **P5** asserted: “If I want to deal with a company in Europe, I have to be GDPR compliant”. **P6** believed that the POPI Act was modelled on GDPR and stated: “POPI is a mirror image of GDPR with a few exceptions”. **P13** indicated: “There is a massive sort of overlap between GDPR compliance and POPIA”. According to Reinwarth (2019), GDPR can be seen as the catalyst for global regulatory efforts towards protecting the personal information of individuals. Therefore, it can be understood why participants were of the opinion that the POPI Act and GDPR were analogous.

Nevertheless, the POPI Act's definition of an entity's protection of personal information extends to juristic persons. **P6** asserted: “The one difference being that where GDPR is only concerned with the personal information of natural persons, POPI expands that to juristic persons as well. So, not only are people protected, but company's personal information”. A notion **P9** concurred with: “Our POPI Act specifically classifies companies as persons. So, storing personal information about companies is regulated by the POPI Act, where in general in the international scene, it is not”. NetApp (2020) established that in comparison to the

majority of data privacy laws, this distinction was a major departure and the practicality of it remained to be proven.

In response to the growing proliferation of data in the digital space, numerous countries enacted (or are in the process of enacting) privacy protection regulations. A significant reason for the increase in data can be attributed to smart devices (predicted to reach 50 billion by 2030) and the ubiquitous nature of IoT environments, which make it prone to malicious attacks.

6.3.1.2 Regulation of personal information

The policy documents from ten countries, inclusive of the EU, San Marino, USA, South Korea, New Zealand, Brazil, British Virgin Islands, Egypt, Kenya and South Africa, highlighted in Table 4.10, were analysed. Reference made to countries in this chapter, was inclusive of the EU as a collective state, unless otherwise specified. In the USA an all-encompassing, countrywide regulation does not exist; however various states have enacted privacy policies in relation to consumer privacy (Green, 2021). Therefore, in this study the USA was represented by the California Consumer Privacy Act (CCPA) which falls within the time period and selection criteria of the document review. When discussing the policy documents, the research will refer to the policy documents by country name.

The findings were generally captured under the overarching theme, *regulation* and the sub-themes included *personal information* or *personal data definition*, processing personal information, individual rights, responsible parties, operators and supervision and international transfers of personal information, discussed below. In addition to that, the interview findings captured under the theme, regulation are also deliberated in relation to the impact of the POPI Act on IoT-based organisations and protocols or mechanisms for POPI Act compliance.

6.3.1.2.1 Personal information or personal data definition

There are divergent views on a universal nomenclature for the protection of personal information and the employment of certain terms essentially depends on the continent or country (Bygrave, 2010; Cobb, 2016; Richardson et al., 2017; Schwartz et al., 2019). Correspondingly, the policy documents utilised the terms, *personal information* or *personal data*. Six of the countries (EU, San Marino, Brazil, British Virgin Islands, Kenya and Egypt) used and defined the term, *personal data* and four of the countries (USA, South Korea, New Zealand and South Africa) defined and used the term, *personal information*. Furthermore, four of the countries also differentiated between *sensitive personal data* (Brazil, British Virgin Islands and Kenya) and *sensitive data* (Egypt).

Out of the ten countries, only the British Virgin Islands defined personal data in relation to that which were obtained indirectly from autonomous sources as information that “is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose”. The EU defined personal information as “...an identifiable natural person is one who can be identified, directly or indirectly”. Egypt also made reference to indirect identification, thus implying personal data collected from autonomous devices. Similar definitions were shared by the USA and South Africa, however no statement on indirect or autonomous data collections were made. Nevertheless, they made relatable reference to personal information as “online identifier or other particular assignment to the person”. In the same vein, South Korea referred to unique information that can be indirectly rendered by the use of technology. On the other hand, Brazil, Kenya and New Zealand had no explicit provisions for data sourced indirectly by means of technology in their documents.

According to NetApp (2020) the definition of personal information for South Africa was comparably the most extensive in its inclusion of what encompassed an individual's personal information (race, health or religion, etc.). However, in relation to data generated by automated devices, like those found in IoT environments, there were no explicit definitions regarding what constitutes direct or indirect data.

Data collected in IoT environments go beyond personal data and related secondary data. The connected devices collected data on patterns of usage, locations, habits and recorded activity timelines amongst others. This type of personal information collected by the connected devices is very private information that can jeopardise users' safety if maliciously obtained. The restrictive nature of obtaining consent from users, with no subsequent updates on what data were collected and how it was being used, could be seen as a violation of data privacy.

From the responses of the participants, it was obvious that IoT-based organisations did not classify activity data obtained from the use of the connected devices as personal information of the user. **P1** was under the impression that, because they: “Don't play in the consumer space”, the POPI Act had less of an effect on their organisation. **P4** claimed that on the IoT-side, the effect was far less because of the kind of information that the organisation needed. A similar sentiment was shared by **P9**: “Very little of our IoT endeavours fall under the POPI Act, because it doesn't contain any personal information”. **P11** stated that because they used a third-party, the POPI Act “hasn't really affected us at all”. Similarly, **P13** indicated that the POPI Act has meant “very little at this stage” to their organisation. **P6** also claimed that they did not collect what the POPI Act refers to as “unique identifiers”.

This points to the fact that there is ambiguity either in the legislation's classification of what is personal information, or in the interpretation of the responsible parties.

6.3.1.2.2 Processing personal information

According to Lockhat (2021:69), the POPI Act's main objective was to “protect the processing of personal information by public and private bodies”. The POPI Act defined processing as:

“any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including — (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information”.

Roos (2021) ascertained that the definition for processing in the POPI Act was “more than adequate” and broadly related to “anything that can be done to personal information”. However, Mbonye et al. (2021:5) argued that in situations where processing took place “as part of household activities”, the stipulations set forth in the POPI Act did not apply. The authors contended that new data items were created when using smart devices and appliances (in a smart infrastructure setting) that do not fall under the protection of personal information; yet the information was used to identify “the infrastructure and devices” of users. Similarly, Netshakhuma (2020:61) established that the POPI Act provided the minimum requirements for personal information processing by “public or private” entities.

The policy documents incorporated principles or conditions for the processing of personal information. The countries stipulated a number of principles, varying between four (Egypt) to thirteen (New Zealand). Moreover, the responsible parties and operators must make sure that the principles are upheld and compliance is established when processing personal information (Swartz et al., 2021). South Africa's POPI Act specified eight principles for the lawful processing of personal information: “accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation”. According to Zenda et al. (2020) the principles of the POPI Act were in line with those specified by other prominent countries. From a legal perspective, the proposed principles provided a neat package within which to wrap the legal requirements for processing personal information. However, given the scope and diversity, the application to an array of disciplines, as well as the constant advancement of IoT and evolving technologies, continuous revision of the principles may be required.

In addition, to process personal information lawfully, a number of conditions have been outlined by the majority of countries, except the USA and New Zealand. The countries predominantly stipulated consent as the first requirement for processing personal information; however, other circumstances under which personal information could be processed were also provided. For South Africa, the POPI Act stipulated that personal information may only be processed if:

“(a) the data subject or a competent person where the data subject is a child consents to the processing; (b) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party; (c) processing complies with an obligation imposed by law on the responsible party; (d) processing protects a legitimate interest of the data subject; (e) processing is necessary for the proper performance of a public law duty by a public body; or (f) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied”.

The provisions above relate to self-explanatory circumstances such as contractual and legal obligations, protecting the interests of the data subject, etc. The next section expands on two of the circumstances stipulated for the majority of countries, namely consent and for the pursuance of the legitimate interests of the responsible party or in some cases a third party.

▪ **Consent**

Although obtaining consent was not the only circumstance under which personal information can be lawfully processed, it is a preferred method for most organisations. Countries with definitions for consent included the EU, Brazil, Kenya, San Marino and South Africa. Specifications on obtaining consent from users were conspicuously missing from the policy documents, however, the responsibility for acquiring consent should rest with the entities that collect, process or store the information. Roos (2021) concluded that South Africa's POPI Act provided one level of consent for both personal information and sensitive information, whereas the GDPR made explicit provisions for both. Thus, in comparison, the POPI Act did not have the same level of protection as the GDPR.

In turn, the utilisation of smart devices and IoT environments was contingent on consent for the use of data. If a user did not consent to the processing of their personal information, they might not be able to use the device or application. Therefore, the notion of consenting freely and voluntarily became questionable and one could argue that consent in IoT environments was rarely given freely or voluntarily. Lockhat (2021) concurred that the sharing of personal

information by digital applications to third parties often happened without the users' knowledge or consent. Additionally, Baloyi and Kotzé (2018) established that due to the capabilities of IoT devices to collect and process an enormous amount of data, instances might occur where personal information was collected to which users did not consent.

Similarly, by giving consent, a smart device user or IoT client generally agreed to blanket terms and conditions that covered the device makers, app developers and in some cases even third parties. Thus, it could be argued that consent in IoT environments was rarely explicit or informed.

- **Legitimate interests**

Conditions have been specified for the basis of lawful processing of personal information without the expressed consent of the data subject which may jeopardise the subject's data privacy control and permission rights. The majority of the policy documents, with the exception of the USA and New Zealand, included a condition under which a responsible party, data controller or even a third-party may process personal information for legitimate interests. The countries specified that the legitimate interest of the responsible party, data controller or third-party should not outweigh the rights of the data subject. However, Roos (2021) determined that specifications on what interest would be considered legitimate, were absent in the POPI Act. Thus, technically any form of processing may be carried out for any acceptable purpose.

In terms of lawful processing, legitimate interests as a reason could be interpreted and applied flexibly and the necessity of processing left open to the interpretation of the responsible party, data controller or third-party. Thus, given the vast amount and the diverse nature of data collected in IoT environments, the lawful processing of this information could fall under the legitimate interest of the responsible party. Thereby bringing into question the level of protection of personal information for individuals who utilise smart devices (an estimated 22 billion) and IoT environments.

6.3.1.2.3 Individual rights

Personal information is considered valuable and in need of protection, thus individuals are provided with certain rights pertaining to their data (Ngwenya & Ngoepe, 2020). The actions of responsible parties in terms of their obligations towards the data subjects are underpinned by the provision of rights for individuals. The policy documents specify the rights of data subjects in relation to the protection of their personal information. The definitions for each of the specified rights are comparable and self-explanatory. By comparison, three of the ten countries (the EU, San Marino and Brazil) determined that individuals have the right to data

portability which meant that individuals were permitted to receive and move the personal information they had provided, to another controller and across environments without jeopardising the security and usability of the information. Only two of the countries (the EU and San Marino) established that subjects had the right to restrictions of processing which allowed individuals to limit the processing of their personal information, however, storage of the information was allowed.

An individual can restrict processing if the accuracy of the data was in doubt; the data were unlawfully processed and instead of requesting for it to be erased, the data subject requested the restriction; the data were no longer needed by the data controller and an objection has been logged by the data subject. Three of the ten countries (the EU, San Marina and South Africa) specified the right to no profiling or automated decision-making. This right covered aspects related to decisions made, without human intervention, on the eligibility of an individual for certain services such as online bank loans. An individual also had the right to not be profiled based on their digital activities, such as online searches and behaviour data from the use of mobile devices and social media. Additionally, all the countries except New Zealand, defined the right to know or to be informed, which technically are similar rights, but termed differently in the policy documents. Effectively, this right allowed an individual to have knowledge about the collection and utilisation of their personal information, thus fulfilling the transparency requirement of the majority of the policy documents. Baloyi and Kotzé (2020) surmised that individuals unwittingly become data subjects due to the nature of IoT environments such as smart cities where the deployment of smart devices that collected information was commonplace.

In terms of South Africa, the POPI Act specified that individuals have the right to: “be informed, access, rectification, objection, restriction of direct marketing, no profiling or no automated decision-making, erasure, lodge a complaint and institute civil action”. Thus, individuals can exercise these rights in relation to their data privacy and the lawful processing of their personal information. However, one can argue that in terms of IoT environments, individuals might not be aware of information collection and processing practices, let alone their rights as determined by law.

6.3.1.2.4 Responsible parties, operators and supervision

Baloyi and Kotzé (2019) highlighted the importance of organisations determining their roles in terms of the specifications in the POPI Act, as responsibilities vary and so does accountability for the processing of personal information. Definitive roles were specified for the responsibilities of processing personal information which ranged from country to country. The

obligation of upholding the principles and observing the rights of the data subjects fell to data custodians that the majority of the countries defined as *controllers* and *processors*. Other terms used in the description of the data custodians were *personal information controllers* in South Korea, *data controllers* and *data processors* in Kenya and the British Virgin Islands. New Zealand extensively used the term, *agency*, but did not define it in terms of data custodians. A clear distinction between controllers and processors were made by the majority of the countries. A controller could be seen as the entity that determined the purpose and means of processing personal data, whereas the processor was the entity that processed the personal data on behalf of the controller. The onus rested with the controller to assess the competency of the processor to process personal information as well as ensuring the compliance of both entities.

South Africa's POPI Act employed the terms, *responsible parties and operators*. According to Swartz et al. (2019), the protection of personal information and ensuring the lawful processing of the information was the duty of the responsible party. In the POPI Act, responsible party referred to the entity that established processing purpose and means, whereas operator was defined as the entity that, on behalf of the responsible party, processed personal information. Organisations were required to appoint an information officer to ensure compliance and act as a liaison between the organisation and the Information Regulator. It was remarkable that only three of the participants mentioned employing an information officer as part of their measures for compliance (**P4**, **P12** and **P14**). According to NetApp (2020), the POPI Act required the appointment of an information officer. However, in the absence of one, the responsibilities of compliance fell to the organisational head. Swartz et al. (2019) maintained that the information officer was critical to compliance and establishing the strategic privacy policy in an organisation.

In addition to that, supervision of the stipulations specified by the POPI Act included the establishment of the Information Regulator. It is the duty of the Information Regulator to "monitor and enforce compliance and to deal with complaints "about alleged violations of the protection of personal information of data subjects". The Information Regulator was officially appointed in 2016 (Lockhat, 2021). Sekgweleo (2019) remarked that the Information Regulator posted statements regarding breaches in 2018, however information on visible enforcement was lacking. According to Malinga (2021), the Information Regulator recently commented that the breach affecting the DOJ&CD was unfortunate and voiced her concern over the escalating number of breaches (38 reported cases in August). Vermeulen (2021) reported that the data originally leaked by the Experian data breach in 2020 was re-leaked in October 2021 and again the Information Regulator voiced her concern. Furthermore, the

author reported that the perpetrator of the original leak was arrested in September 2020, however, there was no action against the responsible party, Experian.

The lack of visible enforcement and action on the part of the Information Regulator brings into question the enforceability of the stipulations set forth in the POPI Act compounded by the digitalisation and pervasive technologies such as IoT.

6.3.1.2.5 International transfers of personal information

The international transfer or cross-border flow of personal information refers to moving personal data from one country, across its international borders, to another country. Countries prohibited the transfer of personal information to foreign countries or international organisations. However, the following exceptions under which countries may be allowed to transfer data across international borders, are:

- The data subject has consented to the transfer.
- A governing body has decided that the target country or international organisation provided adequate protection.
- The target country or international organisation can provide similar provisions for the protection of personal information as those set out by the originating country's policy document.
- The target country or international organisation can prove adequate protection of personal information.
- The target country or international organisation can provide proof of appropriate security safeguards and the protection of personal information.

Of particular interest is the provision of adequate protection in which a country or organisation has to prove that they can protect a subject's personal information or a governing body affirms the adequateness of the protection provided. In July 2020, The European Court of Justice ruled that the USA did not provide adequate protection for personal information (Fefer & Archick, 2021). Consequently, it placed limitations on the international transfer of personal information between South Africa and the USA. Furthermore, a decision by the European Commission on the adequacy of the POPI Act is currently not in place, meaning that the transfer of personal information between the EU and South Africa based on adequate protection, is not possible.

Mohlameane and Ruxwana (2020) established that due diligence with international data transfer regulations had an impact on the length of time it would take for compliance with the POPI Act. Participants believed that the regulations limit the flow of information and force

organisations to decentralise their databases. **P5** maintained that for IoT devices connecting to the Cloud in other parts of the world, the organisation needed to ensure that identifiable personal information could be distinctly identified, that is, “sending personal data across borders is a no-no”. In addition to that, the participant speculated that this was a primary reason companies such as Amazon were relocating their head office to places like Cape Town. **P6** was of the opinion that the regulations were “discretizing the whole world into smaller parts and making it very hard to flow information across those virtual borders”. Thus, the participant said that to operate in the EU, the organisation would either have to move their infrastructure there or duplicate it. Similarly, **P9** had the experience of dealing with a European client, who, as a regulatory requirement, requested their data to be hosted in Europe. Although updates to privacy laws provided guidance, as per **P8**, it also placed restrictions on the undeterred flow of information across virtual borders. It was evident that the heterogeneity in the standards applicable to data governance by different countries was an inhibitor to the cross-border operations in the business process.

The restrictions on the international transfer of personal information impedes the ability of South African organisations, especially data-driven businesses, to participate in global markets. This results in lost revenue opportunities which adversely affects the economy of the country. Thus, IoT-based organisations in South Africa are disadvantaged from competing in the international market, owing to the non-recognition of the POPI Act by international governing bodies. This censure puts a serious question mark on the capability of the legislation to ensure the effective governance of data privacy in IoT environments in South Africa.

6.3.1.2.6 Impact of POPI Act on IoT-based organisations

Mohlameane and Ruxwana (2020) observed that misunderstandings of how the POPI Act should be applied could influence compliance for South African organisations. Participants largely claimed that the impact of the POPI Act on their organisations’ processes was mostly administrative. **P4** noted that it involved “updating our forms and email policy” and having “less people we can send emails (to) out of the blue”. **P6** concurred and expressed that it involved “lots of agreements, lots of footwork, lots of kind of internal policy things”. For **P7** the process involved getting all parties to “agree to share an information template”, while **P8** enquired from customers via email whether they wanted to have their details removed. **P5** claimed that the effect on their organisation was two-fold: “There is an administrative impact and a cost impact”. Contracts with suppliers, vendors and partners should reflect the new legislative obligations as a starting point in terms of compliance (NetApp, 2020). Moreover, Belanger and Crossler (2019) maintained that regulatory compliance is not a once-off exercise, but rather one that required constant monitoring and altering by organisations to ensure continued compliance.

The POPI Act impacted organisations in varying ways, the extent of which depended on the organisations' collection, utilisation and processing of personal information. Participants maintained that due to the type of information collected in their IoT environments, the effect of the POPI Act was minimal. Nevertheless, the use of "sensors and advanced algorithms" in IoT environments resulted in the "over-collection" of personal information and "specialised processing" which could divulge new information and possibly reveal more than people intended (Baloyi & Kotzé, 2019:1). Additionally, Jiang et al. (2019) contended that IoT devices had become an appealing target for cyber-attacks due to the vast amount of sensitive information the devices generated and processed. Likewise, Amiri-Zarandi et al. (2020:2) argued that the IoT data ecosystem was of such a varying nature that concerns had been raised with regards to the types of data ("sensitive personal or business information") that may be collected and shared.

6.3.1.2.7 Protocols or mechanisms for POPI Act compliance

Organisations are obligated to apply the appropriate security protocols and mechanisms in order to accomplish compliance with the POPI Act. Participants employed varying practices in order for their organisation to comply with the POPI Act stipulations. **P1** implemented a de-linking process, where information of a person (username) was removed from an operation (GPS location) as well as stored separately. However, this comment was surprising as the participant previously stated that they did not play in the consumer space and therefore the effect of the POPI Act was less pronounced. **P8** used a technique called "scrubbing" which involved customers informing the organisation of their preference to have the organisation store or dispose of their details. If a customer opted for the latter, their information was removed from every system. The organisation performed this "scrubbing" process daily.

P13 reported that the organisation utilised "air gapping" (not connected to any network) and "a secure MQTT broker solution" (messaging protocol used for IoT). In addition to updating their documents and email policy, **P4** employed an information officer to ensure compliance, as did **P12** and **P14**. Remarkably, only three of the participants mentioned employing an information officer as part of their measures for compliance. According to NetApp (2020), the POPI Act required the appointment of an information officer, however, in the absence of one, the responsibilities of compliance fell to the organisational head. Swartz et al. (2019) maintained that the information officer was critical to compliance and to establishing the strategic privacy policy in an organisation.

In addition to that, participants used the processes dictated by other organisations. **P2** followed the direction of their parent company. On the other hand, **P3** utilised the service of a third-

party who “took care of the POPI compliance and the security thereof”. Likewise, **P11** claimed: “Our third-party supplier is covering that for us”. Most organisations have put in place distinctly diverse measures to accomplish the conditions stipulated by the POPI Act for data governance, in line with adhering to personal information protection, while a few depended on third-party suppliers to ensure compliance.

6.3.1.3 Data regulation and IoT

According to Baloyi and Kotzé (2019:1), the IoT presented a unique challenge in the protection of personal information in the sense that the “over-collection” of personal data and advanced algorithms disclosed sensitive information about individuals. The majority of the participants remarked that the POPI Act not adequately provide for data management in IoT. **P1** surmised that the POPI Act relate to personal private data and glossed over machine-to-machine (M2M) or IoT data, yet the participant believed that POPI was a good enough standard to follow for personal information. **P2** commented that although the POPI Act did not specifically mention IoT, the principles of the Act would fundamentally apply to IoT. **P5** observed that the POPI Act pertained to information of people, rather than data obtained through IoT devices and therefore it had not addressed it fully. **P6** corroborated that POPI addressed the management of data “terribly, the reason being is no one knows what POPI says”. **P8** confirmed: “In a perfect world, I think it [POPI] addresses it, but in an imperfect world, I don't think it's spot on”. **P10** also thought the Act was inadequate stating: “It's giving lip service”.

In similar vein, **P13** stressed the POPI Act: “Doesn't do a very good job” and: “There's lots of interpretation issues”. While **P15** argued: “It [POPI Act] doesn't address the management of data in IoT” because “the people who drafted POPIA never even heard of IoT, don't even know what IoT is, so nowhere in POPIA, does it really address IoT”. Mohlameane and Ruxwana (2020) established that the formulation of regulatory frameworks and policies in South Africa were flawed when it came to technologies such as IoT. The authors further argued that instead of developing frameworks for specific domains, South Africa adopted a holistic approach to solving technology issues. Baloyi and Kotzé (2019) contended that privacy legislation pertaining to technologies was oftentimes established by policymakers who lacked the technical understanding of the concepts to aid them in instituting compliance requirements. To remedy the situation, **P6** suggested that people with more technical knowledge and experience should be involved. **P15** also agreed with that point of view and emphasised that there was a need for skilled and technically specialised individuals to assist with the POPI Act. Additionally, **P8** opined that the POPI Act would need to “morph” to a point where it addressed the situation.

Based on the above stand, effective data privacy governance in IoT environments in compliance with the information protection legislations requires a universal understanding of the dynamics involved. Also, further clarification is required in terms of data classified as personal information to adequately address the uniqueness of managing data in IoT environments. Therefore, it is imperative to ensure that knowledgeable persons are consulted when legislation that deals with technology use and application, is being promulgated.

6.4 Theme 3: Best practices for the governance of data privacy in IoT environments

The objective was to determine existing best practices for the governance of data privacy in an IoT environment. The relevant findings from the interviews were captured under the theme, *data security*, the relevant categories are inclusive of system vulnerabilities and security in IoT environments. The subsequent sub-section presents the discussion of the major categories under the data security theme.

6.4.1 Data security

Digitalisation, aided by technologies such as the IoT, have numerous advantages, but also present a myriad of risks in term of “data security, privacy and trust” (Ngwenya & Ngoepe, 2020:1; Liquid Cyber Security, 2021). NetApp (2020:24) maintained that the POPI Act determined that “appropriate technical” and “organisational measures” must be applied to protect personal information in accordance with accepted practices and procedures for security. Thus, the following section is the discussion of the findings, relative to system vulnerabilities and security factors in IoT environments. It is presented comparative to the literature.

6.4.1.1 System vulnerabilities

There is a plethora of possibilities that can result in a breach of data and most of the participants had some knowledge or experience of unauthorised access and use of personal information. **P5** mentioned instances in which databases were stolen by employees, corporate espionage and electricity meters turned into a bot army and attacking a server. **P1** made reference to the hacking of a fish tank at a US casino through the temperature meter. Apparently, well-known within the cyber security community, the anecdote refers to a hacker that accessed and transferred the casino’s high roller database through an unsecured smart thermostat (Marks, 2021). **P2** talked about a Sony PlayStation hack in which the hacker obtained user credentials. According to Sinclair (2021), the PlayStation breach took place in 2011, the result of which saw the gaming network out of commission for 24 days and the theft of 77 million users’ personal information.

At the time of this research, Transnet, the South African state-owned ports and freight-rail enterprise, fell victim to a ransomware attack as mentioned by **P7**: “Transnet's sort of terror was quite publicised a few days ago”. **P9** described a situation in which someone was able to reuse a voucher on an airtime purchasing application. Commenting on the spate of unauthorised use of personal information, **P10** expressed knowledge of a server farm that was the target of a ransomware attack. **P14** mentioned the number of call centres that contact people on a daily basis. **P12** agreed: “One sees it just in terms of scam calls and emails that just are unabated”. Thus, unauthorised access and use of personal data could include practices as simple as spam emails and text messages with serious consequences, to more nefarious acts such as ransomware. Most organisations offer solutions to well-known threats such as “spam and phishing”, however, organisational preparedness against threats such as “social engineering and ransomware attacks” is a challenge (Liquid Cyber Security, 2021:11).

Suggested solutions to mitigate unauthorised access and use included management level access, preventative and protection controls, architectural oversight for monetary transactions and daily server mirroring. **P8** suggested: “It should be a certain level of management that has access”. **P9** recommended: “As soon as there are money values involved architectural oversight becomes a requirement”. **P10** and **P12**, respectively, proposed: “Do a mirror image of the server every day” and “It's just a plethora of controls that one has to put in place to try and protect one's information assets”.

In the digital era of hyper-connectivity where once “dumb” devices are now becoming smart and bringing with it the threat of attacks on users’ privacy, it becomes increasingly evident that providing secure access and an ability to operate safely in IoT environments have become imperative to ensure data privacy.

6.4.1.2 Security in IoT environments

According to Luyt (2019), the increasing number of IoT devices amplified the existing risk of data security and provided cybercriminals more avenues for exploitation. Additionally, factors such as “complex architecture, inappropriate security configuration, physical security, and insecure firmware or software” also added to the vulnerabilities in an IoT environment (Kandasamy et al., 2020:2). The number of IoT connected devices for 2021 were estimated to be in the region of 13 billion, a nine percent rise from the previous year (Sinha, 2021). Moreover, this figure was forecasted to reach 50 billion in the next ten years (Vailshery, 2021).

The growth of IoT devices correlated with increased volumes of data and participants cited applying security measures such as encryption and having secure storage were essential. **P3**

mentioned utilising encryption on the devices and the network layer, while **P5** noted: “Encryption, using encrypted tunnels to transport data” and **P9** advised: “Encryption of the data in transit” as well as “encrypting the data in storage”. **P13** corroborated the previous assertions: “Good current encryption” was essential. Additional methods were also stated such as “a lockdown network, uninterrupted transfer of data and a secure place to store it” as reported by **P4**. “Stronger firewalls, stronger places that you store it” was suggested by **P8**. In addition to that, **P13** stated: “We tokenise and keep all of the data completely separate”.

El-Gendy and Azer (2020) asserted an IoT environment required CIA which pertains to confidentiality (authorised access), integrity (untampered data transmission) and availability (uninterrupted services). In terms of the IoT, the study chose the five layer architecture (perception, transport, processing, application and business layers) which was considered to fulfil the requirements for security and privacy in IoT environments (Burhan et al., 2018; Gafurov & Chung, 2019).

The perception layer contained the devices (fitted with sensors and actuators) that supported the collection and processing of data (Frustaci et al., 2018; Aydos et al., 2019). The common technologies at this layer included RFID, NFC, WSN and BLE which provided the interconnection of the virtual with the material (Simha et al., 2018; Anand & Sharma, 2020). The common security vulnerabilities at this layer included physical attacks, impersonation, DoS attacks, routing and data transit attacks (Lin et al., 2017; Aydos et al., 2019; Anand & Sharma, 2020).

The transport layer was responsible for the secure, wired or wireless broadcast of collected data between the adjacent (perception and processing) layers and supporting IoT devices in connectivity and communication (Sethi & Sarangi, 2017; Virat et al., 2018; Noor & Hassan, 2019). The common technologies at this layer included 4G-LTE, Wi-Fi and ZigBee (Virat et al., 2018; Aydos et al., 2019; Singh & Mahapatra, 2020). The common security vulnerabilities included routing, DoS and data transit attacks (Frustaci et al., 2018; Aydos et al., 2019; Singh & Mahapatra, 2020).

The processing layer was where the information received via the transport layer was collected and processed and useful data were extracted (Burhan et al., 2018; Gafurov & Chung, 2019). Database management technologies were utilised to store and retrieve data (Virat et al., 2018; Tewari & Gupta, 2020). The common technologies at this layer included Cloud Computing, big data analytics and mobile computing (Singh & Mahapatra, 2020; Tewari & Gupta, 2020).

The common security vulnerabilities included exhaustion and malware attacks (Gafurov & Chung, 2019; Singh & Mahapatra, 2020).

The application layer defined the various applications in which the IoT had been deployed (Burhan et al., 2018; Anand & Sharma, 2020). It was also responsible for the management of smart applications as well as providing users with application specific services (Sethi & Sarangi, 2017; Singh & Mahapatra, 2020). The common security vulnerabilities included data leakage, DoS attacks and malicious code injection (Amiri-Zarandi et al., 2020; Anand & Sharma, 2020).

The full IoT system was maintained in the business layer, including user privacy, commercial and profit modules and applications (Virat et al., 2018; Singh & Mahapatra, 2020). The layer also played a role in determining how information was created, stored and altered (Burhan et al., 2018; Singh & Mahapatra, 2020). The common security vulnerabilities included social engineering, buffer overflow and backdoor (Radoglou Grammatikis et al., 2019). Suggested techniques for enhancing security with IoT environments included fog computing, blockchain technology, edge computing and machine learning (Anand & Sharma, 2020:8).

Security vulnerabilities exist at each layer of the IoT architecture, thus as the number of connected devices and the volume of data generated by these devices increase, so do the focus for the governance and protection of personal information. Suggested measures for the facilitation of the protection of personal information included encryption, a lockdown network, stronger firewalls and providing secure data storage.

▪ **Challenges surrounding the protection of personal information**

Kandasamy et al. (2020) determined that revenue and data loss due to targeted attacks on IoT devices were on the increase. To determine best practices for data governance, discovering the obstacles and difficulties within IoT environments in relation to the protection of personal information was necessary. The biggest challenge participants perceived in IoT environments was the linked devices. **P10** presented the argument that IoT devices such as security cameras were perfect entry points for hackers, as there was seldom security on these devices. Voicing similar concerns, **P5** asserted that there were no certifications or security checks for device creators. In addition to that, **P7** was of the opinion that having so many devices to contend with, became too complicated, while **P12** advanced: “Every device becomes an entry point for a hacker”. Hameed et al. (2019) agreed that IoT networks were complex due to the number of devices and volume of data generated by the devices as well as the devices providing an access point for intruders.

Conrad (2019) established that organisations had been forced to spend capital on updating infrastructures and internal policies in order to achieve compliance with regulations. **P1** and **P5** declared that cost was a challenge. They respectively stated: “Splitting environments means that you’ve got an added fee on your structure”, and “There will be a cost associated with compliance”. **P15** warned that due to the fact that IoT was relatively new and evolving daily, it was difficult to understand and therefore challenging to obtain a budget to protect it. Participants also had varying ideas about other challenges faced in IoT environments, which involved **P1**, **P2**, **P3**, **P6**, **P9** and **P13**. They respectively identified “the management of the data and the end-to-end control component”, “education”, “normal problems of TCP/IP and general web security”, “companies like us can’t own the whole value chain”, “social engineering” of individuals and “maintenance of the data”.

The challenges for the protection of personal information in IoT environments are numerous and diverse, and unsecured devices could provide a perfect entry point for individuals intent on illegally gaining access to personal information. Thus, ensuring the security of devices in an IoT environment becomes key to overcoming one of the major challenges in the protection of personal information.

- **Protocols that guide the protection and use of personal information**

The majority of IoT-based organisations depended on third-party organisations to provide security protocols for the protection and use of a client’s personal information. Participants remarked that they used external companies such as Sigfox, AWS, Microsoft Azure and Google Cloud for their network and Cloud infrastructures. These third parties utilised technologies that inherently had stringent security protocols in place for data transmission and storage. **P2** explained that the telecommunications infrastructure was operated by their organisation which in turn leveraged Sigfox technology for Cloud communication. In addition to that, **P2** added: “When you are using something like Sigfox, because the protocol is done for you, a lot of the really dangerous security flaws are taken care of for you”. **P6** declared: “To a large extent, Internet of Things companies are dependent on other suppliers for their data privacy”. While **P13** affirmed: “We’re relying heavily on Microsoft and what Microsoft are doing to secure their Cloud infrastructure environment”.

Ul Hassan et al. (2019) asserted that utilising cloud servers had become the norm and definitely offered advantages, however, it was not without its security challenges such as unencrypted server data being hacked. Thales (2021) reported that a breach was experienced by 40% of organisations using cloud environments. Moreover, issues with regard to data privacy and protection as well as the loss of control of data in the cloud environment are cause

for concern (Mohlameane & Ruxwana, 2020). Therefore, to ensure accountability in the management of client data, **P3** insisted on thoroughly evaluating and testing third-party providers to ensure that they adhered to all the required security parameters. In contrast, **P8** did not give details of their own protocols, but alluded to utilising their in-house solution rather than trusting external third parties. **P1** claimed that their own security protocol provided about eighty percent of the security for their solution and consisted of several security elements such as AES (Advanced Encryption Standard) and authentication.

Although, the responses did not render any distinct list of protocols, it was indicative of a tendency for IoT-based organisations to rely heavily on external providers for the secure management of their data, thus outsourcing the responsibility of ensuring data security. The legislation places the responsibility for the protection of user data privacy directly with the responsible parties and operators. In conjunction with that, users have expectations in terms of the obligation of the responsible parties (IoT-based organisations) with which they have signed up. It is important that IoT-based organisations be actively involved in the management of user data to ensure transparency and compliance with regulations and stipulations in respect of users' data privacy.

6.5 Theme 4: Data privacy governance framework for IoT organisations in South Africa

The objective was to establish guidelines for governing data privacy in an IoT environment. The related findings from the interviews were captured under the theme, *IoT* with the category data governance and the IoT. The subsequent sub-section presents the discussion of the findings under the theme, IoT.

6.5.1 Internet of Things (IoT)

The growth of IoT is unprecedented and its application limitless as it turns everyday things (from water meters to watches) into smart things (Hassija et al., 2019; Wu et al., 2020). According to Cilliers (2020:1), the vast amounts of "behavioural and physiological" data smart wearables generate, ought to cause privacy fears. The days of stand-alone computers have been replaced by billions of hyper-connected smart devices that are constantly collecting and transmitting data (Fu et al., 2020). However, the increased number of IoT devices and services also meant an increase in the number of attacks targeting IoT devices (Stoyanova et al., 2020). According to SonicWall (2021), global IoT malware attacks saw an increase of 66% in 2020 and South Africa saw an increase of 17%. Furthermore, in a report released by antivirus and cyber security firm Kaspersky, there was an estimated 1.5 billion attacks on IoT devices in the first half of 2021 (Seals, 2021).

6.5.1.1 Data governance and IoT

The IoT altered and continue to alter how people connect to the internet, communicate and do business. The participants believed that the security risks and procedures for conventional systems and IoT environments were similar, however for IoT there were added components such as the devices, the widespread nature of the networks and the vulnerability of having various endpoints. **P2** believed that security issues and processes for conventional systems and IoT environments were inherently similar, but with the added physical component for IoT. **P3** was also in agreement but cited the long-range networks used by IoT for communication as a variant. **P4** noted: “The vulnerability about an IoT environment is the fact that you have so many endpoints”, while **P5** was of the opinion that it was more difficult to secure and have control in IoT environments, because of the widespread nature of the networks. El-Gendy and Azer (2020) asserted that the protection of devices, networks and data from unauthorised access and use is a major concern in the IoT space. However, Fazeldehkordi et al. (2019) contend that it could be very costly for organisations to provide the same level of protection for all devices because of the variety of devices in an IoT environment.

There was a perception that conventional IT systems focused more on people and personal information than IoT environments. **P7** commented that although IoT environments provided accurate “real-time dynamic information”, privacy might be an issue when compared to an ERP (Electronic Resource Planning) system. **P1** was of the impression that in IoT environments there was less focus on personal information than in general IT environments. **P9** opined that compromising information in an IoT environment was more difficult than with conventional systems that involved people, however, this did not include IoT devices connected to a person. **P12** did not think that there was much variation as well as **P14** who noted: “It should be more or less the same”. Similarly, **P15** argued that there was no difference and stated: “You’ve got to protect it [data] wherever it is”. Dasgupta et al. (2019:211) claimed that IoT governance can be seen as supplementary to IT governance, which is concerned with managing IT resources, whereas the focus of governance in IoT should relate to “lifecycle of IoT devices, data managed by IoT solutions and IoT applications”. On the other hand, Morar et al. (2021) contended the term, *IoT governance* was relatively new and requirements still lack clarity, however, the challenges for IoT governance included data governance, privacy rights and security.

Due to the nature of data access and processing, distinctions in relation to data privacy and protection for conventional systems and IoT environments did exist. Nevertheless, similarities were prominent in the application of regulations and the categorisation of data privacy requirements. However, issues such as the security of IoT devices and networks as well as

the volume and the diverse nature of the data being collected and processed needed to be addressed. The broad nature of user consent required to utilise IoT devices and the lack of transparency in regard to the type of data being collected, would also require attention.

- **Compliance with data privacy and regulatory laws**

Data privacy laws intended to regulate the collection of information, notification to data subjects, and data subjects' control over their information as well as stipulate consequences for non-compliance (Carson, 2021). The possibility of being fined and suffering reputational damage are real repercussions of non-compliance to data privacy and regulatory laws. It is therefore imperative for organisations in South Africa to observe the stipulations set forth by these regulations and in particular the POPI Act. To comply with data privacy and regulatory laws in IoT environments, participants recommended utilising compliance experts and security specialists to ensure that the required standardised process and approach were followed. **P2** proposed getting legal advice and making certain service providers were compliant as well. **P4** agreed that gaining knowledge through hired specialists or an Information Officer was encouraged and emphasised closely following the advice they provided. **P7** was also adamant that hiring a good consultant was key to understanding digitalisation as well as using and protecting data.

From a security perspective, **P5** suggested meeting compliance through security and possibly appointing penetration experts "to probe and test" systems. **P9** strongly warned against the development of in-house security systems and advocated contracting authorities in security. Relatively speaking, **P11** advised to obtain "good advice from third parties or advisors". Similarly, **P15** recommended: "They need to employ suitably qualified specialists". **P8** asserted: "There needs to be more education around what the actual Act is, and what you're allowed to and what you're not allowed to do". Alginahi and Kabir (2019) observed that the proper use of data balanced by the privacy rights of individuals can be defined as the purpose of data protection regulations.

For South Africa, compliance to the POPI Act was mandatory, therefore, it was imperative that organisations were knowledgeable about the requirements of the Act, with particular focus on the understanding and application of data privacy regulations in IoT environments in South Africa which provided rich insights and exposition of the research phenomenon.

6.6 Summary

The findings of the study were discussed in relation to the sub-questions. The discussion on the factors that affect privacy regulation in IoT environments in South Africa pertained to the

human risk factor and unsecured devices and networks. Consequently, education on potential threats and security procedures and compliance policies of the relevant organisations were crucial to overcome the human risk factor in the protection of data privacy. Moreover, securing smart devices and networks could be seen as positive steps towards protecting users' data privacy.

A discussion on local and international legislation followed next in which the findings from the interview data and document analysis were deliberated. It was ascertained that although participants had knowledge of regulations, it was not in-depth knowledge. The POPI Act impacted organisations in varying ways, the extent of which depended on the organisations collection, utilisation and processing of personal information. Most organisations had put in place distinctly diverse measures to accomplish the conditions stipulated by the POPI Act for data governance, in line with adhering to personal information protection, while a few depended on third-party suppliers to ensure compliance.

Furthermore, it was important to determine the best practices for the governance of data privacy in IoT environments. Most organisations had security solutions to well-known threats such as phishing and spam, however, threats involving ransomware attacks and social engineering were challenging. Suggested solutions to mitigate unauthorised access and use included management level access, preventative and protection controls, architectural oversight for monetary transactions and daily server mirroring.

To comply with the stipulation of data privacy and regulatory laws, it was suggested that organisations seek the services of experts in the field of compliance, employing security measures and education on the POPI Act.

CHAPTER SEVEN: RECOMMENDATIONS, REFLECTION AND CONTRIBUTIONS

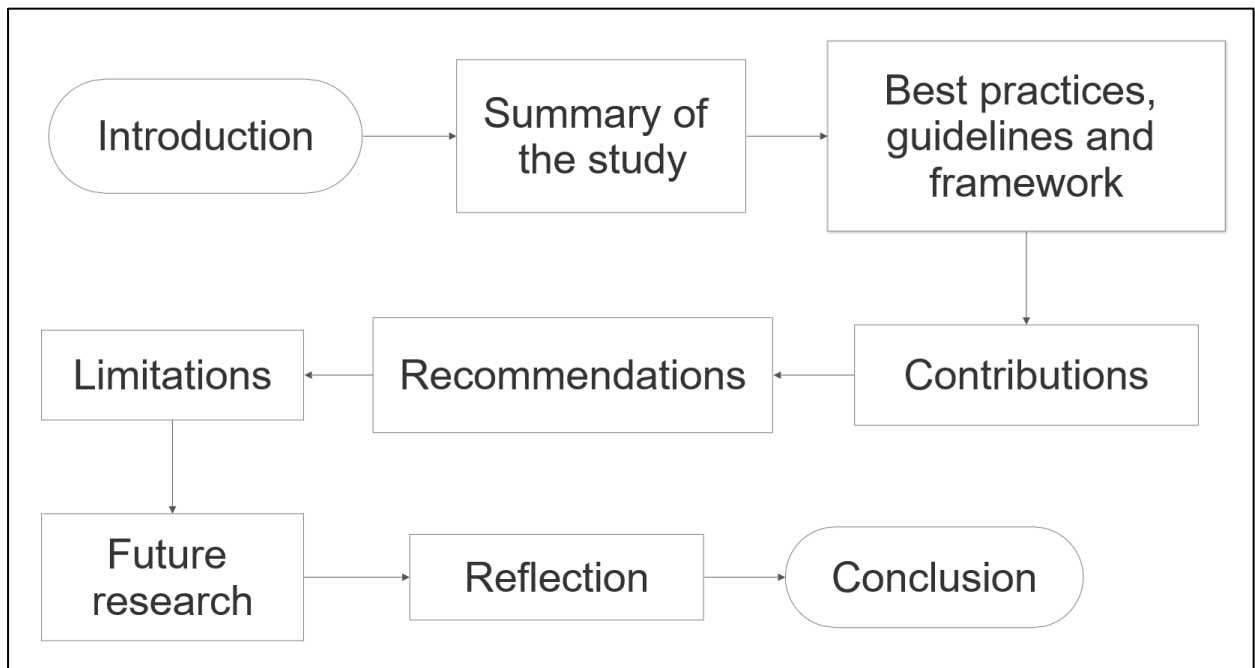


Figure 7.1: Chapter Seven outline

7.1 Introduction

Digitalisation and technological advances such as IoT have had a tremendous effect on our existence. Even more so since the COVID-19 pandemic with emerging technologies bringing forth new ways of working and communicating. However, the pervasive nature of these technologies and hyper-connectivity have not been without impact on the individual's privacy. Opportunities for cyber-attacks and data breaches are exponentially multiplied by the proliferation of connected devices. The increased number of attacks and breaches of data have led to updates and promulgation of privacy protection regulation by several countries, including South Africa. Therefore, this study explored the factors affecting the governance of data privacy regulation and compliance for connected environments, with a view to develop a framework of guidelines and best practices for governing data privacy in IoT environments in South Africa.

This chapter brings the research study to a conclusion by summarising the results of the research process to address the research phenomenon. It offers a reflection on the research problem, the objectives and the research question and sub-questions. The chapter is divided into nine sections as displayed in Figure 7.1. A summary of the study and the extent to which the research questions were addressed can be found in Section 7.2. In section 7.3 the best

practices, guidelines and the framework encompassing these guidelines and best practices for the governance of data privacy in IoT environments in South Africa are presented. Sections 7.4 and 7.5, respectively, highlight the contributions made by this study and recommendations to address identified gaps. The limitations of the study are described in Section 7.6. The study highlights considerations for further research in section 7.7 and the researcher reflects on the research process in section 7.8. The conclusion of the research based on the attempt of this study to address the research phenomenon is presented in section 7.9.

7.2 Summary of the study

A qualitative multiple-case study was employed to explore the factors for the governance of data privacy regulation and compliance for connected environments. An additional aim was to develop a framework of guidelines and best practices for governing data privacy in IoT environments in South Africa.

The aim and objectives of this study were achieved through semi-structured interviews of participants purposively chosen by the researcher and who consented to participation. Data were collected from fifteen IoT-based organisations with similar operational scope, but varying in size till the point of saturation. Additionally, data were sourced from a document review of ten countries with recently updated data protection policies.

The section below presents a summary of the study in an attempt to provide answers to the research questions and subsequently address the research problem. The highlight of the findings relevant to providing insight to the research questions are further expounded in the subsequent sections.

7.2.1 SQ1.1: What are the factors affecting data privacy regulation in IoT organisations in South Africa?

The research question investigated factors affecting data privacy regulation in IoT organisations in South Africa. The findings revealed that there was concern over the upsurge in data breaches in South Africa. There was a revelation that the number of data breaches that occurred were considerably higher than what were reported. In terms of data protection, there was a consensus of opinion that people and their actions presented the biggest risk to IoT-based organisations. In addition to that, unsecured devices and networks also posed a high risk in terms of protecting against data breaches. It was established that there was a need for comprehensive security measures crucial to mitigating threats to data privacy in IoT environments.

A major concern highlighted was the prediction that in the future, the biggest attacks on data privacy would involve IoT environments. In addition, the loose stipulation for the notification of a data breach in the POPI Act, meant that complying with the regulation was left to the interpretation of the responsible party which contradicted the objective of transparency and accountability. Thus, the identified factors that affected data privacy regulation in IoT-based organisations included data breaches, the human factor, unsecured devices and networks.

These highlighted findings provided answers that addressed the research objective: **To determine the factors affecting data privacy regulation in IoT-based organisations in South Africa.**

7.2.2 SQ1.2: How knowledgeable are South African organisations about existing local and international data privacy legislations in relation to IoT environments?

South African organisations' knowledge of local and international data privacy legislation in relation to IoT environments was established with this research question. Overall, a limited knowledge of the POPI Act was demonstrated. Thus, a comprehensive understanding of data privacy laws in South Africa was lacking. However, a general knowledge of the EU's GDPR was displayed by a small number of participants. It was recognised that the POPI Act and GDPR were relatively close in comparison with minor differences in application. In addition to that, the POPI Act also determined that an entity's protection of personal information extended to juristic persons. Consequently, in terms of the POPI Act, legally recognised organisations were also protected.

The study also revealed that current legislation on data privacy in South Africa was trailing technological developments and advances. Concerns were raised about the efficacy of the POPI Act and projections were made that it was destined to fail due to implementation and enforcement challenges. Furthermore, there was agreement that the uniqueness of managing data in IoT environments were not adequately addressed by the POPI Act. In relation to data generated by automated devices, like those found in IoT environments, there was no explicit definition regarding what constitutes direct or indirect data in the POPI Act. It was established that the POPI Act would require continuous revision in line with advancing technologies, global trends and developments. In relation to technologies such as IoT, it was suggested that data privacy regulation should include input from technical experts with specialised knowledge of the dynamic nature of data management in data-driven environments.

Predominantly the policy documents reviewed specified consent as the first requirement for processing personal information. However, the utilisation of smart devices and IoT environments was contingent on consent for use of data, which did not allow for expressive and informed user consent. Furthermore, conditions have been specified for the basis of lawful processing of personal information without the expressed consent of the data subject which may jeopardise the subject's data privacy control and permission rights.

Each country specified definitive roles for the responsibilities of processing personal information. In terms of the POPI Act, the responsible party refers to the entity that established processing purpose and means, whereas the operator was defined as the entity that, on behalf of the responsible party, processes personal information. Additionally, organisations were required to appoint an information officer to ensure compliance with the Act to function as a liaison between the organisation and the Information Regulator. The duty of the Information Regulator was to monitor and enforce compliance in relation to the POPI Act as well as deal with complaints about suspected violations of the protection of personal information.

The transfer of personal information to foreign countries or international organisations was prohibited by the of majority countries. Nonetheless, exceptions existed such as consent from the data subject or a determination of providing adequate protection. Thus, the restrictions impacted on the ability of South African organisations to participate in the global market, especially data-driven, cross-border organisations like those operating in the IoT environment.

The findings highlighted above provided answers that addressed the research objective: **To establish the knowledge of South African organisations of local and international data privacy legislation in relation to IoT environments.**

7.2.3 SQ1.3: What are the best practices for the governance of data privacy in IoT environments?

The research question determined the existing best practices for the governance of data privacy in IoT environments in South Africa. Threats to personal information were established as hacking into smart devices, employee action, corporate espionage, ransomware attacks as well as scam calls and emails. Suggested solutions to mitigate unauthorised access and use of personal data included encryption, secure data storage, management level access, preventative and protection controls, architectural oversight for monetary transactions and daily server mirroring. There was a reliance on third-party vendors such as Sigfox, AWS, Microsoft Azure and Google Cloud for the provision of security protocols. However, these third-

party vendor security measures need to be subjected to scrutiny and oversight actions constantly, to ensure compliance with regulations and standards.

Security in IoT environments should also be guided by the basic principles of information security, namely confidentiality (authorised access), integrity (untampered data transmission) and availability (uninterrupted services). The study incorporated the five-layer architecture (perception, transport, processing, application and business layers) which is considered to fulfil the requirements for security and privacy in IoT environments. Yet, each layer presents its own security vulnerabilities:

- **Perception layer:** It encompasses physical attacks, impersonation, DoS attacks, routing and data transit attacks.
- **Transport layer:** It refers to routing, DoS and data transit attacks.
- **Processing layer:** It covers exhaustion and malware attacks.
- **Application layer:** It relates to data leakage, DoS attacks and malicious code injection.
- **Business layer:** It indicates social engineering, buffer overflow and backdoor.

Suggested measures for the facilitation of the protection of personal information included authentication, encryption, lockdown networks, stronger firewalls and providing secure data storage. This is in line with global practices and acceptable standards for the protection of data privacy in IoT and data-driven processes.

As a requirement of the POPI Act, it was established that entities should appoint an information officer (in the absence of one, the responsibility falls to the head of the organisation) to ensure compliance with the Act and function as a liaison between the organisation and the Information Regulator.

The above-mentioned findings provided answers that addressed the research objective: **To determine existing best practices for the governance of data privacy in an IoT environment.**

7.2.4 SQ1.4: How can a data privacy governance framework for IoT organisations in South Africa be developed?

This question of the research was used to inform the development of a framework of guidelines for the governance of data privacy in IoT environments in South Africa. The adoption of an IoT Framework can assist organisations in providing better overall information security and data privacy. The framework should serve as a checklist to aid organisations in terms of data privacy, data security, data governance and compliance.

Data privacy: IoT presented novel ways for organisations to collect and process large volumes of user information which led to complex data privacy issues. The challenges of securing personal information pertained to data usage and breaches (compliance), the human risk factor (people), unsecured devices and networks (technology) and the implications for data privacy.

Data security: The focus in IoT environments was on securing and controlling access due to the interconnectivity aspect of IoT environments. Compared to conventional systems, the security risk and procedures were similar. Still, an IoT environment had additional components such as devices, widespread networks and a variety of endpoints. Therefore, risk mitigation and management were key components for data security.

Data governance: The governance of data refers to organisations putting in place the required strategies and policies to effectively manage all organisational data aspects. Suggested activities included ensuring that the required processes and approaches were followed for compliance and utilising compliance experts and security specialists.

Compliance: The provision of rights for individuals in legislation (local or international) should underpin the actions of responsible parties in terms of their obligations towards the data subjects. In addition, organisations should ensure adherence to regulatory stipulation, implementation of industry standards, assurance of compliance from third-party vendors and familiarising themselves with practices and requirements for regulatory compliance.

These highlighted findings were proposed to address the research objective: **To develop a framework of guidelines for governing data privacy within IoT environments in South Africa.**

7.3 Best practices, guidelines and framework

Part of the research aim pertained to the development of a framework of guidelines and best practices for governing data privacy in IoT environments in South Africa. Based on the findings and literature, this study identified four key areas of consideration for data privacy governance, namely data privacy, data security, data governance and compliance as depicted in Figure 7.2. The following section provides an overview of the framework and the key areas.

7.3.1 Data privacy

The challenges for data privacy are amplified by the data collection methods presented by IoT environments. This section describes the guidelines and best practices in terms of compliance, people and technology.

- **Compliance:** The POPI Act requires that the notification of a breach incident be made “as soon as reasonably possible” after becoming aware of the breach. Most countries

stipulated 72 hours, therefore this study suggested that prompt data breach notification should be within 72 hours to the data subjects and the Information Regulator. In compliance with the principle of openness, this study suggests that organisations inform users and clients every six months of the usage and processing of their personal data.

- **People:** For consent to be informed and specific, device users and IoT clients should be provided with the exact purpose for the collection and use of their data. People were identified as the biggest risk factor in terms of data privacy, thus it is imperative that organisations educate employees on security practices and protocols.
- **Technology:** Securing smart devices and ensuring the integrity of IoT networks are integral to protecting data privacy. This can be achieved by applying adaptable high-level security measures at each layer of the IoT architecture and continuous risk assessment. These measures include, but are not limited to, authentication, encryption, lockdown networks, stronger firewalls and providing secure data storage.

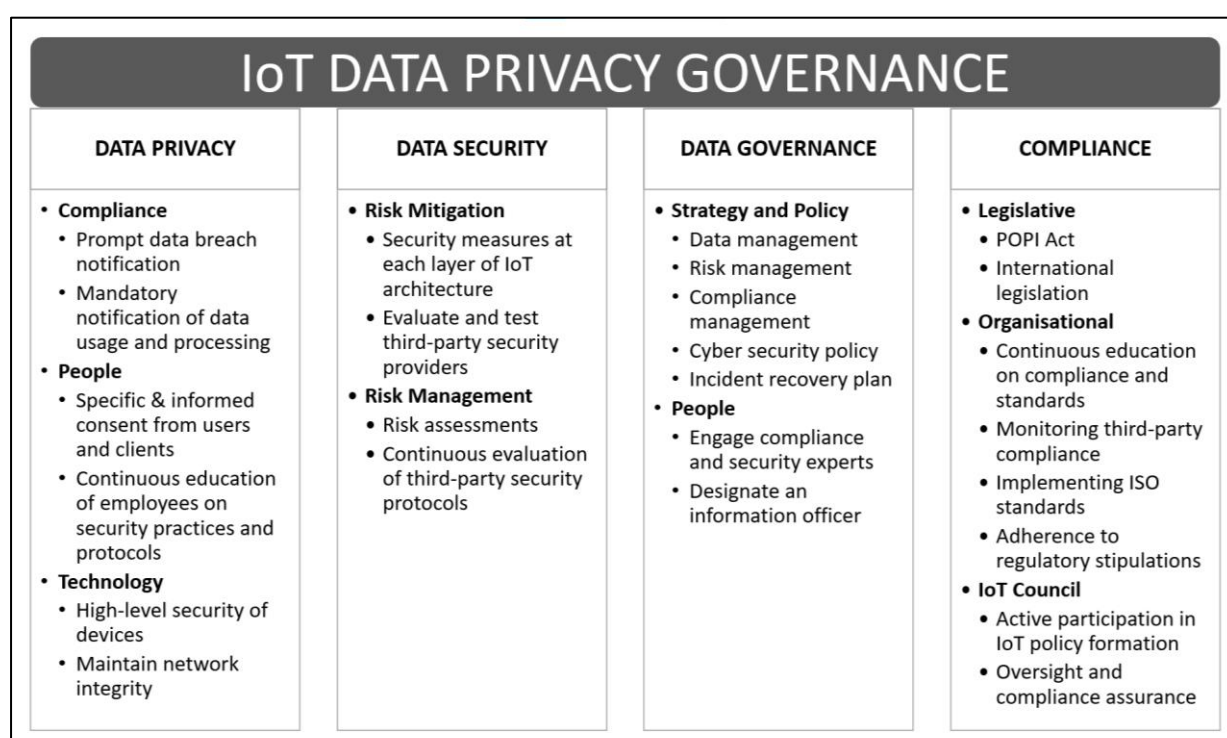


Figure 7.2: Proposed data privacy governance framework

7.3.2 Data security

Cybercriminals are continuously finding new ways to exploit vulnerabilities in an IoT environment, thus overall security require confidentiality (authorised access), integrity (untampered data transmission) and availability (uninterrupted services). This section describes the guidelines and best practices in terms of risk mitigation and management.

- **Risk mitigation:** The mitigation of security risks involved implementing security measures at each layer of the IoT architecture to ensure data security. Security protocols should be stringently evaluated and tested to ensure that the appropriate security safeguards are in place to mitigate any potential risks to data security.
- **Risk management:** In order to minimise data security risks, it is advised to perform daily risk assessments on the devices and entire networks. Third-party security protocols should also be continuously evaluated to ensure that suitable and applicable safety measures are set up.

7.3.3 Data governance

The objective of data governance is to support the organisation by providing direction through the establishment of strategy and policy (Liquid Cyber Security, 2021). Data governance should set out an organisation's guidelines for the processing and protection of personal data, thus it should form part of policies and strategies of an organisation (Swartz et al., 2019). The guidelines and best practices in terms of strategy and policy and people are described in this section.

- **Strategy and policy:** This refers to the establishment of strategy and policy in line with data, risk and compliance management as well as security mitigation and management policies. The formation of a cyber security policy that includes research and development (R&D) investment in threat identification and mitigation is prudent. An incident recovery plan is also advisable to ensure that organisations are operational in the shortest time possible following an attack or breach.
- **People:** It is advisable to involve compliance and security experts when drafting and defining the strategies and policies for data governance. Furthermore, to ensure compliance in line with legislation and organisation policies it would be prudent to appoint an information officer.

7.3.4 Compliance

It is essential for organisations to comply with legislative and regulatory requirements that govern the industry and regions in which they operate (Liquid Cyber Security, 2021). The legislative and organisational requirements as well as the role of the IoT council are illustrated in this section.

- **Legislative:** Local and international legislation dictate the principles for lawful processing of personal information, thus it is imperative to follow these stipulations for compliance.
- **Organisational:** The onus is on organisations to adhere to regulatory stipulations, implement the correct industry standards and ensure that third-party providers are compliant. Education on compliance relates to compelling organisations to understand the

impact of the POPI Act and their obligations concerning the protection of personal information. It involves comprehension of what it means to lawfully collect and process an individual's data as well as being transparent about their processing practices.

- **IoT Council:** The IoT council should be seen to be actively participating in policy formation, setting the standard and providing compliance oversight.

By adopting and implementing the afore-mentioned guidelines and best practices, IoT-based organisations should be able to effectively maintain data privacy governance.

7.4 Contributions

The contributions of this research are classified as theoretical, methodological and practical.

Theoretical contribution:

- This study contributed new knowledge by identifying the factors affecting data privacy regulation in South African IoT-based organisations. These factors provide an insight into the challenges faced by IoT-based organisations in relation to the protection of personal information.
- This study provided insight into best practices and guidelines tailored specifically for the governance of data privacy in IoT environments in South Africa based on acceptable global standards.
- This study contributed towards the body of knowledge by identifying the commonalities and disparities in the legislation and regulation of the protection of personal information based on the perspective of a region or country.
- The application of the Activity Theory as a lens, provides deeper understanding of the relationships and interplay within the network of activities in the activity system for the data privacy governance in IoT environments in South Africa. The findings through the lens of this theory contributes towards a comprehensive depiction and exposition of the subject matter using the components of the Activity Theory.

Methodological contribution:

- The combination of interviews and documents review of recently updated protection of personal information legislations provided a basis for the acquisition of rich and unique data on the dynamics of data privacy governance in IoT environments in South Africa.

Practical contribution:

- This study also developed a framework of guidelines and best practices for governing data privacy in IoT environments in South Africa. It is meant to inform and guide IoT-based

organisations on how to administer users' data privacy effectively in line with stipulated regulations in South Africa and in adherence with global standards.

7.5 Recommendations

The literature and research findings obtained through the participant interviews and policy documents review provided valuable insights and identified gaps in regard to data privacy governance in IoT-based organisations in South Africa. This section provides the recommendations of this study to address the gaps identified, following the research process, towards ensuring a more effective compliance and regulation of data privacy in South Africa, particularly in IoT environments.

Recommendations for policies and regulation:

- It is recommended that the POPI Act be subjected to continuous revision and updates in line with advancing technologies. The Act was implemented eight years after the introduction of the Bill, thus it is already behind in terms of addressing evolving technological trends with adverse impact on data privacy.
- The study recommends that data privacy regulation, relating to evolving technologies such as IoT should involve input from people with requisite technical expertise. Thus, it would be beneficial to involve technology experts and governing bodies such as the IoT council.
- It is recommended that data breach notification in the POPI Act be amended from “as soon as reasonably possible” to within 72 hours after becoming aware of the breach, to promote transparency and inform users expeditiously of any compromise of their personal data and privacy.
- It is recommended that the POPI Act be revised, developed and implemented at a level, such that it is recognised as adequately protecting personal information. This would ease the restrictions placed on data-driven organisations in South Africa in terms of participating in global markets.
- Visible application of penalties and action on the part of the Information Regulator are also recommended.

Recommendations for compliance:

- Due to the implications of data breaches, not only for the organisations, but also for the data subjects, it is imperative that prompt notification (within 72 hours) of the discovery of a breach be implemented.
- The Information Regulator must initiate an information campaign regarding the POPI Act in relation to its principles, the rights of data subjects, breach reporting and general

information relevant to data subjects in relation to the protection of their personal information.

- It is recommended that organisations undergo periodic audits of their compliance and data management processes in line with the regulations and advancement of data privacy standards.
- It is recommended that organisations appoint an information officer to ensure compliance and act as a liaison between the organisation and the Information Regulator to promote accountability and transparency in the compliance process.
- It is recommended that visible and active lines of communication be established between the Information Regulator and organisations to inform updates in data privacy practices and keep abreast of global development and standards.

Recommendations for IoT-based organisations:

- The study revealed a reliance on third-party vendors for data and network security and thereby outsourcing this responsibility. It is therefore recommended that independent auditors be appointed to assess third-party data collection and processing practices, security measures and data management processes in line with regulation and standards.

7.6 Limitation

The study was limited to IoT-based organisations in South Africa. Only four (the Western Cape, Eastern Cape, KwaZulu-Natal and Gauteng) of the nine provinces were represented. Therefore, the findings cannot be generalised to other regions or industries, but might be applicable to entities with a similar contextual orientation.

The participants included high-level executives from fifteen organisations. The study only included two cyber security specialists who provided valuable insights into risk and threat management. It would have been beneficial to the study to include a few more participants with similar expertise. Similarly, insights from the Information Regulator and legal representatives would also have added value. Unfortunately, the Information Regulator was not available to participate and emailed requests to law firms that deal with the compliance process went unanswered.

The data collection process extended over five months. The process was started early in 2021 and the intention was to complete in July. However, most organisations were working towards compliance in line with the POPI Act which came into effect on the 1st of July, 2021. Due to the pandemic, the interviews could not be completed in person and were conducted virtually via Zoom. Consequently, inferences such as body language and dispositions were not easily

captured. In some cases, connection issues such as lag and being disconnected were experienced. Over the five month period, several participants agreed to participate and did not show up for the interviews and it was not until September that responses started picking up, thus the timeline for the study was affected.

The document analysis of recently updated data protection policies was limited to countries that have updated their regulations between years 2018–2021. Unfortunately, a number of documents were excluded owing to credible transcripts of the English versions of the regulatory documents not being found. Another challenge was deciphering the legal vernacular of the policy documents during the document review process. Although beneficial to this study, understanding and interpretation was difficult and therefore time-consuming.

Another time-consuming process was the transcribing of the interviews. Although an automated transcription tool was used, the quality of the transcription was hampered by the uniqueness of the South African accent. Thus, a labour-intensive task of going over each interview and revising ensued. However, it allowed the researcher to get familiar with the participants' responses. In addition to that, the researcher also had to learn and become acquainted with using ATLAS.ti.

7.7 Future research

This study takes into consideration identified limitations of this research and future research is proposed to further explore the factors for the governance of data privacy regulation and compliance for connected environments.

- Future research could focus on obtaining a sample of equal representation of IoT-based organisations, cyber security specialists, legal representation and the Information Regulator.
- To better understand the implications of these results, future research could address the impact of the identified factors (data breaches, the human factor, unsecured devices and networks) that affect data privacy regulation in IoT-based organisation.
- Future research could be conducted to ascertain the effectiveness of the proposed framework through implementation.
- Future research could focus on the effect of obtaining explicit user consent and awareness of the type of collected data from connected devices on the data privacy of users.
- Future research can be carried out to determine the usefulness of block chain technology as a means of documenting and reporting on data standards.

- Furthermore, future research can also investigate compliance and process auditing of third-party vendors in relation to the collection and processing of data and the effect on users' data privacy.

7.8 Reflection

Notwithstanding the limitations and challenges faced, the research provided ample opportunity for the learning and development of this researcher. This study provided greater understanding of research methodology and how a researcher's beliefs and view of the world have an influence on the overall research process. The iterative process of thematic analysis provided this researcher with an opportunity to delve deeper into the data of the study and in so doing gain a richer understanding of the observed phenomenon.

Similarly, the document review process which at first seemed daunting, provided a valuable learning opportunity of the document analysis process and its application. Furthermore, the analysed policy documents informed this researcher of the similarities and differences in the country-specific policies. This researcher discovered that the policy documents specify the requirements for the protection of personal information. However, specification on how to implement the stipulations are lacking. In addition to that, there are stipulations for the lawful processing of personal information without the consent of the data subject. This study also made this researcher more aware of the use of technology and its implication for the users' data privacy.

The theoretical framework utilised by the study was the Activity Theory Framework. The use of the activity system and its components helped this researcher to gain a better understanding of the network of activity for establishing data privacy governance. At the end of the research process, my experience of the topic has been greatly enhanced. My journey as a researcher has shaped my view of the world positively and I am able to approach things more open-mindedly, while being more systematic in my inquisitiveness to learn new things.

7.9 Conclusion

Advancing technologies and the pervasive, hyper-connected and ubiquitous nature of IoT has led to aggressive data collection and processing practices. This has culminated in the promulgation of global privacy protection legislation. Each of these, attempt to provide data subjects with rights in regard to their personal information and legal recourse in the event of unlawful processing actions on the part of responsible parties.

The research revealed that there are several factors that affect data privacy regulation in IoT organisations in South Africa. The factors include the increased number of data breaches, the human risk factor and unsecured devices and networks. Securing smart devices and educating people about security measures can be seen as integral to curbing security violations, ensuring network integrity and ultimately protecting the data privacy of its users.

With regard to privacy protection regulation, stipulations tend to be ambiguous and left open to interpretation. For example, the vague stipulation for data breach notification (as soon as reasonably possible) in the POPI Act begs the question: What is considered as soon as reasonably possible? Therefore, it is suggested that the POPI Act follow the example of other countries and clearly specify a time period which would be considered as reasonable. In addition, revising ambiguous points in the Act could aid the South African policy in being determined as providing adequate protection. This would have a positive effect on data-driven organisations, international relations and the South African economy at large.

According to Dasgupta et al. (2019) from a regulatory standpoint there is no definitive IoT framework that can provide a template to institute a data governance environment. Presently, in South Africa there is an absence of a defined data privacy governance framework for IoT environments. The proposed framework established key areas of consideration, namely data privacy, data security, data governance and compliance. IoT-based organisations can use the proposed framework to assist in the management of data privacy governance in accordance with regulatory compliance.

REFERENCES

- Abbott, M.L. & McKinney, J. 2013. *Understanding and Applying Research Design*. New Jersey: John Wiley & Sons, Inc.
- Adams, J., Khan, H.T.A. & Raeside, R. 2014. *Research Methods for Business and Social Science Students*. Second. Thousand Oaks, California: Sage Publications.
- Adelman, C. 1993. Kurt Lewin and the Origins of Action Research. *Educational Action Research*, 1(1): 7–24.
- Ahamd, T., Aslam, H. & Shahzad, S. 2018. Security of Provider sides in Data Privacy and Data Accessibility Issues in Cloud computing. *University of Sindh Journal of Information and Communication Technology (USJICT)*, 2(1): 7–10.
- Al-Saadi, H. 2014. Demystifying Ontology and Epistemology in Research Methods. *ResearchGate*, (February).
- Alaba, F.A., Othman, M., Abaker, I., Hashem, T. & Alotaibi, F. 2017. Internet of Things security: A survey. *Journal of Network and Computer Applications*, 88: 10–28.
- Alginahi, Y.M. & Kabir, M.N. 2019. Authentication technologies for cloud computing, iot and big data. *Authentication Technologies for Cloud Computing, IoT and Big Data*: 1–370.
- Ali, H. & Birley, S. 1999. Integrating deductive and inductive approaches in a study of new ventures and customer perceived risk. *Qualitative Market Research: An International Journal*, 2(2): 103–110.
- Ali, S., Islam, N., Rauf, A., Din, I.U., Guizani, M. & Rodrigues, J.J.P.C. 2018. Privacy and Security Issues in Online Social Networks. *Future Internet*, 10(114): 1–12.
- Aliyu, A.A., Singhry, I.M., Adamu, H. & Abubakar, M.M. 2015. Ontology, Epistemology and Axiology In Quantitative And Qualitative Research: Elucidation of the Research Philosophical Misconception. *Proceedings of The Academic Conference: Mediterranean Publications & Research International on New Direction and Uncommon*, 2(December).
- Allen, D., Karanasios, S. & Slavova, M. 2011. Working with Activity Theory: context, technology, and information behavior. *Journal of the American Society for Information Science and Technology*, 62(2007): 776–788.
- Allen, M. 2017. Archive Searching for Research. In *The SAGE Encyclopedia of Communication Research Methods*. Thousand Oaks, California: Sage Publications: 47–49.
- Almtrf, A., Alagrash, Y. & Zohdy, M. 2019. Framework modeling for User privacy in cloud computing. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019*: 819–826.
- Almusaylim, Z.A. & Jhanjhi, N. 2020. Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing. *Wireless Personal Communications*, 111(1): 541–564.
- Altaf, A., Abbas, H., Iqbal, F. & Derhab, A. 2019. Trust models of internet of smart things: A survey, open issues, and future directions. *Journal of Network and Computer Applications*, 137(March): 93–111.

- Altman, I. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Monterey: Brooks/Cole Publishing Company, Inc.
- Alvi, M.H. 2016. A Manual for Selecting Sampling Techniques in Research. *Munich Personal RePEc Archive*: 1–56.
- Aly, M., Khomh, F., Haoues, M., Quintero, A. & Yacout, S. 2019. Enforcing security in Internet of Things frameworks: A Systematic Literature Review. *Internet of Things*, 6(100050): 2542–6605.
- Amiri-Zarandi, M., Dara, R.A. & Fraser, E. 2020. A survey of machine learning-based solutions to protect privacy in the Internet of Things. *Computers & Security*, 96.
- Anand, S. & Sharma, A. 2020. Assessment of security threats on IoT based applications. *Materials Today: Proceedings*. <https://doi.org/10.1016/j.matpr.2020.09.350>.
- Anastas, J.W. 1999. *Research Design for Social Work and the Human Services*. Second. New York: Columbia University Press.
- Andrew, J. & Baker, M. 2021. The General Data Protection Regulation in the Age of Surveillance Capitalism. *Journal of Business Ethics*, 168(3): 565–578.
- Appel, G., Grewal, L., Hadi, R. & Stephen, A.T. 2020. The future of social media in marketing. *Journal of the Academy of Marketing Science*, 48(1): 79–95.
- Atlam, H.F. & Wills, G.B. 2020. IoT Security, Privacy, Safety and Ethics. In M. Farsi, A. Daneshkhah, A. Hosseinian-Far, & H. Jahankhani, eds. *Digital Twin Technologies and Smart Cities*. Springer International Publishing: 123–149.
- Aydos, M., Vural, Y. & Tekerek, A. 2019. Assessing risks and threats with layered approach to Internet of Things security. *Measurement and Control*: 1–16.
- Baik, J. (Sophia). 2020. Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA). *Telematics and Informatics*, 52(October 2019): 101431.
- Bailey, R., Parsheera, S., Rahman, F. & Sane, R. 2018. *Disclosures in privacy policies: Does 'notice and consent' work?* New Dehli. <https://www.nipfp.org.in/publications/working-papers/1841/>.
- Baloyi, N. & Kotzé, P. 2018. A Data Privacy Model Based on Internet of Things and Cyber-physical Systems Reference Architectures. In *Proceedings of ACM SAICSIT conference (SAICSIT'18)*. Port Elizabeth, South Africa: Association for Computing Machinery: 258–268.
- Baloyi, N. & Kotzé, P. 2020. Data Privacy Compliance Benefits for Organisations – A Cyber-physical Systems and Internet of Things Study. In H. Venter, M. Looock, M. Coetzee, M. Eloff, & J. Eloff, eds. *Information and Cyber Security. ISSA 2019. Communications in Computer and Information Science*. Springer Cham: 158–172.
- Baloyi, N. & Kotzé, P. 2019. Guidelines for Data Privacy Compliance: A Focus on Cyber-physical Systems and Internet of Things. In *Proceedings of ACM SAICSIT conference (SAICSIT'19)*. Skukuza, South Africa: 1–12.
- Barendt, E. ed. 2017. Privacy. In *The International Library of Essays in Law and Legal Theory*

(*Second Series*). Abingdon: Routledge: 1–30.

- Baxter, G.J., Connolly, T.M., Stansfield, M.H., Gould, C., Tsvetkova, N., Kusheva, R., Stoimenova, B., Penkova, R., Legurska, M. & Dimitrova, N. 2011. Understanding the pedagogy Web 2.0 supports: The presentation of a Web 2.0 pedagogical model. *Proceedings of the 2011 7th International Conference on Next Generation Web Services Practices, NWeSP 2011*: 505–510.
- Baxter, P. & Jack, S. 2008. Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report*, 13(4): 544–559.
- BBC. 2021. Three years of GDPR: the biggest fines so far. <https://www.bbc.com/news/technology-57011639> 7 November 2021.
- Beigi, G. & Liu, H. 2020. *A Survey on Privacy in Social Media*.
- Belanger, F. & Crossler, R.E. 2019. Dealing with digital traces: Understanding protective behaviors on mobile devices. *Journal of Strategic Information Systems*, 28(1): 34–49.
- Bell, J. 2005. *Doing your Research Project: A guide for first-time researchers in education, health and social science*. New York: Open University Press.
- Benbasat, I., Goldstein, D.K. & Mead, M. 1987. The case research strategy in studies of information systems. *MIS Quarterly: Management Information Systems*, 11(3): 369–386.
- Bennett, C.J. & Raab, C.D. 2003. *The Governance of Privacy: Policy instruments in global perspective*. London: Routledge.
- Bhagattjee, P. 2021. South Africa - Data Protection Overview. <https://www.dataguidance.com/notes/south-africa-data-protection-overview> 4 November 2021.
- Bhattacharjee, A. 2012. *Social Science Research: principles, methods, and practices*. Second.
- Blaxter, L., Hughes, C. & Tight, M. 2010. *How to Research*. Fourth. New York: Open University Press.
- Blunden, A. 2009. Criticisms of Vygotsky's concept of activity. *An Interdisciplinary Theory of Activity*, (December): 189–204. <http://home.mira.net/~andy/works/vygotsky-critique.htm>.
- Bold, C. 2012. What Is Narrative? In *Using Narrative in Research*. London, UK: Sage Publications Ltd: 15–31.
- Borgia, E. 2014. The internet of things vision: key features, applications and open issues. *Computer Communications*, 54: 1–31.
- Botha, J. & Grobler, M. 2017. A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws. In *The 12th International Conference on Cyber Warfare and Security (ICCWS)*. Dayton, Ohio: ResearchGate.
- Bowen, G.A. 2009. Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2): 27–40.
- Bowling, A. 2005. Quantitative social science: the survey. In A. Bowling & S. Ebrahim, eds.

- Handbook of Health Research Methods: Investigation, measurement and analysis.* Maidenhead, Berkshire: Open University Press: 190–214.
- Braun, V. & Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2): 77–101.
- Brayne, S. 2017. Big Data Surveillance: The case of policing. *American Sociological Association*, 82(5): 977–1008.
- Brown, M. & Hale, K. 2014. *Applied Research Methods in Public and Nonprofit Organizations.* San Fransisco, California: John Wiley & Sons, Inc.
- Bryman, A. 2012. *Social Research Methods.* Fourth. Oxford: Oxford University Press.
- Burhan, M., Rehman, R.A., Khan, B. & Kim, B.-S. 2018. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors*, 18(9): 1–37.
- Business Insider SA. 2021. Facebook just got 6 extra months to process South African WhatsApp phone numbers. <https://www.businessinsider.co.za/https://www.businessinsider.co.za/information-regulator-postpones-paia-powers-that-could-stop-facebook-processing-whatsapp-data-2021-6> 7 December 2021.
- Butler, J. 2010. *Key Terms in Logic.* F. Russo & J. Williamson, eds. London, UK: Continuum International Publishing Group.
- Bygrave, L.A. 2010. Privacy and Data Protection in an International Perspective. *Scandinavian Studies in Law*, 56: 163–200.
- Byrne, A. & Pfefferle, L. 2015. Creating a Template for the Future: A potential data protection regime between the EU and the US. *European Policy Review*, 1(1): 17–23.
- Cardno, C. 2019. Policy Document Analysis: A Practical Educational Leadership Tool and a Qualitative Research Method. *Educational Administration: Theory and Practice*, 24(4): 623–640.
- Carson, A. 2021. Data privacy laws: What you need to know in 2021. <https://www.osano.com/https://www.osano.com/articles/data-privacy-laws> 6 November 2021.
- Carter, S. & Henderson, L. 2005. Approaches to qualitative data collection in social science. In A. Bowling & S. Ebrahim, eds. *Handbook of Health Research Methods: Investigation, measurement and analysis.* Maidenhead, Berkshire: Open University Press: 215–229.
- Centurion. 2021. POPIA: Do Interim Data Breaches Go Unpunished? <https://centurionlg.com/https://centurionlg.com/2021/07/09/popia-do-interim-data-breaches-go-unpunished/> 21 November 2021.
- Check Point Software Technologies. 2021. *Cyber Attack Trends: 2021 Mid-Year Report.*
- Chiara, P.G. 2020. The Unsecure Side of (Meta) Data in IoT Systems. *Ambient Intelligence and Smart Environments*: 105–114.
- Chong, I., Xiong, A. & Proctor, R.W. 2019. Human Factors in the Privacy and Security of the Internet of Things. *Ergonomics in Design*, 27(3): 5–10.
- Cilliers, L. 2020. Wearable devices in healthcare: Privacy and information security issues. *Health Information Management Journal*, 49(2–3): 150–156.

- Cimpanu, C. 2020. Experian South Africa discloses data breach impacting 24 million customers. <https://www.zdnet.com/article/experian-south-africa-discloses-data-breach-impacting-24-million-customers/> 4 November 2021.
- Clandinin, D.J. & Caine, V. 2013. Narrative Inquiry. In A. A. Trainor & E. Graue, eds. *Reviewing Qualitative Research in the Social Sciences*. New York: Routledge: 166–179.
- Clarke, R. 1999. Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, 42(2): 60–67.
- Clarke, R. 1997. Introduction to dataveillance and information privacy, and definitions of terms. : 1–17.
- Clement, J. 2020. Global number of internet users 2005-2019. *Statista.com*. <https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/> 1 July 2020.
- Cobb, S. 2016. *Data privacy and data protection: US law and legislation*.
- Cohen-Almagor, R. 2011. Internet history. *International Journal of Technoethics*, 2(2): 45–64.
- Conrad, S.S. 2019. Protecting Personal Information and Data Privacy: What Students Need to Know. *J. Comput. Sci. Coll.*, 35(3): 77–86.
- Corbin, J. & Strauss, A. 2008. Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory. <https://methods.sagepub.com/book/basics-of-qualitative-research>.
- Cornwall, A. & Jewkes, R. 1995. What is participatory research? *Social Science and Medicine*, 41(12): 1667–1676.
- Creswell, J.W. 2009. *Research design: Qualitative, quantitative, and mixed methods approaches*. Third. Thousand Oaks, California: Sage Publications.
- Creswell, J.W. 2014. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. Fourth. Thousand Oaks, California: Sage Publications.
- Creswell, J.W., Clark, V.L.P., Gutmann, M.L. & Hanson, W.E. 2003. Advanced mixed methods research designs. In A. Tashakkori & C. Teddlie, eds. *Handbook of mixed methods in social and behavioral research*. Thousand Oaks, California: Sage Publications: 159–196.
- Creswell, J.W. & Creswell, J.D. 2018. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Fifth. Thousand Oaks, California: Sage Publications.
- Cullen, F., Bradford, S. & Green, L. 2012. Working as a practitioner-researcher. In S. Bradford & F. Cullen, eds. *Research and Research Methods for Youth Practitioners*. Abington: Routledge: 18–38.
- Curran, J., Fenton, N. & Freedman, D. 2012. *Misunderstanding the internet*. Oxon: Routledge.
- Danermark, B., Ekström, M., Jakobsen, L. & Karlsson, J.C. 2002. *Explaining Society: Critical realism in the social sciences*. London, UK: Routledge.
- Daniels, H. & Guitierrez, K.D. 2009. *Learning and Expanding with Activity Theory*. A. Sannino, ed. New York: Cambridge University Press.

- Dasgupta, A., Gill, A. & Hussain, F. 2019. A Conceptual Framework for Data Governance in IoT-enabled Digital IS Ecosystems. In *Proceedings of the 8th International Conference on Data Science, Technology and Applications (DATA 2019)*. 209–216.
- Data Privacy Manager. 2020. 5 Things You Should Know About Data Privacy. *dataprivacymanager.net*. <https://dataprivacymanager.net/5-things-you-need-to-know-about-data-privacy/> 14 June 2020.
- Dennedy, M.F., Fox, J. & Finneran, T.R. 2014. *The privacy engineer's manifesto: Getting from policy to code to QA to value*. Apres Media.
- Dey, I. 2004. Grounded Theory. In C. Seale, G. Gobo, J. F. Gubrium, & D. Silverman, eds. *Qualitative Research Practice*. London, UK: Sage Publications: 80–93.
- Diamantopoulou, V., Argyropoulos, N., Kalloniatis, C. & Gritzalis, S. 2017. Supporting the design of privacy-aware business processes via privacy process patterns. *Proceedings - International Conference on Research Challenges in Information Science*: 187–198.
- Diphoko, W. 2021. SA government entities hit by cyber attacks and services affected. <https://www.iol.co.za/technology/sa-government-entities-hit-by-cyber-attacks-and-services-affected-6527c606-4667-4e0c-a162-16f8bc5b2f5a> 4 November 2021.
- Ditsa, G. ed. 2003. *Information Management: Support Systems & Multimedia Technology*. IRM Press.
- Doig, Y., Fuentes, O. & Ortega, A. 2018. Privacy as Data Protection: Some critical legal problems. *Socialsci Journal*, 2(2003): 14–24.
- Doyle, T. 2012. Daniel J. Solove, Nothing to Hide: the false tradeoff between privacy and security. *The Journal of Value Inquiry*, 46(1): 107–112.
- Dudovskiy, J. 2018. *The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance*.
- Dunlap, L., Cummings, J. & Janicki, T. 2017. Information Security and Privacy Legislation: current state and future direction. In *2017 Proceedings of the Conference on Information Systems Applied Research*. Austin, Texas: 1–9.
- Eddine, D., Bouabdallah, A. & Lakhlef, H. 2018. Internet of things security: A top-down survey. *Computer Networks*, 141: 199–221.
- El-Gendy, S. & Azer, M.A. 2020. Security Framework for Internet of Things (IoT). *Proceedings of ICCES 2020 - 2020 15th International Conference on Computer Engineering and Systems*: 0–5.
- Emotiv. Data Privacy. *Emotiv.com*. <https://www.emotiv.com/glossary/data-privacy/> 14 June 2020.
- Etheridge, J. 2018. Hawks, SSA probing major 'leak' of personal data of SA drivers who use ViewFines. <https://www.news24.com/SouthAfrica/News/hawks-ssa-probing-major-leak-of-personal-data-of-sa-drivers-who-use-viewfines-20180524> 11 March 2019.
- European Commission. 2019. Mythbusting: General Data Protection Regulation.
- Fahmideh, M. & Zowghi, D. 2020. An exploration of IoT platform development. *Information*

- Systems*, 87(10409): 1–25.
- Farooq, M.U. & Waseem, M. 2020. A Critical Analysis on the Security Concerns of Internet of Things (IoT). *International Journal of Computer Applications*, 111(7): 1–6.
- Favaretto, M., de Clercq, E., Schneble, C.O. & Elger, B.S. 2020. What is your definition of Big Data? Researchers' understanding of the phenomenon of the decade. *PLoS ONE*, 15(2): 1–20.
- Fazeldehkordi, E., Owe, O. & Noll, J. 2019. Security and Privacy Functionalities in IoT. *2019 17th International Conference on Privacy, Security and Trust, PST 2019 - Proceedings*: 1–12.
- Fefer, R.F. & Archick, K. 2021. EU data protection rules and U.S. implications. *Current Issues in U.S.-European Relations*: 157–162.
- Feltham, L. 2021. Basic web lessons for South Africa: Government hacks point to systematic security issues. <https://mg.co.za/news/2021-09-19-basic-web-lessons-for-south-africa-government-hacks-point-to-systematic-security-issues/> 4 November 2021.
- Fetters, M.D., Curry, L.A. & Creswell, J.W. 2013. Achieving integration in mixed methods designs - Principles and practices. *Health Services Research*, 48(6 PART2): 2134–2156.
- Finn, R.L., Wright, D. & Friedewald, M. 2013. Seven Types of Privacy. In S. Gutwirth, R. Leenes, P. de Hert, & Y. Poullet, eds. *European Data Protection: Coming of Age*. Springer, Dordrecht: 3–32.
- Flick, U. 2009. *An Introduction To Qualitative Research*. Fourth. London, UK: Sage Publications Ltd.
- Fried, C. 1968. Privacy. *Yale Law Journal*, 403: 475–493.
- Friedewald, M., van Lieshout, M., Rung, S., Ooms, M. & Ypma, J. 2015. Privacy and security perceptions of european citizens: A test of the trade-off model. *IFIP Advances in Information and Communication Technology*, 457: 39–53.
- Froomkin, A.M. 2000. The Death of Privacy? *Stanford Law Review*, 52(5): 1461–1543.
- Frustaci, M., Pace, P. & Aloï, G. 2018. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet of Things Journal*, 5(4): 2483–2495.
- Fu, K., Kohno, T., Lopresti, D., Mynatt, E., Nahrstedt, K., Patel, S., Richardson, D. & Zorn, B. 2020. Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things. *Computing Community Consortium*: 1–9.
- Gafurov, K. & Chung, T.M. 2019. Comprehensive survey on internet of things, architecture, security aspects, applications, related technologies, economic perspective, and future directions. *Journal of Information Processing Systems*, 15(4): 797–819.
- Gahi, Y. & Alaoui, I. El. 2019. A secure multi-user database-as-a-service approach for cloud computing privacy. *Procedia Computer Science*, 160: 811–818.
- Gan, M.F., Chua, H.N. & Wong, S.F. 2019. Privacy Enhancing Technologies implementation: An investigation of its impact on work processes and employee perception. *Telematics and Informatics*, 38(August 2018): 13–29.

- Garrett, B. 2018. *Empirical Nursing: The Art of Evidence-Based Care*. Bingley, UK: Emerald Group Publishing Limited.
- Gerring, J. 2007. *Case Study Research: Principles and Practices*. Cambridge, UK: Cambridge University Press.
- Goel, A. & Gupta, L. 2020. Social Media in the Times of COVID-19. *Journal of Clinical Rheumatology*, 26(6): 220–223.
- Gorski, P.S. 2013. "What is Critical Realism? And Why Should You Care?" *Contemporary Sociology: A Journal of Reviews*, 42(5): 658–670.
- Government Gazette. 2019. *Revised Schedule 1 of the National Definition of Small Enterprise in South Africa*.
- Goyal, P., Sahoo, A.K., Sharma, T.K. & Singh, P.K. 2019. Internet of Things: Applications, security and privacy: A survey. *Materials Today: Proceedings*, 34: 752–759.
- Green, A. 2021. Complete Guide to Privacy Laws in the US. <https://www.varonis.com/>. <https://www.varonis.com/blog/us-privacy-laws/> 27 October 2021.
- Greener, S. 2008. *Business research methods*. Ventus Publishing ApS.
- Greenleaf, G. 2013. Data Protection in a Globalised Network. In I. Brown, ed. *Research Handbook on Governance of the Internet*. Cheltenham: Edward Elgar Publishing.
- Greve, M., Masuch, K. & Trang, S. 2020. The more, the better? compensation and remorse as data breach recovery actions - An experimental scenario-based investigation. *Wirtschaftsinformatik*: 1278–1293.
- Grix, J. 2001. *Demystifying Postgraduate Research: From MA to PhD*. Birmingham: University of Birmingham Press.
- Grix, J. 2002. Introducing Students to the Generic Terminology of Social Research. *Politics*, 22(3): 175–186.
- Gross, J.M.S. 2018. To guard against bias, document analysis can be used in conjunction with other data sources, such as interviews, to 'corroborate or refute, elucidate, or expand on findings'. In *International Encyclopedia of Education Research, Measurement, and Evaluation*. Thousand Oaks, California: SAGE Publications, Inc.: 380–385.
- Grossoehme, D.H. 2014. Overview of Qualitative Research. *Journal of Health Care Chaplaincy*, 20(3): 109–122.
- Gruschka, N., Mavroeidis, V., Vishi, K. & Jensen, M. 2019. Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*: 5027–5033.
- Gryz, J. 2017. Privacy as an Asset. In *Proceedings of ACM CASCON*. Markham, Ontario: 266–271.
- Gupta, R.K. & Awasthy, R. eds. 2015. *Qualitative Research in Management: Methods and Experiences*. Sage Publications.
- Gutwirth, S. 2002. *Privacy and the Information Age*. Rowman & Littlefield Publishers.

- Hafner, K. & Lyon, M. 1996. *Where Wizards Stay Up Late: The Origins of the Internet*. New York: Touchstone.
- Haghi Kashani, M., Madanipour, M., Nikravan, M., Asghari, P. & Mahdipour, E. 2021. A systematic review of IoT in healthcare: Applications, techniques, and trends. *Journal of Network and Computer Applications*, 192(July): 103164.
- Hameed, S., Khan, F.I. & Hameed, B. 2019. Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. *Journal of Computer Networks and Communications*, 2019: 1–14.
- Hammond, M. & Wellington, J. 2013. *Research Methods: The Key Concepts*. Abingdon: Routledge.
- Harris, A.L. & Rea, A. 2009. Web 2.0 and Virtual World Technologies: A Growing Impact on IS Education. *Journal of Information Systems*, 20(2): 137–145.
- Harrison, A.K. 2014. Ethnography. In P. Leavy, ed. *The Oxford Handbook of Qualitative Research*. Oxford University Press: 223–253.
- Hasan, H. & Kazlauskas, A. 2014. *Activity Theory: who is doing what, why and how*. University of Wollongong. <https://ro.uow.edu.au/buspapers/403>.
- Hashim, N.H. & Jones, M. 2007. Activity Theory: A framework for qualitative analysis. In *4th International Qualitative Research Convention (QRC)*. Malaysia: 1–21. <http://ro.uow.edu.au/commpapers/408>.
- Hassan, Q.F. ed. 2018. *Internet of Things A to Z: Technologies and Applications*. John Wiley & Sons, Inc.
- Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. & Sikdar, B. 2019. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access*, 7: 82721–82743.
- Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G. & Tsatsoulis, C. 2019. Review of security and privacy for the internet of medical things (IoMT): Resolving the protection concerns for the novel circular economy bioinformatics. *Proceedings - 15th Annual International Conference on Distributed Computing in Sensor Systems, DCOSS 2019*, (May 2019): 457–464.
- Hedley, N. 2018. Facebook data leak exposed up to 60,000 in SA. *Times Live*. <https://www.timeslive.co.za/news/south-africa/2018-04-09-facebook-data-leak-exposed-up-to-60000-in-sa/> 10 March 2019.
- Higginbottom, G. & Liamputtong, P. 2015. What is Participatory Research? Why do it? In G. Higginbottom & P. Liamputtong, eds. *Participatory Qualitative Research Methodologies in Health*. London, UK: Sage Publications: 1–21.
- Holden, M.T. & Lynch, P. 2006. Choosing the Appropriate Methodology: Understanding Research Philosophy. *The Marketing Review*, 4(4): 397–409.
- Hoofnagle, C.J., Sloot, B. Van Der, Borgesius, F.Z., Jay, C., Sloot, B. Van Der & Zuiderveen, F. 2019. The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1): 65–98.

- Horn, J., Koohang, A. & Paliszkiewicz, J. 2019. The Internet of Things: Review and theoretical framework. *Expert Systems With Applications*, 133: 97–108.
- van den Hoven, J., Blaauw, M., Pieters, W. & Warnier, M. 2020. Privacy and Information Technology. *The Stanford Encyclopedia of Philosophy*. <https://seop.illc.uva.nl/entries/it-privacy/> 31 October 2021.
- Howell, K.E. 2013a. Empiricism, Positivism and Post-Positivism. In *An Introduction to the Philosophy of Methodology*. Sage Publications: 32–54.
- Howell, K.E. 2013b. Methods of Data Collection. In *An Introduction to the Philosophy of Methodology*. Sage Publications: 193–210.
- Hughes-Lartey, K., Li, M., Botchey, F.E. & Qin, Z. 2021. Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, 7(3): e06522.
- Hughes, M. & Nimmo, G. 2017. Models of Clinical Reasoning. In N. Cooper & J. Frain, eds. *ABC of Clinical Reasoning*. Oxford: John Wiley & Sons: 17–21.
- Hussain, F. 2017. *Internet of Things: Building Blocks and Business Models*. Springer.
- Hyde, K.F. 2000. Recognising deductive processes in qualitative research. *Qualitative Market Research: An International Journal*, 3(2): 82–90.
- IBM Security. 2021. *Cost of a Data Breach Report*. New York.
- IBM Security. 2020. *Cost of a Data Breach Report*. New York.
- Information Commissioner's Office. Introduction to Data Protection. [ico.org.uk. https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/](https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/) 14 June 2020.
- Information Regulator (South Africa). 2021. Information Regulator's IT systems affected by a ransomware attack on the Department of Justice & Constitutional Development.
- International Trade Administrator. 2021. South Africa - Country Commercial Guide. <https://www.trade.gov>. <https://www.trade.gov/knowledge-product/south-africa-information-technology> 15 November 2021.
- Irwin, L. 2020. The 6 most common ways data breaches occur. <https://www.itgovernance.eu/blog/en/the-6-most-common-ways-data-breaches-occur> 8 November 2021.
- Ivankova, G. V., Mochalina, E.P. & Goncharova, N.L. 2020. Internet of Things (IoT) in logistics. *IOP Conference Series: Materials Science and Engineering*, 940(1).
- Jacobs, Y. 2021. WhatsApp privacy policy updates: Information Regulator threatens legal action. <https://www.iol.co.za/>. <https://www.iol.co.za/technology/mobile/whatsapp-privacy-policy-updates-information-regulator-threatens-legal-action-93b1c700-0d20-4e69-9de6-e37a0680319c> 7 December 2021.
- Jha, K., Anumotu, S., Pronika & Soni, K. 2021. Security Issues and Architecture of IOT. *Proceedings - International Conference on Artificial Intelligence and Smart Systems, ICAIS 2021*: 1381–1385.
- Jiang, Y., Wang, C., Wang, Y. & Gao, L. 2019. A cross-chain solution to integrating multiple

- blockchains for IoT data management. *Sensors (Switzerland)*, 19(9): 1–18.
- Job, A. 2018. Did one simple issue crash Liberty? *IT Web*. <https://www.itweb.co.za/content/dgp45qaGabl7X9l8> 23 March 2019.
- Johnson-Laird, P.N. 1999. Deductive reasoning. *Annual Review of Psychology*, 50: 109–135.
- Jonassen, D.H. & Ronrer-Murphy, L. 1999. Activity Theory as a Framework for Designing Constructivist Learning Environments. *ETR&D*, 47(1): 61–79.
- Jozani, M., Ayaburi, E., Ko, M. & Choo, K.K.R. 2020. Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, 107(August 2019): 106260.
- Kandasamy, K., Srinivas, S., Achuthan, K. & Rangan, V.P. 2020. IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *Eurasip Journal on Information Security*, 2020(8): 1–18.
- Kandeh, A.T., Botha, R.A. & Futchet, L.A. 2018. Enforcement of the Protection of Personal Information (POPI) Act: Perspective of data management professionals. *SA Journal of Information Management*, 20(1): 1–9.
- Kaptelinin, V. & Nardi, B. eds. 2006. *Acting with Technology*. The MIT Press.
- Kassab, W. & Darabkh, K.A. 2020. A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations. *Journal of Network and Computer Applications*, 163(September 2019): 102663.
- Kaur, J. & Kaur, K. 2017. Internet of Things: a review on technologies, architecture, challenges, applications, future trends. *I.J. Computer Network and Information Security*, 4(April): 57–70.
- Kaur, N., Azam, S., Kannoorpatti, K., Yeo, K.C. & Shanmugam, B. 2017. Browser Fingerprinting as User Tracking Technology. In *2017 11th International Conference on Intelligent Systems and Control (ISCO)*. Coimbatore, India: IEEE: 103–111.
- Khanna, A. & Kaur, S. 2020. Internet of Things (IoT), Applications and Challenges: A Comprehensive Review. *Wireless Personal Communications*, 114: 1687–1762.
- Khayyat, M. 2016. A Proposed Model for the Fourth Generation of Activity Theory to be Applied on the Smart City Research. In *Thirty Seventh International Conference on Information Systems*. Dublin: 1–9. https://www.researchgate.net/profile/Mashael_Khayyat/publication/311677620_A_proposed_model_for_the_fourth_generation_of_Activity_Theory_to_be_applied_on_the_Smart_City_Research_Arena/links/5853ef3108ae95fd8e1ff46b/A-proposed-model-for-the-fourth-generati.
- Killam, L. 2013. *Research Terminology Simplified: Paradigms, Axiology, Ontology, Epistemology and Methodology*. Sudbury, ON.
- Kivunja, C. & Kuyini, A.B. 2017. Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of Higher Education*, 6(5): 26–41.
- Klein, H.K. & Myers, M.D. 1999. A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS quarterly*, 23(1): 67–94.

- Klenke, K. 2016. *Qualitative Research in the Study of Leadership*. Second. Bingley, UK: Emerald Group Publishing Limited.
- Kothari, C.R. 2004. *Research methodology: methods and techniques*. Second. New Dehli: New Age International Publishers.
- Krishnaswami, O.R. & Satyaprasad, B.G. 2010. *Business Research Methods*. Mumbai, India: Himalaya Publishing House.
- Kuada, J. 2012. *Research Methodology: A Project Guide for University Students*. Samfundslitteratur.
- Kumar, R. 2011. *Research methodology: a step-by-step guide for beginners*. 3rd ed. London: Sage Publications.
- Kuutti, K. 1995. Activity Theory as a Potential Framework for Human-Computer Interaction Research. In B. A. Nardi, ed. *Context and Consciousness: Activity Theory and Human-Computer Interaction*. London: The MIT Press: 9–22.
- Ladley, J. 2012. *Data Governance: how to design, deploy, and sustain an effective data governance program*. A. Dierna & R. Day, eds. Elsevier Inc.
- Ladyman, J. 2002. *Understanding Philosophy of Science*. London, UK: Routledge.
- Leavy, P. 2017. *Research Design: Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches*. New York: The Guildford Press.
- Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G. & Wolff, S.S. 1997. The past and future history of the Internet. *Communication of the ACM*, 40(2): 102–108.
- Leloglu, E. 2017. A Review of Security Concerns in Internet of Things. *Journal of Computer and Communications*, 5: 121–136.
- Leskin, P. 2018. The 21 scariest data breaches of 2018. *Business Insider*. <https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12?IR=T> 24 March 2019.
- Levy, M. 2009. WEB 2.0 implications on knowledge management. *Journal of Knowledge Management*, 13(1): 120–134.
- Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. & Zhao, W. 2017. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal*, 4(5): 1125–1142.
- Liquid Cyber Security. 2021. *The evolving Cyber Security threat in Africa*.
- Lockhat, R. 2021. Social media and the Protection of Personal Information Act. *Southern African Journal of Anaesthesia and Analgesia*, 27: 69–72.
- Lukacs, A. 2017. *What Is Privacy? The history and definition of privacy*. University of Szeged.
- Luyt, D. 2019. Information Security and the Internet of Things. <https://www.michalsons.com/blog/information-security-and-the-internet-of-things/38945> 24 November 2021.

- Mack, L. 2010. The philosophical underpinnings of educational research. *Polyglossia*, 19: 5–11.
- Mahlaka, R. 2020. SA's regulator battles to cope with increasing data breach incidents as funding dries up. <https://www.dailymaverick.co.za/article/2020-08-24-sas-regulator-battles-to-cope-with-increasing-data-breach-incidents-as-funding-dries-up/> 7 December 2021.
- Makridis, C.A. 2021. Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. *Journal of Cybersecurity*, 7(1): 1–8.
- Malinga, S. 2019. Data breaches affect over 1bn users in 2018. *IT Web*. <https://www.itweb.co.za/content/8OKdWMDEGDXqbznQ> 23 March 2019.
- Malinga, S. 2021. Justice dept cyber attack spills over to Info Regulator. <https://www.itweb.co.za/>. <https://www.itweb.co.za/content/xA9PO7NZOBI7o4J8> 4 November 2021.
- Manda, M.I. 2017. Towards “Smart Governance” Through a Multidisciplinary Approach to E-government Integration, Interoperability and Information Sharing: A Case of the LMIP Project in South Africa. In M. Janssen, K. Axelsson, O. Glassey, B. Klievink, R. Krimmer, I. Lindgren, P. Parycek, H. J. Scholl, & D. Trutnev, eds. *Electronic Government*. St. Petersburg: Springer: 36–44.
- Marcus, D.J. 2018. The Data Breach Dilemma: proactive solutions for protecting consumers' personal information. *Duke Law Journal*, 68: 555–593.
- Marczyk, G., DeMatteo, D. & Festinger, D. 2005. *Essentials of research design and methodology*. A. S. Kaufman & N. L. Kaufman, eds. Hoboken, New Jersey: John Wiley & Sons.
- Marks, G. 2021. A Casino Gets Hacked Through a Fish-Tank Thermometer. <https://www.entrepreneur.com/>. <https://www.entrepreneur.com/article/368943> 22 November 2021.
- Marsh, D. & Furlong, P. 2002. A Skin Not a Sweater: Ontology and Epistemology in Political Science. In *Theory and Methods in Political Science*. 17–41.
- Martin, W.J. 1988. The information society—idea or entity? *Aslib Proceedings*, 40(11–12): 303–309.
- Masse, E. 2018. Data protection: why it matters and how to protect it. *Accessnow.org*. <https://www.accessnow.org/data-protection-matters-protect/> 14 June 2020.
- Matos, E. de, Amaral, L.A. & Hessel, F. 2017. Context-Aware Systems: Technologies and Challenges in Internet of Everything Environments. In J. M. Batalla, G. Mastorakis, C. X. Mavromoustakis, & E. Pallis, eds. *Beyond the Internet of Things: Everything Interconnected*. Switzerland: Springer: 3–27.
- Mavriki, P. & Karyda, M. 2018. Profiling with Big Data: Identifying privacy implication for individuals, groups and society. In *MCIS 2018 Proceedings*. Corfu: 1–14.
- Mavrommati, I., Birbilis, G. & Darzentas, J. 2013. A conceptual framework for the design of IoT architectures that support end-user development. *Networking Science*, 3(1–4): 71–81.

- Mayring, P. 2014. *Qualitative Content Analysis: theoretical foundation, basic procedures and software solution*. Klagenfurt.
- Mbonye, V., Subramaniam, P.R. & Padayachee, I. 2021. POPIA Compliant Regulatory Framework for Smart Grids to Secure Gaps in Existing Privacy Laws. *icABCD 2021 - 4th International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems, Proceedings*: 1–8.
- McCausland, C., Pyke, S. & O'Sullivan, S. 2018. The Ethics and Politics of Drones in Animal Activism. *Animals Studies Journal*, 7(1): 80–103.
- McKane, J. 2020. South Africa's POPI Act – What you need to know. *My Broadband*. <https://mybroadband.co.za/news/government/345917-south-africas-popi-act-what-you-need-to-know.html> 1 June 2020.
- Medhora, R.P. 2018. *Data governance in the digital age*. Ontario.
- Merriam, S.B. & Tisdell, E.J. 2016. *Qualitative Research: A Guide to Design and Implementation*. Fourth. San Fransisco, California: John Wiley & Sons, Inc.
- Mills, A.J. & Mills, J.H. 2018. Archival Research. In C. Cassell, A. L. Cunliffe, & G. Grandy, eds. *The SAGE Handbook of Qualitative Business and Management Research Methods: Methods and Challenges*. City Road, London: Sage Publications Ltd: 32–45.
- Mishra, D.S.B. & Alok, D.S. 2017. *Handbook of Research Methodology: A Compendium for Scholars & Researchers*. EDUCREATION PUBLISHING.
- Mligo, E.S. 2016. *Introduction to Research Methods and Report Writing: A Practical Guide for Students and Researchers in Social Sciences and the Humanities*. Eugene, Oregon: Resource Publications.
- Mohajan, H.K. 2018. Qualitative Research Methodology in Social Sciences and Related Subjects. *Journal of Economic Development, Environment and People*, 7(1): 23.
- Mohapi, T. 2020. South Africa's notable data breaches and data leaks in the past half-decade. <https://iafrikan.com/>. <https://iafrikan.com/2020/10/27/south-africa-biggest-top-data-breaches-leaks/> 16 November 2021.
- Mohlameane, M. & Ruxwana, N. 2020. Exploring the impact of cloud computing on existing South African regulatory frameworks. *SA Journal of Information Management*, 22(1): 1–9.
- Moon, K. & Blackman, D. 2014. A Guide to Understanding Social Science Research for Natural Scientists. *Conservation Biology*, 28(5): 1167–1177.
- Moore, A. 2008. Defining privacy. *Journal of Social Philosophy*, 39(3): 411–428.
- Moore, N., Salter, A., Stanley, L. & Tamboukou, M. 2017. *The Archive Project: Archival Research in the Social Sciences*. Abingdon, Oxon: Routledge.
- Morar, B., Barkawie, Y., Balakrishnan, R., Khasawneh, M., Bangara, J. & Baker, H.A. 2021. *IoT Governance framework*.
- Mowery, D.C. & Simcoe, T. 2002. Is the Internet a US invention? - An economic and technological history of computer networking. *Research Policy*, 31(8–9): 1369–1387.

- Moyo, A. 2019. Final POPI regulations published. *IT Web*. <https://www.itweb.co.za/content/GxwQDq1A9rPqIPVo> 18 March 2019.
- Moyo, A. 2021a. No extension to POPI Act grace period, says info regulator. <https://www.itweb.co.za/>. <https://www.itweb.co.za/content/WnpNgM2KkBQqVrGd> 21 November 2021.
- Moyo, A. 2018. SA's average data breach costs escalate. *IT Web*. <https://www.itweb.co.za/content/Pero37ZgOnXMQb6m> 9 March 2019.
- Moyo, A. 2021b. SA's govt entities under attack as space agency hit by data breach. <https://www.itweb.co.za/>. <https://www.itweb.co.za/content/6GxRKMYJy1bqb3Wj> 9 November 2021.
- Mujere, N. 2016. Sampling in Research. In M. Baran & J. Jones, eds. *Mixed Methods Research for Improved Scientific Study*. 107–121.
- Muntjir, M., Rahul, M. & Alhumyani, H.A. 2017. An Analysis of Internet of Things (IoT): Novel Architectures, Modern Applications, Security Aspects and Future Scope with Latest Case Studies IoT in Latest Trends. *International Journal of Engineering Research & Technology*, 6(06): 422–448.
- Mursu, Á., Luukkonen, I., Toivanen, M. & Korpela, M. 2007. Activity Theory in information systems research and practice: Theoretical underpinnings for an information systems development model. *Information Research*, 12(3): 1–21.
- Naeini, P.E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. & Sadeh, N. 2017. Privacy Expectations and Preferences in an IoT World. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA: 399–412.
- Nardi, B.A. 1995. Activity Theory and Human-Computer Interaction. In B. A. Nardi, ed. *Context and Consciousness: Activity Theory and Human-Computer Interaction*. 4–8.
- Nathanael, D., Marmaras, N. & Papantoniou..., B. 2002. Socio-technical Systems Analysis: Which approach should be followed? *Cognition, Culture & Design*: 137–142. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.112.6190&rep=rep1&type=pdf>.
- National Intelligence Council (U.S.). 2008. *Disruptive Civil Technologies: Six Technologies With Potential Impacts on US Interests Out to 2025*.
- Naughton, J. 2016. The evolution of the Internet: from military experiment to General Purpose Technology. *Journal of Cyber Policy*, 1(1): 5–28.
- NetApp. 2020. *Worldwide Data Privacy Regulations Compared*.
- Netshakhuma, N.S. 2020. Assessment of a South Africa national consultative workshop on the Protection of Personal Information Act (POPIA). *Global Knowledge, Memory and Communication*, 69(1–2): 58–74.
- Neuman, W.L. 2014. *Social Research Methods: Qualitative and Quantitative Approaches*. Seventh. Essex: Pearson Education Limited.
- Neves, J. 2021. How vulnerable is South Africa to cyber attacks? <https://www.biznews.com/thought-leaders/2021/09/03/cyber-attacks> 4 November 2021.

- Neville, C. 2005. Introduction to research and research methods. : 1–44.
- New Zealand Human Rights Commission. 2018. *Privacy , Data and Technology: Human Rights Challenges in the Digital Age*. Auckland.
- Newman, R., Chang, V., Walters, R.J. & Wills, G.B. 2016. Web 2.0 – The past and the future. *International Journal of Information Management*, 36: 591–598.
- Ngwenya, M. & Ngoepe, M. 2020. A framework for data security, privacy, and trust in 'consumer internet of things' assemblages in South Africa. *Security and Privacy*, 3(122): 1–10.
- Niculescu, R., Huth, M., Radanliev, P. & Roure, D. De. 2018. Mapping the values of IoT. *Journal of Information Technology*, 33: 345–360.
- van Niekerk, G. 2017. 'Master Deeds' Data Breach: The Full Investigation. *Huffpost*. https://www.huffingtonpost.co.uk/2017/10/19/master-deeds-data-breach-the-full-investigation_a_23248618/?ncid=other_saredirect_m2afnz7mbfm 11 March 2019.
- Nissim, K. & Wood, A. 2018. Is privacy privacy? *Philosophical Transactions Royal Society A*, 376: 1–17.
- Noor, M.B.M. & Hassan, W.H. 2019. Current research on Internet of Things (IoT) security: A survey. *Computer Networks*, 148: 283–294.
- NortonLifeLock. What Is Data Privacy and Why Is it Important? *LifeLock.com*. <https://www.lifelock.com/learn-identity-theft-resources-what-is-data-privacy-and-why-is-it-important.html> 14 June 2020.
- Nowell, L.S., Norris, J.M., White, D.E. & Moules, N.J. 2017. Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, 16(1): 1–13. <https://doi.org/10.1177/1609406917733847>.
- O'Dea, S. 2021. Smartphone users worldwide 2016-2021. <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/> 31 October 2021.
- O'Reilly, T. 2009. *What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software*. O'Reilly Media Inc.
- Oates, M., Ahmadullah, Y., Marsh, A., Swoopes, C., Zhang, S., Rebecca, B. & Cranor, L.F. 2018. Turtles, Locks, and Bathrooms: Understanding mental models of privacy through illustration. In *Proceedings on Privacy Enhancing Technologies*. 5–32.
- Organisation For Economic Co-Operation and Development (OECD). 2011. *Thirty Years After the OECD Privacy Guidelines*.
- Orlikowski, W.J. & Baroudi, J.J. 1991. Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research*, 2(1): 1–28.
- Oussous, A., Benjelloun, F.Z., Ait Lahcen, A. & Belfkih, S. 2018. Big Data technologies: A survey. *Journal of King Saud University - Computer and Information Sciences*, 30(4): 431–448.
- Palić, M., Vignali, C., Hallier, B. & Stanton, J.L. 2015. Research Methodology. *International*

Journal of Sales, Retailing and Marketing, 4(9).

- Palmieri III, N. 2020. Who Should Regulate Data?: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws. *Hastings Science and Technology Law Journal*, 11(1): 37–60. https://repository.uchastings.edu/hastings_science_technology_law_journal/vol11/iss1/4.
- Parikli, S., Dave, D., Patel, R. & Doshi, N. 2019. Security and privacy issues in cloud, fog and edge computing. *Procedia Computer Science*, 160: 734–739.
- Park, M., Oh, H. & Lee, K. 2019. Security Risk Measurement for Information Leakage Awareness Perspective. *Sensors*, 19(2148): 1–24.
- Patra, J., Gantait, A. & Mukherjee, A. 2018. Governing your IoT data: how to manage enterprise-wide IoT initiatives. *IBM Developer*. <https://developer.ibm.com/articles/iot-governance-03/> 30 May 2019.
- Patton, M.Q. 2015. *Qualitative Research & Evaluation Methods*. Fourth. Thousand Oaks, California: Sage Publications, Inc.
- Paulus, T.M. 2018. ATLAS.ti. In B. B. Frey, ed. *The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation*. Thousand Oaks, California: SAGE Publications, Inc.: 130–132.
- Peerzade, E. 2021. The role of IoT sensors in the COVID-19 fight. <https://www.fierceelectronics.com/>. <https://www.fierceelectronics.com/electronics/role-iot-sensors-covid-19> 2 November 2021.
- Persson, S., Serrato, J.K., Roosa, S., Fernandez, A. & Rudawski, A. 2018. California passes major legislation, expanding consumer privacy rights and legal exposure for US and global companies. *Data Protection Report*. <https://www.dataprotectionreport.com/2018/06/california-passes-major-privacy-legislation-expanding-consumer-privacy-rights/> 19 March 2019.
- Peters, J. 2020. Data Privacy Guide: Definitions, Explanations and Legislation. <https://www.varonis.com/blog/data-privacy/#dimensions> 14 June 2020.
- Phillips, B.D. 2014. Qualitative Disaster Research. In P. Leavy, ed. *The Oxford Handbook of Qualitative Research*. Oxford: Oxford University Press: 533–556.
- Phillips, P.P. & Stawarsk, C.A. 2008. *Data Collection: Planning For and Collecting All Types of Data*. San Fransisco, California: John Wiley & Sons, Inc.
- Pico-Valencia, P., Holgado-Terriza, J.A., Herrera-Sánchez, D. & Sampietro, J. 2018. Towards the internet of agents: An analysis of the internet of things from the intelligence and autonomy perspective. *Ingeniería e Investigación*, 38(1): 121–129.
- Pizzirani, A., Di Gioia, R., Chaudron, S., Draper, G.G. & Sanchez, I. 2017. *Privacy safeguards and online anonymity*.
- Ponemon Institute LLC. 2018. *2018 Cost of a Data Breach Study: Global Overview*. <https://www.ibm.com/security/data-breach>.
- Prevailion. 2021. Why Corporate Hacks Go Unreported. <https://www.prevailion.com/>.

- <https://www.prevailion.com/why-corporate-hacks-go-unreported/> 20 November 2021.
- Priharti, W., Sumaryo, S., Saraswati, T. & Nurfadilah, M.R. 2020. IoT Based Logistics Vehicle Security Monitoring System. *IOP Conference Series: Materials Science and Engineering*, 771(1).
- Privacy International. 2017. 101: Data Protection. *privacyinternational.org*. <https://privacyinternational.org/explainer/41/101-data-protection> 14 June 2020.
- Radoglou Grammatikis, P.I., Sarigiannidis, P.G. & Moscholios, I.D. 2019. Securing the Internet of Things: Challenges, threats and solutions. *Internet of Things (Netherlands)*, 5: 41–70. <https://doi.org/10.1016/j.iot.2018.11.003>.
- Rayes, A. & Salam, S. 2017. *Internet of Things From Hype to Reality: The Road to Digitization*. 2nd ed. Springer.
- Reed, M. 2005. Reflections on the 'realist turn' in organization and management studies. *Journal of Management Studies*, 42(8): 1621–1644.
- Reinwarth, M. 2019. CCPA: GDPR as a Catalyst for Improving Data Protection Outside the EU. <https://www.kuppingercole.com/>. <https://www.kuppingercole.com/blog/reinwarth/ccpa-gdpr-as-a-catalyst-for-improving-data-protection-outside-the-eu> 6 November 2021.
- Ren, Z., Liu, X., Ye, R. & Zhang, T. 2017. Security and Privacy on Internet of Things. In *Proceedings 2017 IEEE 7th International Conference on Electronics Information and Emergency Communication*.
- Richardson, M., Bosua, R., Clark, K., Webb, J., Ahmad, A. & Maynard, S. 2017. Towards responsive regulation of the internet of things: Australian perspectives. *Internet Policy Review*, 6(1): 1–14.
- Robinson, R. 2020. Data Privacy vs. Data Protection. *ipswitch.com*. <https://blog.ipswitch.com/data-privacy-vs-data-protection> 14 June 2020.
- Robson, C. & McCartan, K. 2016. *Real World Research: A Resource for Users of Social Research Methods in Applied Settings*. Fourth. Chichester: John Wiley & Sons Ltd.
- Roos, A. 2012. Activity theory as a theoretical framework in the study of information practices in molecular medicine. *Information Research*, 17(3): 1–21.
- Roos, A. 2021. The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles'. *Comparative and International Law Journal of Southern Africa*, 53(3).
- Roux, E. 2021. POPI comes into effect on 1 July 2021 – What you need to know. *The South African*. <https://www.thesouthafrican.com/lifestyle/pop-i-comes-into-effect-on-1-july-2021-what-you-need-to-know/> 7 October 2021.
- Rudo, H.P. & Reagan, A. 2021. The global landscape of data privacy: Important points about new laws in three key jurisdictions. *Practical Compliance*.
- Rugg, G. & Petre, M. 2007. *A Gentle Guide to Research Methods*. Maidenhead, Berkshire: Open University Press.

- Russell, B.H. 2006. *Research Methods in Anthropology: Qualitative and Quantitative Methods*.
- Ryan, G. 2018. Introduction to positivism, interpretivism and critical theory. *Nurse Researcher*, 25(4): 14–20.
- Saldaña, J. 2009. *The Coding Manual for Qualitative Researchers*. London, UK: Sage Publications.
- Salkind, N.J. ed. 2010. Narrative Research. In *Encyclopedia of Research Design*. Thousand Oaks, California: Sage Publications Ltd: 869–874.
- Sani Cln, L.I. 2013. Data Collection Techniques a Guide for Researchers in Humanities and Education. *International Research Journal of Computer Science and Information Systems (IRJCSIS)*, 2(3): 40–44. <http://www.interestjournals.org/IRJCSIS>.
- Santanen, E. 2019. The value of protecting privacy. *Business Horizons*, 62(1): 5–14.
- Saunders, M. & Lewis, P. 2012. *Doing Research in Business & Management: an essential guide to planning your project*. Essex: Pearson Education Limited.
- Saunders, M., Lewis, P. & Thornhill, A. 2009. *Research methods for business students*. Fifth. Pearson Education Limited.
- Saunders, M., Lewis, P. & Thornhill, A. 2019. Understanding research philosophy and approaches to theory development. In *Research Methods for Business Students*. Pearson Education Limited: 128–171.
- Saura, J.R., Ribeiro-Soriano, D. & Palacios-Marqués, D. 2021. Setting Privacy “by Default” in Social IoT: Theorizing the Challenges and Directions in Big Data Research. *Big Data Research*, 25: 100245.
- Sayer, A. 2000. *Realism and social science*. London, UK: Sage Publications.
- Schwartz-Shea, P. & Yanow, D. 2012. *Interpretive Research Design: Concepts and Processes*. New York: Routledge.
- Schwartz, P.M. 2019. Global data privacy: The EU way. *New York University Law Review*, 94(4): 771–818.
- Schwartz, P.M. & Peifer, K.-N. 2017. Transatlantic Data Privacy Law. *Georgetown Law Journal*, 15(4): 250–260.
- Seals, T. 2021. IoT Attacks Skyrocket, Doubling in 6 Months. <https://threatpost.com/https://threatpost.com/iot-attacks-doubling/169224/> 2 November 2021.
- Sekgweleo, T. 2019. Critical analysis of PoPI Act within the organisation. *International Journal of Computer Science and Information Security (IJCSIS)*, 17(9): 64–69.
- Sethi, P. & Sarangi, S.R. 2017. Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*: 1–26. <https://doi.org/10.1155/2017/9324035>.
- Shin, D.-H. & Park, Y.J. 2017. Understanding the Internet of Things ecosystem: multi-level analysis of users, society, and ecology. *Digital Policy, Regulation and Governance*, 19(1): 77–100.

- Simha, C.Y., Harshini, V.M., Raghuvamsi, L.V.S. & Kounte, M.R. 2018. Enabling Technologies for Internet of Things & Its Security issues. *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, (June): 1849–1852.
- Simons, H. 2014. Case Study Research: In-Depth Understanding in Context. In P. Leavy, ed. *The Oxford Handbook of Qualitative Research*. Oxford: Oxford University Press: 455–470.
- Sinclair, B. 2021. PlayStation Network's 24 days of downtime | 10 Years Ago This Month. <https://www.gamesindustry.biz/>. <https://www.gamesindustry.biz/articles/2021-04-14-playstation-networks-24-days-of-downtime-10-years-ago-this-month> 22 November 2021.
- Singh, A. & Mahapatra, S. 2020. Network-Based Applications of Multimedia Big Data Computing in IoT Environment. In S. Tanwar, S. Tyagi, & N. Kumar, eds. *Multimedia Big Data Computing for IoT Applications: Concept, Paradigms and Solutions*.
- Singh, S., Singh, K. & Saxena, A. 2020. Security Domain, Threats, Privacy issues in the Internet of Things (IoT): A Survey. *Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020*: 287–294.
- Sinha, S. 2021. State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 billion globally, cellular IoT now surpassing 2 billion. <https://iot-analytics.com/>. <https://iot-analytics.com/number-connected-iot-devices/> 11 October 2021.
- Smith, T., Tadesse, A.F. & Vincent, N.E. 2021. The impact of CIO characteristics on data breaches. *International Journal of Accounting Information Systems*, 43(February 2020): 100532.
- Sobers, R. 2021. 98 Must-Know Data Breach Statistics for 2021. <https://www.varonis.com/>. <https://www.varonis.com/blog/data-breach-statistics/> 17 November 2021.
- Soiferman, L.K. 2010. Inductive and Deductive Research Approaches. , (April): 1–23.
- Solove, D.J. 2006. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3): 477–564. <https://www.jstor.org/stable/40041279>.
- Solove, D.J. 2002. Conceptualizing Privacy. *California Law Review*, 90(4): 1088–1156.
- Solove, D.J. 2004. *The Digital Person: technology and privacy in the information age*. New York: New York University Press.
- SonicWall. 2021. 2020 SonicWall Cyber Threat Report. <https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/>.
- South African Government. 2021. South Africa's provinces. <https://www.gov.za/>. <https://www.gov.za/about-sa/south-africas-provinces> 14 October 2021.
- Spencer, R., Pryce, J.M. & Walsh, J. 2014. Philosophical Approaches to Qualitative Research. In P. Leavy, ed. *The Oxford Handbook of Qualitative Research*. Oxford University Press: 81–98.
- Stake, R.E. 2005. Qualitative Case Studies. In N. K. Denzin & Y. S. Lincoln, eds. *The SAGE Handbook of Qualitative Research*. Thousand Oaks, California: Sage Publications, Inc: 443–466.

- Stake, R.E. 1995. *The Art of Case Study Research*. Thousand Oaks, California: Sage Publications, Inc.
- Statista Research Department. 2021a. Biggest data breach fines and settlements worldwide as of August 2020. <https://www.statista.com/statistics/1170520/worldwide-data-breach-fines-settlements/> 9 November 2021.
- Statista Research Department. 2021b. Global social networks ranked by number of users 2021. <https://www.statista.com/>. <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> 31 October 2021.
- Steinfeld, N. 2017. Track me, track me not: Support and consent to state and private sector surveillance. *Telematics and Informatics*, 34(8): 1663–1672. <http://dx.doi.org/10.1016/j.tele.2017.07.012>.
- Stewart, A. 2014. Case Study. In *Qualitative Methodology: A Practical Guide*. London, UK: Sage Publications: 145–160.
- Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E. & Markakis, E.K. 2020. A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE Communications Surveys and Tutorials*, 22(2): 1191–1221.
- Sun, P.J. 2020. Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, 160(August 2019): 102642. <https://doi.org/10.1016/j.jnca.2020.102642>.
- Swartz, P., Veiga, A. Da & Martins, N. 2019. A conceptual privacy governance framework. In *Conference on Information Communications Technology and Society (ICTAS)*. IEEE: 1–6.
- Swartz, P., Da Veiga, A. & Martins, N. 2021. Validating an information privacy governance questionnaire to measure the perception of employees. *Information and Computer Security*, 29(5): 761–786.
- Swire, P.P. & Ahmad, K. 2012. *Foundations of Information Privacy and Data Protections*. Portsmouth: International Association of Privacy Professionals.
- Tadevosyan, G. & Schoenhuth, M. 1997. Participatory Research Approach: Principles, Challenges and Perspectives. , 55(1): 69–75.
- Talari, G., Cummins, E., McNamara, C. & O'Brien, J. 2021. State of the art review of Big Data and web-based Decision Support Systems (DSS) for food safety risk assessment with respect to climate change. *Trends in Food Science & Technology*, (March).
- Tewari, A. & Gupta, B.B. 2020. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future Generation Computer Systems*, 108: 909–920. <https://doi.org/10.1016/j.future.2018.04.027>.
- Thales. 2021. *2021 Thales Cloud Security Study*.
- The Department of Trade and Industry. 2020. *Investing in South Africa's Global Business Services Sector*.
- The Heritage Foundation. 2020. *2021 Index of Economic Freedom: South Africa*.

- Thinakaran, K., Dhillon, J.S., Gunasekaran, S.S. & Chen, L.F. 2017. A conceptual privacy framework for privacy-aware IoT health applications. In J. Zulikha & N. H. Zakaria, eds. *Proceedings of the 6th International Conference on Computing and Informatics*. Kuala Lumpur: 175–183.
- Thompson, D. ed. 1993. *The Oxford Dictionary of Current English*. Second. Oxford: Oxford University Press.
- Thomson, J.J. 1975. The Right to Privacy. *Philosophy & Public Affairs*, 4(4): 295–314.
- Thorburn, R., Margheri, A. & Paci, F. 2019. Towards an integrated privacy protection framework for IoT: contextualising regulatory requirements with industry best practices. In *Living in the Internet of Things*. 1–6.
- Toker, K.A. 2013. Data Protection. In S. O. Idowu, N. Capaldi, L. Zu, & A. D. Gupta, eds. *Encyclopedia of Corporate Social Responsibility*. Berlin, Heidelberg: Springer: 752–758.
- Tsegaye, T. & Flowerday, S. 2019. PoPI compliance through access control of electronic health records. *ACM International Conference Proceeding Series*, (September).
- Ud Din, I., Guizani, M., Hassan, S., Kim, B.S., Khurram Khan, M., Atiquzzaman, M. & Ahmed, S.H. 2019. The Internet of Things: A Review of Enabled Technologies and Future Challenges. *IEEE Access*, 7: 7606–7640.
- Ul Hassan, M., Rehmani, M.H. & Chen, J. 2019. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Generation Computer Systems*, 97: 512–529.
- Vailshery, L.S. 2021. Number of internet of things (IoT) connected devices worldwide in 2018, 2025 and 2030. *Statista Research Department*. <https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/> 10 October 2021.
- Vaismoradi, M., Jones, J., Turunen, H. & Snelgrove, S. 2016. Theme development in qualitative content analysis and thematic analysis. *Journal of Nursing Education and Practice*, 6(5).
- Vakkayil, J.D. 2010. Activity theory: A useful framework for analysing project-based organizations. *Vikalpa*, 35(3): 1–18.
- Varrella, S. 2021. African countries with the highest Gross Domestic Product (GDP) in 2021. <https://www.statista.com/>. <https://www.statista.com/statistics/1120999/gdp-of-african-countries-by-country/> 14 October 2021.
- Venktesh, K. 2017. Ster-Kinekor website flaw puts 7 million users' data at risk. *Fin24*. <https://www.fin24.com/Tech/News/ster-kinekor-website-flaw-puts-7-million-users-data-at-risk-20170316> 11 March 2019.
- Vermeulen, J. 2021. Experian data of 25 million South Africans re-leaked on Telegram. <https://mybroadband.co.za/>. <https://mybroadband.co.za/news/security/420238-experian-data-on-25-million-south-africans-re-leaked-on-telegram.html> 27 November 2021.
- Virat, M.S., Bindu, S., Aishwarya, B., Dhanush, B. & Kounte, M.R. 2018. Security and Privacy Challenges in Internet of Things. In *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018)*. IEEE: 454–460.

- Vogt, P.W., Gardner, D.C. & Haeffelle, L.M. 2012. *When to Use What Research?* New York: The Guildford Press.
- Wach, E. 2013. Learning about Qualitative Document Analysis. *IDS Practice Papers*, (August 2013).
- Wachter, S. 2018. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review*, 34(3): 436–449.
- Walliman, N. 2011. *Research Methods: The Basics*. Abingdon: Routledge.
- Walliman, N. 2005. *Your research project*. Second. London: Sage Publications.
- Walton, D. 2005. *Abductive Reasoning*. Tuscaloosa, Alabama: The University of Alabama Press.
- Wang, C., Wang, Y., Chen, Y., Liu, H. & Liu, J. 2020. User authentication on mobile devices: Approaches, threats and trends. *Computer Networks*, 170: 107118. <https://doi.org/10.1016/j.comnet.2020.107118>.
- Wang, Chong, Zhang, N. & Wang, Cong. 2021. Managing privacy in the digital economy. *Fundamental Research*, (April).
- Wang, G.T. & Park, K. 2016. *Student Research and Report Writing: From Topic Selection to the Complete Paper*. West Sussex: John Wiley & Sons Ltd.
- Warren, S.D. & Brandeis, L.D. 1890. The Right to Privacy. *The Harvard Law Review Association*, 4(5): 193–220.
- Watson, H., Finn, R.L. & Barnard-Wills, D. 2017. A gap in the market: The conceptualisation of surveillance, security, privacy and trust in public opinion surveys. *Surveillance & Society*, 15(2): 269–285.
- Welman, C., Kruger, S. & Mitchell, B. 2005. *Research Methodology*. Third. A. van Rooyen, ed. Oxford: Oxford University Press.
- Westin, A.F. 1967. *Privacy and Freedom*. New York: Atheneum.
- Westin, A.F. 2003. Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59(2): 1–37.
- Wheelus, C. & Zhu, X. 2020. IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework. *IoT*, 1(2): 259–285.
- Widyasari, Y.D.L., Nugroho, L.E. & Permanasari, A.E. 2018. Persuasiveness web 2.0 in behavioral intention: A conceptual model. *Proceedings - 2017 International Conference on Sustainable Information Engineering and Technology, SIET 2017*, January: 117–122.
- Williams, C. 2007. Research Methods. *Journal of Business & Economic Research*, 5(3): 65–72.
- Williams, L., Rycroft-Malone, J. & Burton, C.R. 2017. Bringing critical realism to nursing practice: Roy Bhaskar's contribution. *Nursing Philosophy*, 18(2): 1–11.
- Willis, J.W. & Edwards, C. eds. 2014. *Action Research: models, methods, and examples*.

Charlotte, North Carolina: Information Age Publishing Inc.

- Woiceshyn, J. & Daellenbach, U. 2018. Evaluating inductive vs deductive research in management studies. *Qualitative Research in Organizations and Management: An International Journal*, 13(2): 183–195.
- World Health Organisation. 2021. Coronavirus disease (COVID-19). <https://www.who.int/>. https://www.who.int/health-topics/coronavirus#tab=tab_1 2 November 2020.
- Wu, Q., He, K. & Chen, X. 2020. Personalized Federated Learning for Intelligent IoT Applications: A Cloud-Edge based Framework. *IEEE Computer Graphics and Applications*, 1(April): 35–44.
- Yaqoob, I., Ahmed, E., Habib, M., Ibrahim, A., Ahmed, A., Al-garadi, M.A., Imran, M. & Guizani, M. 2020. The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, 129(2017): 444–458.
- Yebenes, J. & Zorrilla, M. 2019. Towards a data governance framework for third generation platforms. *Procedia Computer Science*, 151: 614–621.
- Yin, R.K. 2003. *Case Study Research: Design and Methods*. Third. Thousand Oaks, California: Sage Publications, Inc.
- Yin, R.K. 2014. *Case Study Research: Design and Methods*. Fifth. Thousand Oaks, California: Sage Publications, Inc.
- Yin, R.K. 2009. *Case Study Research: Design and Methods*. Fourth. Thousand Oaks, California: Sage Publications Ltd.
- Zaidi, A.Z., Chong, C.Y., Jin, Z., Parthiban, R. & Sadiq, A.S. 2021. Touch-based continuous mobile device authentication: State-of-the-art, challenges and opportunities. *Journal of Network and Computer Applications*, 191(June): 103–162.
- Zarsky, T.Z. 2019. Privacy and Manipulation in the Digital Age. *Theoretical Inquiries in Law*, 20(1): 157–188.
- Zenda, B., Vorster, R. & Da Viegua, A. 2020. Protection of personal information: An experiment involving data value chains and the use of personal information for marketing purposes in South Africa. *South African Computer Journal*, 32(1): 113–132.
- Zheng, X., Cai, Z. & Li, Y. 2018. Data Linkage in Smart Internet of Things Systems: A Consideration from a Privacy Perspective. *IEEE Communications Magazine*, 56(September): 55–61.

APPENDICES

APPENDIX A: ETHICAL CLEARANCE FROM FACULTY OF INFORMATICS AND DESIGN, CPUT



P.O. Box 652 • Cape Town 8000 South Africa • Tel: +27 21 469 1012 • Fax +27 21 469 1002
80 Roeland Street, Vredehoek, Cape Town 8001

Office of the Research Ethics Committee	Faculty of Informatics and Design
---	-----------------------------------

14 May 2020

Ethics approval is granted to Ms Leona Annelise McArdle, student number 193052873, for research activities related to the MTech: Information Technology at the Faculty of Informatics and Design, Cape Peninsula University of Technology (CPUT).

Title of thesis:	Data privacy governance framework for the internet of things in South African organisations
------------------	---

Comments

Data collection permission is required from the relevant institution/s and research activities are restricted to those detailed in the research proposal.

 Signed: Faculty Research Ethics Committee	14 May 2020 Date
--	---------------------

APPENDIX B: RESEARCH PARTICIPATION EMAIL REQUEST

Hello,

My name is Leona McArdle, I am an Information Technology Master's degree student at Cape Peninsula University of Technology. As part of the degree course, each student is required to undertake a research project, inclusive of data collection, and write a thesis on a topic area in a particular field of study in South Africa.

My research project is based on the Internet of Things (IoT) and the aim is to develop a framework of guidelines and best practices for governing data privacy within IoT environments in South Africa.

I am approaching your organisation, which comes highly recommended as one of the forerunners of IoT in South Africa, to secure an interview with knowledgeable persons on the topic area in your organisation.

I would appreciate it if we could arrange a virtual interview at your earliest convenience within the next couple of weeks. It is expected that the interview will range between 30-45 minutes and will focus on aspects of data privacy governance and regulation within IoT environments in South Africa.

Attached is a copy of the research brief with information on the research topic for your perusal. Your consideration and time is greatly appreciated, and I look forward to hearing from you soon.

Thank you in advance.

Kind regards,

Leona McArdle

APPENDIX C: RESEARCH BRIEF

Research Brief

Topic: Data Privacy Governance Framework for The Internet of Things in South African Organisations

Rapid technological advances, intensification of connectivity and society's reliance on technology have triggered a proliferation of data privacy concerns.

The governance of data privacy regulation and compliance for the Internet of Things (IoT) in relation to people, data, processes and things is a cause of concern for individuals and organisations worldwide. The regulation of data privacy and compliance in South Africa remains largely invisible, and despite the advent of the Protection of Personal Information (POPI) Act there continues to be a growing threat of data breaches within connected environments.

Consequently, the lack of active regulation within IoT environments, in relation to data privacy may lead to massive violations of user data and breaches of privacy, with an adverse impact not only on users and organisations, but also the country at large.

Therefore, given the ubiquitous nature of IoT and the participation of South African organisations within the international market, the regulation of data privacy and compliance becomes imperative for South Africa to remain a global contender in technological advances.

Aim of the research:

The aim of this study is to explore the factors for the governance of data privacy regulation and compliance for connected environments, with a view to develop a framework of guidelines and best practices for governing data privacy use within IoT environments in South Africa.

Objectives of the research:

The objectives of the study are as follows:

- To determine the factors affecting data privacy regulation within IoT-based organisations in South Africa.
- To establish awareness of organisations' adherence to data privacy and regulatory laws in the use of data obtained through IoT environments.
- To determine existing best practices for the governance of data privacy within an IoT environment.
- To develop a framework of guidelines for governing data privacy within IoT environments in South Africa.

Data will be collected through semi-structured interviews of the person(s) responsible for privacy compliance (data controllers, data processors, compliance officers, etc.) within IoT-based organisations in South Africa.

Each participant will be required to complete an informed consent form before participation in this study. The research process and objectives will be fully communicated with intended participants and free from pressure or coercion. Participants will be given the opportunity to consent freely or refuse to participate. The confidentiality of research participants will be maintained, and subjects' anonymity will be preserved through the use of pseudonyms. The data collated in the research will be stored on a password-protected USB with the researcher having sole access to the data.

Thanking you in advance for your assistance and cooperation.

Yours sincerely,
Leona McArdle
193052873

APPENDIX D: PARTICIPANT CONSENT FORM



Cape Peninsula
University of Technology

FID/REC/ICv0.1

FACULTY OF INFORMATICS AND DESIGN

Individual Consent for Research Participation

Title of the study: Data privacy governance framework for the Internet of Things in South African Organisations

Name of researcher: Leona McArdle
Contact details: Email: mcardle.leona@gmail.com Phone: +27 (0) 71 117 6576.

Name of supervisor: Mr. Ayodeji Afolayan
Contact details: Email: afolayana@cput.ac.za Phone: +27 (0) 21 464 3836.

Purpose of the Study: The aim of this research is to develop a framework of guidelines and best practices for governing data privacy use within IoT environments in South Africa.

Participation: My participation will consist essentially of interviews.

Confidentiality: I have received assurance from the researcher that the information I will share will remain strictly confidential unless noted below. I understand that the contents will be used only for the purpose of developing a framework of guidelines and best practices for governing data privacy use within IoT environments in South Africa and that my confidentiality will be protected using pseudonyms.

Anonymity: The subjects of this research will remain nameless, and responses will not be linked back to them. Photo and video usage are highly unlikely, but in the event of this occurring, the faces of the participants will be blacked out.

Conservation of data: The researcher will employ steps such as utilising a password-protected recording and storage devices to ensure that subjects' personal information is kept confidential and limiting the risk of exposing participants identities. The recordings will be preserved purely for audit purposes and only the investigator will be able to decrypt the storage locations of the data.

Voluntary Participation: I am under no obligation to participate and if I choose to participate, I can withdraw from the study at any time and/or refuse to answer any questions, without suffering any negative consequences. If I choose to withdraw, all data gathered until the time of withdrawal will be destroyed.

Additional consent: I make the following stipulations (please tick as appropriate):

	In thesis	In research publications	Both	Neither
My image may be used:				
My name may be used:				
My exact words may be used:				
Any other (stipulate):				

Acceptance: I, (print name) _____

agree to participate in the above research study conducted by Leona McArdle of the Faculty of Informatics and Design at the Cape Peninsula University of Technology, which research is under the supervision of Mr. Ayodeji Afolayan.

If I have any questions about the study, I may contact the researcher or the supervisor. If I have any questions regarding the ethical conduct of this study, I may contact the secretary of the Faculty Research Ethics Committee at +27 (0)21 469 1012, or email: naidoove@cput.ac.za.

Participant's signature: _____

Date: _____

Researcher's signature:



Date: 15/04/2021

APPENDIX E: INTERVIEW SCHEDULE

DATA PRIVACY GOVERNANCE FRAMEWORK FOR THE INTERNET OF THINGS IN SOUTH AFRICAN ORGANISATIONS

INTERVIEW SCHEDULE

Opening:

Rapid technological advances, intensification of connectivity and society's reliance on technology have triggered a proliferation of data privacy concerns. The governance of data privacy regulation and compliance for the Internet of Things (IoT) in relation to people, data, processes and things is a cause of concern for individuals and organisations worldwide. The regulation of data privacy and compliance in South Africa remains largely invisible, and despite the advent of the Protection of Personal Information (POPI) Act there continues to be a growing threat of data breaches within IoT environments.

Consequently, the lack of active regulation within IoT environments, in relation to data privacy may lead to massive violations of user data and breaches of privacy, with an adverse impact not only on users and organisations, but also the country at large. Therefore, given the ubiquitous nature of IoT and the participation of South African organisations within the international market, the regulation of data privacy and compliance becomes imperative for South Africa to remain a global contender in technological advances.

Aim of the research:

The aim of this study is to explore the factors for the governance of data privacy regulation and compliance for connected environments, with a view to develop a framework of guidelines and best practices for governing data privacy use within IoT environments in South Africa.

We are kindly requesting answers to the questions listed below in your good faith. Your answers will be used specifically for this study purposes only and they will be treated with the highest degree of confidentiality and privacy. Also, participation in this interview is voluntary and allows anonymity as well as autonomy.

Section A: Participant's Details

Name: _____	Date: _____
Surname: _____	Email: _____
Position: _____	Contact No: _____

Section B: Company Information

Q.1 Where is your organisation based?
Comments:
Q.2 Do you have offices located in other provinces, cities or countries?
Comments:
Q.3 What is the size of organisation?
Comments:
Q.4 How long have your organisation been in operation?
Comments:
Q.5 What is your role and responsibilities in the organisation?
Comments:
Q.6 How would you describe your organisation's role in terms of facilitating the application/utilisation of IoT in SA?
Comments:

Section C: Interview Questions

Research Problem Statement	There is no defined holistic framework of best practices and guidelines for the governance of data privacy within IoT environments in South Africa.
Q.1 How would you describe the current situation of data breaches affecting South African organisations? Possible follow-up: What do you believe are the reasons behind (increased) the number of data breaches in South African organisations?	
Comments:	
Q.2 Can you describe the difficulties IoT-based organisations face in terms of the protection of data privacy? Possible follow-up: What processes does your organisation have in place to manage these difficulties?	
Comments:	
Q.3 As an IoT-based organisation, what are the types of data privacy infringements your organisation has experienced? Possible follow-up: What type of exposures are you safeguarding against? How do you mitigate against these types of threats to data privacy?	
Comments:	
Q.4 Can you share your knowledge of South African data privacy and regulatory laws? Possible follow-up: What is your opinion of the current situation surrounding the implementation of the POPI Act?	
Comments:	
Q.5 How well do you think the POPI Act addresses the uniqueness of managing data within IoT environments? Possible follow-up: What needs to be done to address this situation effectively?	
Comments:	
Q.6 What does the POPI Act mean to your organisation? Possible follow-up: How has the POPI Act impacted data privacy and compliance in your organisation?	
Comments:	
Q.7 You may be aware, the deadline for POPI Act compliance was the 1st of July 2021, what mechanisms/protocols have your organisation put in place to fulfil the requirements set out by the Act?	
Comments:	

Q.8 What is your knowledge of the evolving nature of data privacy regulation and laws globally? Possible follow-up: How would you describe the data privacy regulations set out in the POPI Act in comparison to international data privacy laws?
Comments:
Q.9 How do these data privacy regulations and laws inform the management of data, specifically those obtained through IoT environments?
Comments:
Q.10 Given the universal nature and the amount of data generated by connected devices, how can organisations facilitate the protection of personal information? (in an ideal world)
Comments:
Q.11 What are the challenges / complexities surrounding the protection of personal information within IoT environments?
Comments:
Q.12 Can you describe the protocols that guide the protection and use of personal information within IoT environments in your organisation?
Comments:
Q.13 Can you share a situation you have experienced or know of where there was unauthorised access and use of personal data?
Comments:
Q.13b What measures were applied or could have been applied to mitigate and resolve such a situation?
Comments:
Q.14 In your opinion, how does data privacy and protection differ between IoT environments and conventional systems?
Comments:
Q.15 And lastly, how would you suggest organisations operating within IoT environments go about ensuring compliance for data privacy and regulatory laws?
Comments:

APPENDIX F: SAMPLE INTERVIEW TRANSCRIPT

Researcher

Great stuff. And so, I do know from speaking to [REDACTED] you're not an IoT based organization as such. So, can you maybe explain what your organization does, per se?

Participant 15

Yes, sure. So, our organisation is an organisation which develops specific risk management software to disrupt, audit, traditional audit, and do continuous risk assessment in the cyber and IT, audit space. And naturally, with the world we're living in, with all the connectivity that we have, and we find, as we connect more and more to IoT, and the sort of industrial devices and things that we use in our everyday life, it's become necessary for us to consider all the risks that attach to the IoT parts of the networks. So, we're very involved with IoT.

Researcher

Okay, great answer. All right. So that is all the questions for your organisation. And I'm going to move on to the interview questions now. So, first question, how would you describe the current situation of data breaches affecting South African organizations?

Participant 15

I would describe it as a very huge concern given that we understand the level of, because we in the business of risk management, and we work every day with understanding executives' knowledge about the sensitivity of their data, and the ease of hacking. We're very concerned about the current situation and we know, one more complicating factor is the lack of professional skills as CSOs [chief security officers] to manage this particular issue, and so we only see it getting worse. In fact, we're heading one of these days for one of the biggest sort of attacks you're ever going to see. And it will involve IoT that I'm very interested in your research.

Researcher

Okay, thank you. That was a very good answer. Thank you so much for that. And then can you describe the difficulties IoT based organizations face in terms of the protection of data privacy?

Participant 15

Sure. IoT is relatively new technology, it's evolving each day. And the ability of organisations to understand the sensitivity of it complicates the obtaining of budget. So what we're finding is businesses are unable to procure enough budget to protect it and then this challenge is even more complex because there's no skills. So, there's a lack of skills complicated with the lack of budget, and that leads to disaster situation.

Researcher

Good stuff. And what are some of the types of data infringements that your organisation may have experienced?

Participant 15

We've seen total ransom of large databases. I've personally had experience with the ransom of drawings on a CAD/CAM system. I've had experience with, if you call a photoplotter, an IoT device, I've

seen corruption of the drivers of an IoT device and then a demand for a ransom to give them back, I've been involved with Stuxnet [malware]. I've seen machinery, the drivers being corrupted. So on any machine, you've got to think, or the PLC is a programmable logic controller. I've seen the Stuxnet virus attack a brick- and-tile making machine through the Siemens PLCs. So I've had a lot of experience in data being stolen through interfaces with IoT, but I've also seen IoT devices being corrupted.

Researcher

Okay, and how do you mitigate against these types of threats to data privacy?

Participant 15

Focus, focused cyber risk assessments on a continuous basis. Organisations have to be aware that each day, new malware is being developed and without doing continuous, ongoing cyber risk assessments, you can never mitigate against it. It starts with a very interesting problem, which I've studied, and I've done a lot of research. To develop a piece of malware, you need a hacker sitting in a coffee shop anywhere in the world. It costs him nothing, but a cup of coffee here and there, and a laptop and a little bit of good programming and coding skills. To defend against that you need huge budget. So it's an equal equation, you can't defend at a limited cost. And so this is why we're going to see this thing growing exponentially. The rate of attacks is going to grow exponentially as we move to more automated systems.

Researcher

Definitely, I think I agree with you on that. Thank you for that. So, question number four, can you share your knowledge of South African data privacy and regulatory laws?

Participant 15

When you say my knowledge, do you understand POPIA? So, I have a very good understanding of POPIA, I have a very good understanding of GDPR, I have a very good understanding of HIPAA and all the privacy sort of legislation that operates across the countries where we work.

Researcher

Okay, that's great. I'll get to the international side of it. So, what is your opinion on the current situation surrounding the implementation of the POPI Act?

Participant 15

So, I think personally, a lot of big organisations have taken it very seriously. But I personally, don't believe that government has any clue on how to implement and manage POPIA. They're very good at passing legislation, they're very weak at policing. So, you can already see by the fact that the portal that they've developed to register Information Officers doesn't even work.

Researcher

Okay, I don't know that.

Participant 15

I think, yeah, that's a fact. They've already had to change certain timelines for implementation and appointment of IOs. They don't have the skills to police the POPIA legislation.

Researcher

Thank you for that. And how well do you think the POPI Act addresses the uniqueness of managing data within IoT environments?

Participant 15

Well, it doesn't address the management of data in IoT. The people who drafted POPIA never even heard of IoT, don't even know what IoT is. So nowhere in POPIA, does it really address IoT.

Researcher

Brilliant, and what needs to be done to address this situation effectively?

Participant 15

You need to use skilled, specialised people in the implementation and the rollout of POPIA from a regulators point of view. But the regulator is basing it only on a legal basis. So, they don't have technically qualified people looking at the rollout of POPIA, it's merely done as another piece of legislation, and it will be a failure. It's also in my opinion, it's also just another piece of legislation where they can levy some punitive fines.

Researcher

I'm smiling, I'm not going to get into that, because we don't want to go there, but thank you for that.

Participant 15

That is the, I'm being honest with you.

Researcher

No, I totally agree with you. Alright, so I'm going to move on to my next question. What does the POPI Act mean to your organization?

Participant 15

Well, the POPI Act to our organisations mean a revenue stream basically, we're spending a lot of time with clients, helping them develop the processes and procedures to make sure they're compliant. So we've jumped, I could say, you could think of it like this, we've jumped on the bandwagon, we've developed software to make sure that there's compliance and we've built ourselves a little business out of it.

Researcher

Okay, great stuff there. And what mechanisms or protocols have your organization put in place to fulfil the requirements set out by the Act?

Participant 15

We've done full automated assessments, and we continue to do the assessments on an ongoing basis in our organisation. So, we practice what we preach. We've made sure that all our data is very secure. And we're safe and free from any fines or penalties that could be levied if we did have a breach, but we do that just out of good governance anyway, we didn't need POPIA to tell us to do that we're experts in governance, and so we know that it's the right thing to do.

Researcher

Okay, brilliant. Yeah, I've had the same, almost similar answers to what you just said there with regards to the POPI Act and what it meant for some patients. So yeah, that's great. Okay, so we've already established that you have some knowledge of global data privacy regulations and laws. How would you describe the data privacy regulations set out in the POPI Act in comparison to international data privacy laws?

Participant 15

I think very, very similar. If you look closely at the GDPR and you look at POPIA, you'll see that I've actually taken a lot of the GDPR legislation and just fine tuned it for South African use. So that's a cut and paste on GDPR, that's my view.

Researcher

Okay, brilliant. And how do these data privacy regulations and laws inform the management of data, specifically, those obtained through IoT environments?

Participant 15

Well, the data that's obtained through IoT environments actually ends up sitting on a database somewhere, and management know that they have to protect that piece of data, or the databases wherever they are. So, it doesn't matter where you collect the data from, management should be aware, and I'm not convinced they are, that they have to have adequate protection of the data. Whether it's collected from IoT, or it's collected manually, actually doesn't make any difference to POPIA or to GDPR.

Researcher

Okay, we've just discussed the universal nature and the amount of data being generated by the connected devices, how can organisations facilitate the protection of personal information in an ideal world?

Participant 15

In an ideal world, they should be doing ongoing continuous assessment of the data, they should be reviewing their controls, and their control environment almost on a continuous basis. And if they don't do that, there's no way they can control the data because the hackers are out there, the malware is becoming more and more sophisticated. And that's the real existence of our business, we decided that and I was a partner and...

Researcher

Hello, [name withheld], I seem to have lost you. Can you hear me? Hello? Hello.

APPENDIX G: SAMPLE OF ATLAS.TI TRANSCRIPTS AND CODES FOR INTERVIEW ANALYSIS

Project: MTech 2021

Report created by Leona McArdle on 09/12/2021

Code Report

All (77) codes

● comp: establishing compliance of data privacy and regulatory laws

28 Quotations:

5:69 ¶ 153, IQ15_Response in Participant 2

the first thing would be to chat to someone that he has knowledge of things like PoPI Act to start there. So an attorney or law firm, and understand at least on that level. And then you need to ensure that your service providers are compliant as well.

6:32 ¶ 85, IQ7_Response in Participant 3

what they went and did was to combat this was they went to set up their own service, that would allow us to pass our information through them, they would keep a PoPI compliant data retention copy of the data. And we would only work on data then copied from that database to us. So they took care of the PoPI compliance, and the security thereof,

6:33 ¶ 79, IQ7_Response in Participant 3

we actually teamed up with a, I don't know if you know, a company

6:37 ¶ 157, IQ15_Response in Participant 3

a lot of it can be addressed beforehand. So doing a bit of brainstorming on all the different angles on a system. Most of that can be engineered out or planned out of the roll out of the project

6:38 ¶ 157, IQ15_Response in Participant 3

make it very transparent to the end customer as to where the liabilities are, and what the possible outcomes can be of the data coming out in the field

7:63 ¶ 228, IQ15_Response in Participant 8

I think they first have to actually understand what the laws are, and who benefits from it and who doesn't benefit from it.

7:64 ¶ 228, IQ15_Response in Participant 8

There needs to be more education around what the actual Act is, and what you're allowed to and what you're not allowed to do.

8:58 ¶ 214, IQ15_Response in Participant 1

I would definitely say a community approach to this where it is community defined or industry defined and deployed - defined, agreed and deployed.

9:49 ¶ 282, IQ15_Response in Participant 4

know exactly what the laws are through a hired company or Information Officers or both. And then that's obviously you do what they tell you to do.

11:35 ¶ 193, IQ15_Response in Participant 7

from a privacy point of view, I think it's a question of protecting the data as such, in order for the data not to be used for malevolent purposes

11:36 ¶ 193, IQ15_Response in Participant 7

get a [obscene language] good consult! Because I think ultimately if you don't understand digitalization, invariably you're going to fall into a trap because you have to anticipate in every step what is going to happen, which data is used and you need to really anticipate going forward that the data will need to be utilized, and then deployed as intelligence.

12:73 ¶ 333, IQ15_Response in Participant 5

the system must have like 256 encryption or work through a VPN tunnel.

12:74 ¶ 333, IQ15_Response in Participant 5

encryption at rest, encryption in motion, it must have those basic things in place, the system must be protected with a firewall. You must have intrusion detection

12:75 ¶ 333, IQ15_Response in Participant 5

check if your systems are secure, and try and meet the compliance of security, you would have to test the systems, you would have to probably hire penetration experts like white hat hackers, you know, to test and probe that system to see.

13:48 ¶ 176, IQ15_Response in Participant 9

audits not only in terms of post hoc audits, looking at existing service systems, but also, when designing systems actually have that as one of the primary design criteria.

13:56 ¶ 182, IQ15_Response in Participant 9

Never build your own security system, use one that is already existing, that was built by somebody whose business it is to do security.

14:21 ¶ 373, IQ15_Response in Participant 10

I don't know to be perfectly honest. All I can say there needs to be a framework

15:51 ¶ 237, IQ15_Response in Participant 11

get good advice from third parties or advisors

15:52 ¶ 237, IQ15_Response in Participant 11

We also utilise companies to regularly, well not regularly, twice a year audit us to determine what we doing on a compliance basis is correct or sufficient.

15:53 ¶ 237, IQ15_Response in Participant 11

next part is really talking to openly to customer about the risk and how they'd like to manage that risk rather than enforcing it upon them

15:54 ¶ 237, IQ15_Response in Participant 11

becomes a bespoke solution rather than a forced solution.

16:50 ¶ 158, IQ15_Response in Participant 12

they just have to apply the same systematic methodology for seeking to protect every endpoint in the network. So the IoT devices are considered endpoints and those endpoints, the controls around every endpoint, security must be considered and reviewed

34:66 ¶ 210, IQ15_Response in Participant 13

first is you have to make sure your privacy policies are legally sound and reviewed, and compliant. I think there's a second aspect to this, which is around the human behaviour and the physical access to the data. And that's where you need security protocols around who accesses, how do they access, what access to they have and so forth. And if somebody leaves, how do you lock access? And so, there's got to be policies and procedures around that. And lastly, I think it's about testing compliance continuously

34:67 ¶ 210, IQ15_Response in Participant 13

it's monitoring that access to that data, and red flagging unauthorized access or unusual access at unusual times

35:58 ¶ 168, IQ15_Response in Participant 14

Well for now think we've got the POPI Act and that sort of is the governing Act that we need to stick by and it's to keep having a look at that Act and making sure that it's kept up to date and that we are kept abreast of it and companies all protect, make sure that data, both the company data and the personal data is protected of the customers

36:68 ¶ 228, IQ15_Response in Participant 15

They need to employ suitably qualified specialists. And if I can't employ them, then I need to outsource the protection to businesses that can do the protection based on continuous assessment.

36:69 ¶ 234, IQ15_Response in Participant 15

Consulting businesses, who have the skills and the know-how to do it

36:70 ¶ 234, IQ15_Response in Participant 15

they must ensure that their code is suitably protected and that there are no backdoors and weaknesses in the code and that means having proper software companies do code reviews to make sure that the programmers who built the code haven't built-in some backdoor weakness areas.

● **comp: GDPR compliance**

4 Quotations:

5:50 ¶ 84, IQ8_Response in Participant 2

As far as our core products is concerned, we are in, I think a fortunate position in that we adopt or the data flow is actually done by Sigfox and they are already GDPR compliant.

8:42 ¶ 130, IQ8_Response in Participant 1

we've always been following GDPR as a global standard because we've got global customers.

12:46 ¶ 157, IQ8_Response in Participant 5

GDPR now, if we're interacting with any European company we have to look at that.

34:48 ¶ 132, IQ7_Response in Participant 13

all of our policies, privacy policies, our end-user terms and conditions, our commercial terms and conditions are really centered around GDPR compliance as opposed to POPIA.

● **comp: regulatory processes adopted from parent company**

1 Quotations:

5:54 ¶ 90, IQ7_Response in Participant 2

even though we are small company, and we've adopted the processes and mature regulations of a much larger organization that has much more intense oversight.

● **comp: SA data privacy compliance**

APPENDIX H: SAMPLE OF ATLAS.TI TRANSCRIPTS AND CODES FOR DOCUMENT ANALYSIS

Project: MTech2021_DocumentAnalysis

Report created by Leona McArdle on 09/12/2021

Code Report

All (378) codes

○ access: denial of

1 Quotations:

8:22 p 12 in Data-Protection-BVI

16. (1) A public body or a private body is not obliged to comply with a request for access to personal data (a) unless it is supplied with such information as it may reasonably require in order to satisfy itself as to the identity of the person making the request and to locate the personal data which that person seeks; (b) if compliance with the request will be in contravention of the exemptions contained in Part IV or of any duty of confidentiality recognised by law; (c) where another person who can be identified from the personal data consents to the disclosure of his or her personal data to the person making the request; or (d) where the body obtains the written approval of the Information Commissioner.

○ access: form of

1 Quotations:

8:23 p 12 in Data-Protection-BVI

17. (1) Where a data subject is to be given access to personal data requested pursuant to section 14, the public body or private body shall (a) permit the data subject to examine the personal data; or (b) provide the data subject with a copy of the personal data.

○ activities prohibited

1 Quotations:

6:72 p 59, Article 59 (Prohibited Activities) in Data-Protection-SouthKorea

Anyone who processes or has processed personal information shall be prohibited from undertaking any of the following activities: 1. To acquire personal information or to

obtain consent to personal information processing by fraud, improper or unjust means; 2. To divulge personal information acquired in the course of business, or to provide it for any third party's use without authority; 3. To damage, destroy, alter, forge, or divulge other's personal information without legal authority or beyond proper authority.

○ **agency: access to id info**

1 Quotations:

5:29 p 103 in Data-Protection-NewZealand

An accessing agency may, for the purpose specified in the second column of Schedule 3 opposite the name of the accessing agency, have access to an individual's identity information held by a holder agency specified in the third column of that schedule opposite the name of the accessing agency.

○ **agency: refusal of access**

1 Quotations:

5:16 p 41, 46 Decision to refuse access to personal information in Data-Protection-NewZealand

(1) An agency may refuse access to the personal information requested, or some of the personal information requested, only if the agency is able to rely on any of sections 49 to 53 (see also section 24).

○ **application**

3 Quotations:

10:22 p 9 in Data-Protection-Kenya

4. This Act applies to the processing of personal data (a) entered in a record, by or for a data controller or processor, by making use of automated or non-automated means: Provided that when the recorded personal data is processed by non-automated means, it forms a whole or part of a filing system; (b) by a data controller or data processor who — (i) is established or ordinarily resident in Kenya and processes personal data while in Kenya; or (ii) not established or ordinarily resident in Kenya, but processing personal data of data subjects located in Kenya.

13:2 p 11 in Data-Protection-South Africa

(a) entered in a record by or for a responsible party by making use of automated or non-automated means: Provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof; and (b) where the responsible party is— (i) domiciled in the Republic; or (ii) not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.

13:3 p 9 in Data-Protection-South Africa

3. (1) This Act applies to the processing of personal information—

○ certification

1 Quotations:

1:137 p 58, Article 42: Certification in Data-Protection-GDPR

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors.

The specific needs of micro, small and medium-sized enterprises shall be taken into account.

○ certification bodies: accreditation

1 Quotations:

1:141 p 60 in Data-Protection-GDPR

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

○ certification bodies: responsibilities

1 Quotations:

1:142 p 60 in Data-Protection-GDPR

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

○ code of conduct

3 Quotations:

1:131 p 56, Article 40: Codes of Conduct in Data-Protection-GDPR

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

1:132 pp 56 – 57, Article 40: Codes of Conduct in Data-Protection-GDPR

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to: (a) fair and transparent processing; L 119/56 EN Official Journal of the European Union 4.5.2016

(b) the legitimate interests pursued by controllers in specific contexts; (c) the collection of personal data; (d) the pseudonymisation of personal data; (e) the information provided to the public and to data subjects; (f) the exercise of the rights of data subjects; (g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained; (h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32; (i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects; (j) the transfer of personal data to third countries or international organisations; or (k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3:69 pp 21 – 22, Art.41 (Codes of conduct) in Data-Protection-SanMarino

1. Associations and other bodies representing categories of controllers or processors may prepare or amend or extend codes of conduct, taking account of the specific features of the various

APPENDIX I: SAMPLE OF FULL CODING TABLE IN MS EXCEL

FullCodingTable_Interviews_201021							Search (Alt+Q)		Leona McArdle			
File	Home	Insert	Draw	Page Layout	Formulas	Data	Review	View	Help	Comments	Share	
Undo	Paste	Clipboard	Font	Alignment	Number	Styles	Cells	Editing	Analysis			
H291												
1	Interview Question (IQ)	Participant	Response	Comment	Codes	Categories	Themes					
509	IQ3_Response	Participant 11	Luckily, to date, none		infringements experienced by organisation	Knowledge of Infringements	DATA PRIVACY					
510	IQ3_Follow-up Q_Response	Participant 11	the corruption of the data and a third party collecting that data		types of vulnerabilities to safeguard	Threats to Personal Information	DATA PRIVACY					
511	IQ4_Response	Participant 11	It's very sketchy. The part I know of which recently is so well published is the POPI Act.		knowledge of SA data privacy regulation	Protection of Personal Information	REGULATION					
512	IQ6_Response	Participant 11	we don't assimilate the data, we collect it, it goes to the server farm and sent to the customer. So there's no storage of that data in any formal way in our business.		impact of PoPI on organisation	Regulation of Personal Information	REGULATION					
513	IQ5_Response	Participant 11	I don't have an in-depth knowledge of that at all.		organisations lack understanding and knowledge	System Vulnerabilities	DATA SECURITY					
514	IQ6_Follow-up Q_Response	Participant 11	Not at all because our third-party supplier is covering that for us. Yeah, it hasn't really affected us at all		Impact of PoPI on organisation	Regulation of Personal Information	REGULATION					
515	IQ6_Follow-up Q_Response	Participant 11	we've done very little additional security or additional steps since it's promulgated.		impact of PoPI on organisation	Regulation of Personal Information	REGULATION					
516	IQ8_Response	Participant 14	I don't have much knowledge on that account		opinion of global data privacy regulation	Knowledge of Regulations	REGULATION					
517	IQ9_Response	Participant 11	I said I have no idea. No, in fact I haven't even given it the slightest thought at all.		regulation and data management in IoT	Data Governance & IoT	INTERNET OF THINGS (IOT)					
518	IQ10_Response	Participant 14	we keep our servers out of South Africa, on a server farm in Europe and it's got extremely high level of security		approach for safeguarding personal information	Protecting Personal Information	DATA PRIVACY					
519	IQ10_Response	Participant 14	ensure that one's websites are secure, and passwords are secure, and to ensure that the clients if they are having to login to the website, is to ensure that they change it every 30 days.		approach for safeguarding personal information	Protecting Personal Information	DATA PRIVACY					
	IQ11_Response	Participant 15	The nature of the complex environment in which data sits is becoming more and more complex by the day, it's becoming more and more accessible to the attack vectors that we see being used. The world is becoming more and more interconnected. So we live		challenges of safeguarding personal information	Challenges of Securing Personal	DATA PRIVACY					
	THEMES	ALL CODES	DATA PRIVACY	REGULATION	DATA SECURITY	INTERNET OF THINGS	PROFILE	Info ...				

AutoSave Off FullCodingTable_Interviews_201021 Search (Alt+Q) Leona McArdle

File Home Insert Draw Page Layout Formulas Data Review View Help

Undo Clipboard Font Alignment Number Styles Cells Editing Analysis

H291

	A	B	C	D	E	F	G	H	I
1	Interview Question (IQ)	Participant	Response	Comment	Codes	Categories	Themes		
536	IQ1_Response	Participant 15	We're very concerned about the current situation		upsurge in data breaches	Data Breaches	DATA PRIVACY		
	IQ2_Response	Participant 12	I think the greatest challenge is the lack of maybe knowledge of not quite knowing the extent to which the IoT environment makes the organization more vulnerable. So I think it's being uninformed.		organisations lack understanding and knowledge	System Vulnerabilities	DATA SECURITY		
537	IQ11_Response	Participant 15	As military is developing, so are the skills for, let's call them the bad threat actors and so your complexities, as I mentioned, or you end up with threats from actors which have serious training and have huge capability at low cost		challenges of safeguarding personal information	Challenges of Securing Personal Information	DATA PRIVACY		
538	IQ11_Response	Participant 15	IoT is relatively new technology, it's evolving each day. And the ability of organisations to understand the sensitivity of it complicates the obtaining of budget. So what we're finding is businesses are unable to procure enough budget to protect it		cost challenge	Challenges of Securing Personal Information	DATA PRIVACY		
539	IQ4_Response	Participant 12	we have the POPI Act that has been promulgated and implemented		knowledge of SA data privacy regulation	Protection of Personal Information	REGULATION		
540	IQ4_Follow-up Q_Response	Participant 12	the biggest problem facing the Regulator right now is the volume of reports that are flooding in, of breaches of the Act. So I think the Regulator's completely overwhelmed just in terms of the volume. And I think that's become a weakness and hence there is the continued disregard of privacy policies.		opinion of PoPI	Knowledge of Regulations	REGULATION		
541	IQ13_Response	Participant 12	one sees it just in terms of scam calls and emails that just are unabated		personal experience of infringements	Knowledge of Infringements	DATA PRIVACY		
542	IQ5_Response	Participant 12	I think it addresses it sufficiently		PoPI and IoT	Data Governance & IoT	INTERNET OF THINGS (IOT)		
543	IQ4_Follow-up Q_Response	Participant 12	the issue with policies, procedures, mandatory requirements or acts is more the sanction that should be following the contravention of the Act. And so the weakness is not so much in the Act as much as in the ability to impose sanction and to prosecute. So there's the prosecution side and the legal side of prosecution that is most probably the weakness, not so much the Act itself		opinion of PoPI	Knowledge of Regulations	REGULATION		

THEMES ALL CODES DATA PRIVACY REGULATION DATA SECURITY INTERNET OF THINGS PROFILE Info ...

Ready

AutoSave Off FullCodingTable_Interviews_201021 Search (Alt+Q) Leona McArdle

File Home Insert Draw Page Layout Formulas Data Review View Help

Clipboard Font Alignment Number Styles Cells Editing Analysis

H291

	A	B	C	D	E	F	G	H	I
	Interview Question (IQ)	Participant	Response	Comment	Codes	Categories	Themes		
1	IQ9_Response	Participant 6	we've had business opportunities in the EU, but because of GDPR, we would need servers running in the EU, actually, and what that would mean for us is moving our infrastructure or duplicating it.		impact of global regulations	Regulation of Personal Information	REGULATION		
470	IQ9_Response	Participant 8	It informs me to make a better decision based on the data I get in, you know, it's an informed decision		regulation and data management in IoT	Data Governance & IoT	INTERNET OF THINGS (IOT)		
471	IQ9_Response	Participant 9	one of our clients required their data to be hosted physically in Europe, which was not a technical requirement, but a regulatory requirement		regulation and data management in IoT	Data Governance & IoT	INTERNET OF THINGS (IOT)		
472	IQ9_Response	Participant 9	one specific client because of the regulations in Europe, required that the data was stored on a server in Europe, which was a bit of a unique requirement. There was no real technical reason for that other than our clients interpretation of their data laws, stating that was a requirement.		impact of global regulations	Regulation of Personal Information	REGULATION		
473	IQ9_Response	Participant 13	most telemetry data is not considered personal information. It's only when the telemetry data is matched to personal information, that you have to be more vigilant and so forth. So, I think from a management perspective, we take it serious, but there's no real personal information that we're receiving from our IoT devices.		regulation and data management in IoT	Data Governance & IoT	INTERNET OF THINGS (IOT)		
474	IQ9_Response	Participant 13	When a client gives us personal information, we have to protect that personal information		regulation and data management in IoT	Data Governance & IoT	INTERNET OF THINGS (IOT)		
475	IQ9_Response	Participant 15	So it doesn't matter where you collect the data from		regulation and data management in IoT	Data Governance & IoT	INTERNET OF THINGS (IOT)		
476	IQ9_Response	Participant 15	Whether it's collected from IoT, or it's collected manually, actually doesn't make any difference to POPIA or to GDPR.		regulation and data management in IoT	Data Governance & IoT	INTERNET OF THINGS (IOT)		
477	Nerospec is actually a holding company and Nerospec IoT is one of the...	Participant 3	[Company name withheld] is actually a holding company and [Company name withheld] is one of the sub-verticals. We all come from a history of mining technologies, where we the underground telematics and communication for the mining industry. Said that		organisation experience and background	Organisation Profile	PROFILE		

THEMES ALL CODES DATA PRIVACY REGULATION DATA SECURITY INTERNET OF THINGS PROFILE Info ...

Ready 100%

APPENDIX J: PROOFREADING CERTIFICATE

FELICITY KAREN TITUS

B.A (Afrikaans-Nederlands and Psychology); B.Ed; M.Ed

Language editing and bibliographic citation

DECLARATION OF EDITING

2 Jolton Street

Nooiensfontein

Kuils River

7580

0796950577

felicitykarentitus0@gmail.com

The Master of Technology thesis by **Leona Annelise McArdle**, titled 'Data privacy governance framework for the Internet of Things in South African organizations' has been edited, the references have been checked for correctness and formatted according to the CPUT Harvard bibliographic referencing style guide, all in-text citations have been checked against the references, and the all items in the reference list have been checked against the text. The candidate has been advised to make the recommended changes.



Felicity Titus

8 December 2021

APPENDIX K: TURNITIN REPORT

DATA PRIVACY GOVERNANCE FRAMEWORK FOR THE INTERNET OF THINGS IN SOUTH AFRICAN ORGANISATIONS

by Leona Annelise McArdle 193052873

Submission date: 08-Dec-2021 07:47AM (UTC+0200)

Submission ID: 1721064897

File name: ALL_CHAPTERS_Turnitin_07122021a.docx (9.86M)

Word count: 83648

Character count: 488668

DATA PRIVACY GOVERNANCE FRAMEWORK FOR THE INTERNET OF THINGS IN SOUTH AFRICAN ORGANISATIONS

ORIGINALITY REPORT

9%	8%	4%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	repository.up.ac.za Internet Source	1%
2	researchspace.ukzn.ac.za Internet Source	<1%
3	uir.unisa.ac.za Internet Source	<1%
4	etd.cput.ac.za Internet Source	<1%
5	www.jonesday.com Internet Source	<1%
6	salawreform.justice.gov.za Internet Source	<1%
7	hdl.handle.net Internet Source	<1%
8	www.dataguidance.com Internet Source	<1%
9	"Data Protection in the Internet", Springer Science and Business Media LLC, 2020	<1%

Exclude quotes On
Exclude bibliography On

Exclude matches < 4 words