DATA PRIVACY, SECURITY AND TRUST IN "CONSUMER INTERNET OF THINGS" ASSEMBLAGES AND ASSOCIATED MOBILE APPLICATIONS IN SOUTH AFRICA

by

MFANASIBILI NGWENYA

Student number: 36092444

submitted in partial fulfilment of the requirements for the degree of

DOCTOR OF PHILOSOPHY
IN
INFORMATION SCIENCE

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF M NGOEPE

January 2020

ABSTRACT

The Internet of Things (IoT) brings with it opportunities and challenges. IoT technology makes it possible to connect all of a person's devices to create a smart eco-system or assemblage. Various stakeholders share personal data with companies in the consumer IoT space for marketing, tracking and assessment of the IoT products. In a world where cybercriminals have increased enormously, people need to be aware of the advantages, and the risks that come with these technological advances. The purpose of this study was to explore the data privacy**,** security and trust issues faced by consumers of IoT in South Africa, to propose an integrated and holistic framework that promotes safer adoption of consumer Internet of Things (CIoT). The researcher explained the difference between Industrial IoT (IIoT) and consumer CIoT in the study and focused the research on the latter. This study utilized a qualitative narrative inquiry and Delphi technique to explore the challenges that come with CIoT assemblages and associated mobile applications in South Africa. The researcher's original contribution was to develop a holistic framework that all stakeholders may use to protect consumers of IoT. The proposed framework addresses the challenges of CIoT from a legal, technical and social context viewpoint. The study looked at legal instruments around the world and compared them to the South African existing legal instruments. The researcher established that South Africa has various pieces of legislation such as the Protection of Personal Information Act 4 of 2013, the Consumer Protection Act 68 of 2008, the Electronic Communications Act 36 of 2005, and the Electronic Communications and Transactions Act 25 of 2002, that law enforcers may use to deal with the challenges IoT. However, the researcher ascertained that these laws do not necessarily address IoT specifically as they are; in fact, they are either outdated or fragmented. In addition to the background literature, the research sought expert opinions to address the technical viewpoints of the CIoT assemblage. The technical approach looked at the existing technologies, design and development considerations, and the overall architecture of CIoT. The researcher generated theme and sub-themes using thematic analysis. There main themes were regarding regulatory frameworks, privacy of personal information, security concerns, trust issues, and convenience

and benefits. The study further established that consumers enjoy the convenience and benefits that IoT technology brings. The study suggested an integrated and holistic framework that promote safer adoption of CIoT and associated mobile apps. The conclusion is that for CIoT to thrive, safety is crucial, and all the stakeholders in the IoT assemblage need to ensure the protection of consumers. The suggested framework may assist in the protection of consumers of IoT. The researcher recommends a further study that covers the regulators such as ICASA in detail and the enforcement of the POPI Act.

Keywords: data security, privacy, trust, personal information, consumer internet of things, internet of things, mobile apps, legal instruments, South Africa

ACKNOWLEDGEMENT

This study was possible with the help of my supervisor, Prof. Mpho Ngoepe. His experience, immense knowledge, drive for quality and excellence have helped me complete this study. My sincere gratitude goes to him for trusting in my abilities, motivating me, being patient with me and guiding me throughout the study.

Moreover, thanks to my wife, Boitumelo Ngwenya, for trusting and being patient with me. Thanks for understanding that sometimes I needed to be excused from family matters to push the study to completion. To the participants of this study, I salute you for the information provided. Finally, I am forever grateful to my siblings, friends and work colleagues who continuously encouraged me when the work became challenging. I appreciate all the moral support that helped me accomplish this goal.

DEDICATION

I dedicate this work to the ladies in my life, that is, my mother Mavis Sikhubongani Phakathi, my wife Boitumelo Motlhouwane Ngwenya, and my daughters (Letsiwe Oamogetswe Ngwenya and Anezelwe Otlotleng Ngwenya).

DECLARATION

Name: Mfanasibili Ngwenya

Student number: 36092444

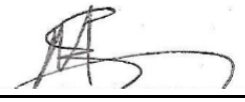
Degree: Doctor of Philosophy in Information Science

Data privacy, security and trust in 'consumer internet of things' assemblages and associated mobile applications in South Africa

I declare that the above dissertation is my work and that all the sources that I have used or quoted have been indicated and acknowledged using complete references.

I further declare that I submitted the dissertation to originality checking software and that it falls within the accepted requirements for originality.

I further declare that I have not previously submitted this work, or part of it, for examination at Unisa for another qualification or at any other higher education institution.



SIGNATURE

30 January 2020

DATE

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

2G	Second Generation
3G	Third Generation
4G	Fourth Generation
CalOPPA	California Online Privacy Protection Act
CASL	Canada's Anti-Spam Legislation
CIA	Confidentiality, availability and integrity
CIoT	Consumer Internet of Things
COP	Code of Practice
CPA	Consumer Protection Act 68 of 2008
CPU	Central Processing Unit
CRC	Checksum and Cyclic Redundancy Check
DDoS	Distributed Denial of Service
DNSSEC	Domain Name Service Security Extensions
DOPPA	Delaware Online Privacy and Protection Act
DoS	Denial of Service
DPA	Data Protection Act
ECA	Electronic Communications Act 36 of 2005 (ECA)
ECT Act	Electronic Communications and Transaction Act 25 of 2002
EUDPD	European Union Data Protection Directive
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HAIL	High Availability and integrity Layer
HIPAA	Health Insurance Portability and Accountability Act

ICASA Act	Independent Communications Authority of South Africa Act 13 of 2000
ICT	Information and Communications Technologies
IIoT	Industrial Internet of Things
IoT	Internet of Things
LoRa	Long Range
LPWAN	Low Power Wide Area Network
LTE-A	Long Term Evolution Advanced
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NVR	Network Video Recorder
PA	Privacy Act
PET	Privacy Enhancing Technologies
PIA	Protection Impact Assessments
PII	Personally Identifiable Information
PIPEDA	Personal Information Protection and Electronic Documents Act
PIR	Private Information Retrieval
POPIA	Protection of Personal Information Act
PTT	Perceived Technology Trust
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RFID	Radio Frequency Identification
ROM	Read-Only Memory
SABS	South African Bureau of Standards
SoC	System on Chip
TLS	Transport Layer Security
TPM	Trusted Platform Module
UWB	Ultra-Wide Bandwidth

VPN	Virtual Private Networks
WSN	Wireless Sensor Network

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

1 INTRODUCTION: SETTING THE SCENE

1.1 Introduction and background to the study

The Internet of Things (IoT) is in no doubt, a subject of economic, social, and technical significance. Projections of the impact of IoT on economies are impressive. For example, Manyika, Chui, Bisson, Woetzel, Dobbs, Bughin et al. (2015) predict that the economic effect of IoT on the worldwide economy may rise from $3.9 trillion in 2015 to $11.1 trillion by 2025. Coetzee and Eksteen (2011) make a point that policymakers and public authorities have a responsibility to ensure that IoT contributes to economic growth and address societal problems. The rise of IoT has driven mobile applications (mobile apps) development. For example, in the consumer IoT (CIoT) space, any product almost always comes with a smartphone application to either control, program, or just view what is happening with the product. Tiwary, Mahato, Chidar, Chandrol, Shrivastava and Tripathi (2018) point out that the consumer has to download the required application using a smartphone, a tablet or a laptop. Through this application, he or she can communicate with a centralized database and obtain valuable data about the environment.

Manogaran, Varatharajan, Lopez, Kumar, Sundarasekar and Thota (2018) ascertain that wearable medical devices have sensors that continuously generate enormous data called big data, which may be structured or unstructured. Many other scholars (Piwek, Ellis, Andrews and Joinson, 2016; Shankar, Kleijnen, Ramanathan, Rizley, Holland and Morrissey, 2016; Munos, Baker, Bot, Crouthamel, Vries, Ferguson et al., 2016; Lea, 2018) have mentioned the usefulness of wearables and mobile apps. Wearables support health systems, symptom tracking and fitness, education, among other things. According to Schmitt, Meier, Diez and Stiller (2018), IoT connects various devices via the internet with a wide variety of resources such as memory, computational capacity, and energy consumption. Babar, Mahalle, Stango, Prasad and Prasad (2010) allude that IoT is an intelligent coordinated effort of tiny sensors and devices bringing new difficulties to data privacy, security and trust. In this study, the researcher uses the terms “things” “objects”

and “devices” interchangeably whereby each word provides specific emphasis on certain points. The sensors and actuators sit on the devices to make them smarter. The connection between the sensors and the gateway can happen via any communication IoT protocol such as LoRa, NB-IoT, Zigbee, Z-Wave and Wi-Fi to name but a few. The schematic diagram in Figure 1.1 summarizes an underlying IoT architecture. The Gateway allows access to the internet and thus to a centralized server location. The consumers are therefore able to access the server via the internet for viewing, controlling and making configuration changes if need be.

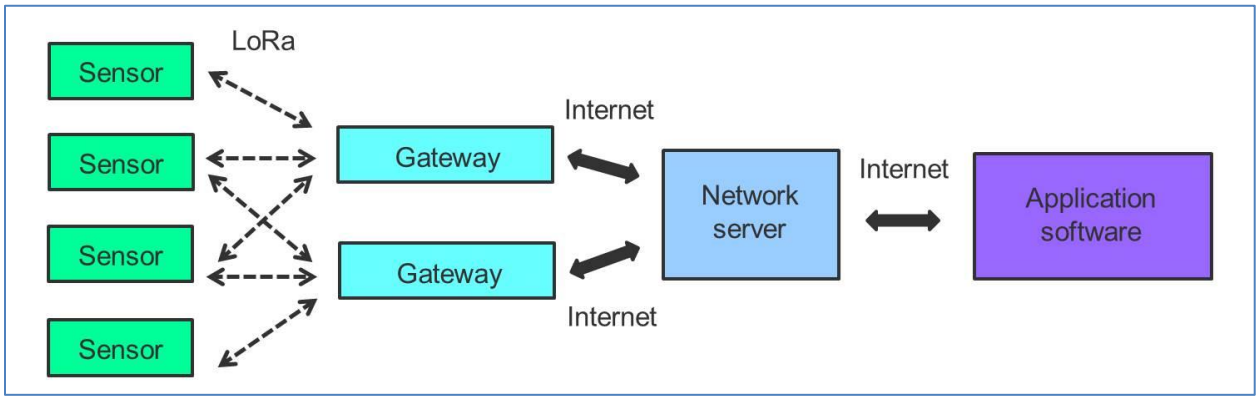


Figure 1.1: An underlying IoT architecture (Ebi, 2016).

The original contribution of this research was to bring awareness to all stakeholders of a CIoT assemblage and develop a holistic framework that addresses the challenges that come with the adaptation of CIoT such as data privacy, security and trust concerning consumers of IoT that use mobile apps. The framework looks at all the issues from a technological, legal and social context. The contribution acknowledges the role that information science plays in a world where big data, mobile apps and IoT have become part of our lives. Many types of technologies, such as the Big Data, IoT, Artificial Intelligence, Augmented Reality, and Relational Databases expose people’s private lives in one way or another. Paul, Kumar, Chatterjee, Ghosh, Shivraj and Ganguly (2014), acknowledge that the field of Information Science is interdisciplinary and is responsible for several activities in IoT such as information selection, collection, organization, management, processing, and dissemination. They further ascertain that these activities

require many tools and technologies to succeed, including communication technologies, multimedia technologies and database technologies. Information Science integrates with subdomains such as management science, computing, information and communication technology, cognitive science and other related fields. IoT and mobile apps technologies use a combination of these already mentioned technologies. Paul et al. (2014) allude that Information Science is responsible for a strong relationship between technology, information and people. This research sought to preserve this existing relationship while taking cognizance of the dangers that exist when it comes to people and the data thereof while using these advanced technologies.

The IoT technology makes it possible to connect all of a person's devices to create a smart eco-system or what is called assemblage by the assemblage theory (DeLanda, 2016; Hoffman and Novak, 2017), and thus makes a person's life a far more integrated one. Each of these devices has internet connections, meaning that people connect to devices via the internet. Such links and interactions share personal data with the mobile apps developers and their partners or any other stakeholders. Consumers need to be aware of the benefits and risks in a world where the number of cyber criminals has increased tremendously.

Belk (1988) argues that objects are passive and that consumers use them in a one-directional relationship. However, the advancement of technology and the widespread availability of smart objects prove that these objects are far from being passive. Smart things have properties that make them something more than what consumers do with them. These properties allow them to affect the consumers and for the consumers to influence the devices in return. In essence, such features permit interaction with consumers and with other objects. Hoffman and Novak (2017) allege that IoT has made it possible for smart things to transgress or go beyond their ontological borders. In essence, smart devices and humans are entities that can be on the same ontological footing and thus are irreducible by the other. They argue that as soon as smart objects connect to the internet, and use their computational powers and memory, they assume the same ontological footing as humans in one way or another. Zwick and Dholakia (2006)

agree and state that capacities of smart things to affect consumers and of consumers to affect smart things in return suggest that smart objects are becoming ontologically indeterminate and emerging entities akin to life forms. In CIoT, things act and generate data without human intervention and finally learn new things through machine learning and artificial intelligence because of the continuous interaction that exists amongst smart things and between humans and smart things.

Service providers store most of the information generated within the IoT ecosystem in fragmented data silos or some centralized location. The devices in CIoT technology send data to a centralized database and analytical system, and consumers can communicate with smart devices via mobile apps on smartphones or tablets. Kang, Pang, Da Xu, Ma and Wang (2014) emphasize that smart screens are the primary interfaces when communicating with IoT devices and accessing the central storage, database and analytical system. The smart screens include the light-emitting diode (LED) that display on smart refrigerators. All smart screens provide the view of apps the same way as in tablets and smartphones. Consumers judge the quality of smart home systems based on the functioning of the IoT mobile app. Some of the examples of CIoT are,

- a thermostat that the consumer operates from a smartphone
- a connected car that the consumer operates from a smartphone
- home automation and an alarm system that the consumer operates through a mobile app
- a biometric system in the watch or any wearable

Bassi, Bauer, Fiedler, Kramp, Van Kranenburg, Lange et al. (2016) mention that IoT is a rising network that connects physical devices and people employing software and thus enables an assemblage of applications and services that improve and simplify the lives of consumers. If this network can guarantee data privacy, security and trust for people and businesses, it can contribute to sustainable growth in many ways. Rose, Eldridge and Chapin (2015) claim that when service providers effectively use IoT models to communicate, they enhance innovation and thus open up opportunities for business development. They further imply that IoT brings an essential promise for conveying

economic and social and benefits to rising economies such as South Africa. For example, areas such as sustainable agribusiness, water quality, human services, healthcare industrialization, and ecological administration, among others, bring hope of economic development and dealing with societal ills.

IoT and mobile apps make it possible to have smart homes and smart cities (Blowers, Iribarne, Colbert and Kott, 2016; Wyman, 2015; Perera, Zaslavsky, Christen and Georgakopoulos, 2014). Manufacturers of Smart devices and developers of mobile apps have to consider the dangers that come with IoT. The designers of CIoT systems need to integrate data privacy, security, and trust in the design of the hardware of the appliance. A framework that addresses all stakeholders such as policymakers and authorities, original equipment manufacturers, mobile apps developers and consumers is critical to address the concerns related to data privacy, security and trust in CIoT in a holistic fashion.

It is safe to assume that consumers will always use mobile apps for every possible interactive experience with IoT devices used in CIoT. The assumption that consumers will always use mobile apps with CIoT devices comes from two factors, namely:

- mobile apps for both Android and IOS offer practical means to interact with smart devices, and
- there have been substantial financial benefits with mobile apps that the expectation is that they will continue to be part of our lives

This study focused on data privacy, security and trust in as far as they relate to storage, connectivity, management and processing issues. Consumers of IoT need to keep the following questions in mind when using mobile apps and when interacting with smart devices:

- Who can have access to the collected data?
- Where do service providers store the data that they collect?
- Who owns the data that service providers collect?
- What do service providers do with the data that they collect?

The data in question may reside anywhere in the world. Each country has its own set of laws concerning data privacy and ownership. Regardless of where the data resides in the world, the issues of data privacy, security and trust are real, and the internet has no boundaries. The topic of inquiry relates to the overall CIoT assemblage, and such an assemblage may include wearables, mobile apps, security, privacy and trust issues in the assemblage. Much research has focused on the technical approach to data privacy, security and trust, giving no attention to the legal and socio-economic strategies that may address societal concerns and jurisdictional issues. Shang, Zhang, Zhu and Zhou (2016) agree that current studies have investigated the technical aspects of implementing IoT technology. Some scholars (Hancke, Markantonakis and Mayes, 2010; Medaglia and Serbanati, 2010) already identified challenges in CIoT as security and data privacy but fell short in providing a framework to deal with these challenges. Fantana, Riedel, Schlick, Ferber, Hupp, Miles et al. (2013) state that prior research on IoT technology has focused on design and usage side of organization or industry. Li and Wang (2013) suggest that there has not been much attention given to understanding how consumers interact with the IoT technology. In essence, previous research ignored the social context and consumers on CIoT. Given the high functional importance and a shortage of earlier empirical work, the present investigation aims at developing an all-encompassing and integrated model of factors to determine safer ways for consumers to use IoT technology.

1.2 Problem statement

The biggest problem is that mobile apps and smart devices used in IoT are an overlooked security risk. Customers download applications and use them without mulling over the type of personal information they are exposing to the rest of the world (Fong, Lam and Law, 2017). Smart devices allow for ubiquitous data collection and tracking.

Generally, some consumers are not even aware that smart devices collect their data and have no idea of the intended destination and usage. The benefits of CIoT come with privacy and security threats, especially when people do not correctly implement the CIoT vision. As a result, the trust of CIoT comes into question. The available data generated

from CIoT can benefit humans immensely. For example, when the collected data ends up with the right people, we may save lives, convict criminals, and curb further criminal activities. However, the very same collected data may end up with the criminals who may use one's data for illegal activities such as compromising one's financial data, stealing identities, and many more. Rose et al. (2015) acknowledge that in information technology, there has always been a concern when it comes to security. However, CIoT brings with it new and unique difficulties. Consumers need to have trust that CIoT devices and all associated services are safe from online threat. Such faith is critical as CIoT has become more pervasive and integrated into our lives. When IoT devices and services do not have robust security, they can become entry points for any potential cyberattacks and expose the consumers' information to cybercriminals.

Moreover, Rose et al. (2015) allude that when IoT devices connect to the internet without proper security by the CIoT service providers, they compromise the safety of the consumers and the resilience of the internet. This threat is further made worse by,

- the massive deployment of these heterogeneous CIoT devices,
- devices being able to link to other devices automatically, and
- deploying the devices environments that are not safe.

Consumers behave differently, and the researcher assumes two types of people for this study. Some understand that mobile apps and IoT devices come with risks and others do not. Unfortunately, the majority of the people fall in the latter category (Liang, Li, Yang and Wang, 2015). Riggins and Wamba (2015) argue that there is an increased doubt by consumers when it comes to deploying location sensor devices because of privacy and security worries. Hoffman and Novak (2017) demonstrate that consumer experiences vary and are dependent on those consumers interacting with smart objects. For example, in an intelligent home environment, the mother of the house may be using Amazon Alexa to order products online. The father may be interested in setting the alarm system remotely and catching up on the news, and finally, the child may only be interested in Alexa assisting him with his homework or reminding him of the online game with his friend.

Each consumer uses the same home system to achieve his or her different interests. The way each consumer interacts may be either positive or negative.

The emerging literature on the topic of consumer-object interaction identified data privacy, security and trust concerns as being among the critical hindrances of the widespread adoption of CIoT (Lee and Lee, 2015; Babar et al., 2010). When service providers do not attend to security concerns, the results may be reduced adoption by consumers. This means one of the factors that drive the adoption and success of CIoT is security. Ali, Vecchio, Pincheira, Dolui, Antonelli and Rehmani (2018) mention that gathered data from CIoT devices may have private and confidential information. The authors further state that various threats exist that aim to take advantage of the vulnerabilities of existing CIoT infrastructures. Another challenge raised by Rose et al. (2015) is that of hacking of internet-connected devices, surveillance concerns, and privacy fears. They further mention that CIoT comes with technical difficulties, new policies and legal challenges. Ziegeldorf, Morchon and Wehrle (2014) emphasize some of the problems as the pervasive privacy-aware management of individual information, and methods to control or avoid ubiquitous tracking and profiling. These challenges could inhibit the realization of the potential benefits of CIoT and hence this research specifically gave an overview, analysis and taxonomy of data privacy, security, and trust challenges in CIoT.

We cannot ignore the advantages that come with CIoT and the convenience of using mobile apps to communicate with IoT devices. However, it is equally valid that we cannot ignore the associated risks. The world is not short of stories of data breaches. These stories come from all angles, such as providers of health insurance, mobile phone operators, government agencies, and social media, to name but a few. The reliance on smart devices has tremendously increased over the years, and thus it is only natural to be concerned when stories of data breaches are all over mainstream media. Many everyday activities will continue to rely on smart devices and apps such as our health, nutrition, location-related services, productivity and the security status of our homes (Stankovic, 2014). Manogaran et al. (2018) indicate that data security is a crucial

requirement in healthcare big data system. Data security is also critical in home security systems, banking, agriculture and any industry that make use of IoT and generate data.

The priority in terms of using IoT differs from one country to another. The focus of this study is on the South African environment. In South Africa, the levels of crime are higher than in certain parts of the world, and thus there have been many initiatives around community safety using the IoT technology. For example, according to UNODC (2016), South Africa has intentional or deliberate homicide victims of 34 per 100 000 population in 2016, while the world average was 6.0. The United Nations on Drugs and Crimes defines deliberate homicide as unlawful death inflicted upon a person with the intent to cause death or severe injury. Dlodlo, Mbecke, Mofolo and Mhlanga (2015) mention that the government of South Africa has a massive task of reducing crime levels yearly. They ascertain that the use of information and communications technologies (ICT) in general is crucial in finding solutions to be used to curb crime. The South African government, businesses and consumers need to look at new ways of fighting crime. IoT and associated mobile apps may be a catalyst in the fight against crime in one way or another. CIoT allows consumers to make use of the technology in securing their environments such as homes, parks and communities at large.

Furthermore, in South Africa, there is a high unemployment rate, which means that there is a dire need for entrepreneurs to create jobs, and IoT and other technologies can assist in curbing the high unemployment rate. However, Palattella, Dohler, Grieco, Rizzo, Torsner, Engel et al. (2016) warn that we cannot realize business opportunities and advance entrepreneurial spirit when we do not address some fundamental issues around IoT data privacy, security and trust. The proposed framework raises new and comprehensive requirements between different actors concerning authentication, accountability and non-repudiation. Hoffman and Novak (2017) adopt a non-human centric approach, using the assemblage theory that considers all entities on equal ontological footing when dealing with consumer experiences in CIoT and challenges thereof. They point out that objects are much smarter than ever. Thus the non-human

centric approach allows consideration of how non-human entities may affect experiences of humans and their own experiences.

Rose et al. (2015) mention that the scope of IoT issues does not just affect industrialized nations, but also the developing world. If developing countries such as South Africa are to benefit fully from IoT, they need to respond to the challenges and realize the benefits of IoT. Besides, society needs to address the unique needs and challenges that are prevalent in less developed countries. Some of these challenges include the infrastructure that needs to be ready, market and investment incentives, technical skill requirements, and policy resources. In essence, South African infrastructure needs to support these emerging technologies. It may include better management of spectrum, network coverage to remote areas, infrastructure that can handle the bandwidth associated with big data, data centres, to name but a few. On the market and investment incentives, business owners need to realize their returns on investments. They also need to be supported by allowing policies and regulations in South Africa.

There are many legal implications to take into account when it comes to IoT technology. Weber (2010) raises the importance of regulating IoT through state laws. He asserts that IoT is a significant field that needs regulation. The author further alludes that national laws are not sufficient in dealing with global systems like IoT. He worries that it will be challenging to have an intergovernmental regulation body. This study acknowledges that different parts of the CIoT system may reside in other jurisdictions across the globe. Several issues need regulations, including where the data is stored and processed from a geographical location point of view. Weber (2010) is of the view that national regulations should be able to influence where data is stored. In South Africa, the state needs innovative approaches to ensure that they use old and new effective legal instruments in dealing with CIoT issues.

Finally, the bandwidth should be scalable, and free of latency and jitter, that may influence the performance of the CIoT assemblages. South Africa needs adequate human capital to supports these technological advances from a deployment and support point of views.

The problems in CIoT as far as privacy, security and trust are real, and the researcher summarizes them in the “definition of keywords” section.

Palattella et al. (2016) acknowledge that fitness and health tracking systems, smartwatches and sensor-rich smartphones may expose sensitive data such as someone’s health status or life habits. They further state that the increase in the number of devices and the exchange of data multiplies the vulnerabilities of the systems, and thus becomes more susceptible to privacy leaks and attacks from the internet. Ali et al. (2018) allege that centralized cloud services have made significant contributions to the growth of IoT. However, they admit that a centralized approach can be a hindrance in the development of the IoT because of the potential risks associated with a single point of failure when the system is under attack. When the cloud services such as the database are centralized, and are under lethal security attack, or have faults, the attacker may bring down the whole assemblage. Ali et al. (2018) assert that consumers of IoT do not have total confidence and control over how service providers use the data they share and therefore, do not trust the CIoT ecosystem.

1.3 Purpose and objectives of the study

The purpose of this study was to explore the data privacy**,** security and trust issues faced by consumers of IoT in South Africa, to propose an integrated and holistic framework that promotes safer adoption of CIoT and associated mobile apps in South Africa as consumers of IoT continue to interact with smart things. The specific objectives were to:

- Analyse the legislative frameworks for data privacy, security and trust concerning CIoT in South Africa.
- Determine the technical approaches in dealing with data privacy, security and trust in CIoT in South Africa.
- Analyse the dynamics and experiences of consumers of IoT concerning data privacy, security and trust while using mobile apps as the primary interface to communicate with smart devices.

- Analyse the responsibilities of CIoT stakeholders that may influence the challenges that come with of CIoT.
- Develop a framework for data protection, security and trust in CIoT when using mobile apps.

1.4 The originality of the study

Stankovic (2014) indicates that in academia, originality of the work output is valuable. This originality is even more critical at the doctoral level. There are several ways to ensure the freshness of the study and may include developing new methodologies, new tools or techniques, new researcher area, a new way of interpreting existing material, and new applications of the current literature to the new domain or unique blend of ideas. This study is essential as it addresses a new area of interest regarding data privacy, security, and trust in CIoT and associated mobile apps. The study sought to develop an integrated and holistic framework that addresses data privacy, security and trust issues related to consumers of IoT that use mobile apps as they adopt the IoT technology.

Very often, data generated and stored in mobile apps pose a security danger to consumers. However, there have been limited studies in this area of research. Furthermore, there are limited studies of IoT and mobile apps in the South African environment. Therefore, the issue of security, data privacy and trust in CIoT and associated mobile apps offer a new area of research that is in its infancy. In the process of generating new knowledge, the researcher acknowledges the role of information science in a world where information travels from one part of the world to another at the speed of light. The researcher approaches the CIoT assemblage from a holistic point of view that considers regulatory issues, technical issues, the social context and stakeholders' responsibilities.

1.5 Scope and delimitation of the study

This study considered privacy and security threats in several perspectives as in the following:

- Existing privacy and security legislations concerning the unique and evolving features in CIoT
- Technical viewpoints in CIoT
- Experiences of consumers of IoT and their future behavioural intentions
- Responsibility of all stakeholders

Ziegeldorf et al. (2014) allude that there has to be a clear understanding and appropriate countermeasures of the issues that arise from CIoT. Without this understanding and without taking proper steps to counter the threats, the success of services like those from CIoT will be in peril. The researcher confined this study to matters relating to data privacy, security and trust, from a technological, legal and socio-economic perspective in CIoT and associated mobile apps in the South African environment. The study further addressed all stakeholder interactions in the CIoT assemblage.

1.6 Definition of keywords

It is of paramount importance to define the keywords in the study. This section seeks to identify and clarify the essential keywords, namely information privacy, personally identifiable information (PII), Internet of Things (Consumer IoT and Industrial IoT), smart things.

1.6.1 Information privacy or data privacy

Many scholars (Dinev and Hart, 2006; Akturan and Tezcan, 2012; Rose et al., 2015) agree on the definition of data privacy and use personal information as private information. They allude that personal information is valuable to the owner of that

information. It is for this reason that relevant stakeholders put measures in place to control it. Private or confidential information includes such information as physical location and movement of the person. Rose et al. (2015) allude that it is vital to respect people's privacy to gain full benefits of CIoT. Such respect for people's privacy should come from all stakeholders of the assemblage. Besides, service providers and regulatory bodies need to implement privacy enhancement technologies (PETs) and relevant protection laws. Finally, there is a need for standards, methodologies and tools to identify consumers and objects. Dinev and Hart (2006) state that the loss of private information is a huge privacy risk. Akturan and Tezcan (2012) are of the view that when the issue of data privacy relate to consumers losing control over personal data. The threat to personal privacy can happen at data collection, data storage and data transfer. When a person feels that certain information is private to him or, then it is as per their right to choose. Ziegeldorf et al. (2014) capture the idea of informational self-determination by saying that every person needs:

- to assess his privacy risks,
- to take appropriate action to protect his privacy,
- be assured that all relevant stakeholder can enforce privacy beyond his immediate sphere of control

1.6.2 Security

The study looks at security from both information security and from the security of the assemblage itself. The Security triad (or CIA Triad) is a recognized model for the improvement of security mechanisms in information technology. According to Farooq, Waseem, Khairi and Mazhar (2015), the CIA Triad executes the security by utilizing the three areas, which are data confidentiality, integrity and availability. A compromise of any of these three areas could cause severe issues to the system, and thus they must be accounted for. Al-Momani, Mahmoud and Sharifuddin (2016) state that security is about the extent to which a person believes that using a particular application will be risk-free. When consumers of IoT use IoT, they need to be risk-free as much as possible. The developers of CIoT need to ensure safety from the design stage to the execution stage.

Services providers of CIoT need to be proactive in the identification and protection of IoT from arbitrary attacks such as denial of service (DoS) attacks and abuse. In addition, service providers need to ensure that malicious software does not enter the IoT ecosystem. The CIoT service provider is responsible for continuously updating the software and firmware of devices in response to security threats.

1.6.3 Trust

Trust comes in many different forms. Chen, Bao and Guo (2015) allude to social trust metrics such as honesty, cooperativeness, and community interest. These trust metrics complement each other. Diamantopoulou, Androutsopoulou, Gritzalis and Charalabidis (2020) state some consumers are complacent with their personal information and express implicit trust in their service providers, and government and legislation, believing that they will protect them from the unlawful use of their data.

Consumers need to be comfortable in exchanging personal information with any CIoT stakeholder. The information exchange is critical in the success of CIoT, and sensitive data must be protected. This trust also applies when smart objects communicate on behalf of consumers with trustworthy services. Trust has to be incorporated from the design stage of CIoT and must be in-built in the system. Also, trust needs to exist amongst all stakeholders, such as cloud providers, device manufacturers, connectivity providers, and mobile apps developers, to mention just a few, in the CIoT assemblages. The literature review section in Chapter Two expands on trust issues when it comes to the CIoT assemblage.

1.6.4 Internet of Things

Internet of Things is about connecting everything on earth with the help of the internet. The ubiquitous connectivity and communication among the objects transform the ability to collect, analyse and distribute the data so that any stakeholder can gain insights and

thus proactively perform useful actions. Many scholars (Palattella et al., 2016; Stojmenovic, 2014; Smutný, 2016) have made a distinction between the consumer internet of things (CIoT) and the industrial internet of things (IIoT) as below:

- **CIoT** – This is when we use the IoT technology for consumer-oriented applications. In CIoT, data volumes and rates are low. It is the interconnection of consumer electronic devices and anything belonging to consumers' environments such as homes, offices, wearables and cities.
- **IIoT** – This is when IoT is machine-oriented, implying machine-machine communication with a distributed control. In essence, once implemented, IIoT does not require human intervention. It is when operational technology (OT) and information technology (IT) meet. It allows smart machines, networked sensors, and data analytics to improve business-to-business (B2B) services industries. Such improvements may be from manufacturing to mining to public services. In IIoT, data volumes are very high and hence the term big data.

1.6.5 Smart Things

Silverio-Fernández, Renukappa and Suresh (2018) define a smart device as a context-aware electronic device. This electronic device can perform autonomous computing and connect to other devices to exchange data. The key phrase in the definition is context-awareness. The smart things are context-aware because of built-in sensors that come with the devices. Smart things come in many forms and shapes. According to Ma, Yang, Apduhan, Huang, Barolli and Takizawa (2005), we can classify smart things into three categories namely;

- smart object,
- smart space and smart system,
- according to their appearances and function

1.7 Conceptual framework development

Ngulube (2020) advises students at the doctoral level to spend more time on topics related to the application of theory in research. He argues that this will give future professionals a sound basis for applying theory in their work and study irrespective of the discipline and context. Furthermore, Ngulube (2020) illustrates five ways of formulating a conceptual framework of a study as:

> (i) putting together various concepts from different theories, (ii) aspects of a theory, (iii) incorporating aspects of a theory or theories, concepts from the literature, personal experiences, knowledge of the context and models, (iv) integrating all the concepts from more than one theory, and (v) combining concepts from the extant literature.

This study utilized the third category by putting together concepts from literature. As a result, to come up with a conceptual framework for this study, the researcher took into consideration different factors that affect the assemblage such as the legal and regulatory factors, technological factors, and stakeholders' involvement. After that, the researcher analysed how these factors affect the social context. The researcher integrated these factors with storage and connectivity issues, management issues, and processing issues, as highlighted earlier. The conceptual framework addressed the three primary constructs under study, namely data privacy, security and trust. This study looked at theoretical approaches to how things interact in general and how they interact with humans from a philosophical perspective. The researcher developed the proposed framework with the guidance of detailed literature review, assemblage theory, Dewey's experience theory, and the CIA (Confidentiality, Integrity, and Availability) Triad. The next sub-section briefly explains the assemblage theory.

1.7.1 Assemblage theory

The Assemblage Theory (DeLanda, 2016) was used to assist in the interpretation of the CIoT ecosystems or assemblages in Chapter Five. The Assemblage Theory considers

external influences and thus includes the social context, legislators and policymakers, original equipment manufacturers and mobile apps developers, and historical factors. Many scholars (DeLanda, 2006; Harman, 2008; Hoffman and Novak, 2017; Buchanan, 2015; Hoffman and Novak, 2015) have applied the assemblage theory in various fields, taking advantage of the theory's prominent characteristics. Some of the aspects are about the inter-relationships, interactions and inter-connectivity of different elements within the assemblage and between assemblages and the environment, and thus further exacerbate the complexity of an assemblage. The other theory to be used in the interpretation of the experiences in Chapter Five is Dewey's experience theory and is explained below.

1.7.2 Dewey's experience theory

Dewey's experience theory is three dimensions of experience theory (Clandinin and Connelly, 2000; Dewey, 1958). The experience theory was coined by Dewey (1958) and expanded by Clandinin and Connelly (2000). Dewey (1958) ascertain that a person's present experiences are a direct result of their previous experiences. That means people's current behaviour can either be careless, careful, based on their experiences. The revised experience theory by Clandinin and Connelly (2000) look at personal and social (interaction); past, present, and future (continuity); and place (situation). For example, if a person was once a victim of phishing, they become more cautious when communicating with their banks, or even any email correspondence (interaction). Alternatively, those victims are most likely to take precautions in the present, and thus influencing their present and future experiences (continuity). Finally, if the crime took place online, they are most likely not to be comfortable with online transactions (situation). The researcher used this theory, in addition to the assemblage theory and CIA Triad, to further interpreter the findings of a CIoT ecosystems or assemblages in Chapter Five, and thus forging a holistic view when it comes to the concerns or challenges of CIoT.

Consumers can relate their experiences as they interact with mobile apps and devices. Storytelling is part of our lives and thus analysing stories from consumers of IoT gave

insight into their experiences as part of the research. The consumers narrated their past and present experiences, as well as how they intended to do things differently in the future. Finally, the consumers provided context or situations as to where they felt it is worth using IoT and mobile apps.

A combination of consumer experiences through narrative inquiry and the findings from experts using the Delphi Technique was critical in developing a holistic framework. The concerns of data privacy, security and trust were then analysed to create a structure that considers consumer experiences and expert findings while taking cognisance of theories that do not abide by human-centric approach when dealing with CIoT challenges. In addition to the assemblage theory and Dewey's experience theory, the researcher used the CIA triad to deal with the security issue and later introduces data privacy and trust.

1.7.3 CIA Triad

The CIA (Confidentiality, Integrity, and Availability) Triad is an excellent theory to introduce and analyse data security as it addresses the confidentiality, integrity and availability of data. This model is discussed further in Chapter Two under the security section. Dardick (2010) state that the CIA Triad is a widely used model in information security, and is a recognized model for the improvement of security mechanisms, and executes the security by utilizing the three areas of the triad (data confidentiality, integrity and availability). According to Farooq et al. (2015), if any of the three components of the triad is compromised, the consequences can be severe to the overall system. They allude that an IoT ecosystem needs to ensure proper identity authentication mechanisms and provide confidentiality about the data. The next sub-section briefly describes security from data or information point of view as per the current study.

1.7.4 Data privacy, security and Trust

Security – any IT system requires some form of protection to avoid any type of abuse and unauthorized use. Babar, Stango, Prasad, Sen and Prasad (2011) state that a sound security solution should consider the security from design to implementation and from manufacturer to consumption and even disposal. The study highlights the need for built-in, end-to-end security measures in the devices and the whole assemblage. Security is critical to the efficient functioning of CIoT. Service providers need to provide infrastructures that are flexible and can dynamically prevent, detect, diagnose, isolate and respond appropriately to avoid breaches. The security part unpacks data confidentiality, data availability and data integrity (Farooq et al., 2015). The proposed framework expands to include data privacy and trust in addition to security. It is essential to understand the limitations of CIA Triad to address holistically the challenges raised concerning CIoT. If providers of IoT do not address security issues in a CIoT assemblage, it affects personal information privacy. It increases the trust issue of the whole ecosystem and between all stakeholders. The literature review in Chapter Two discussed information and data security in more detail.

Data Privacy – The framework considers data privacy as a critical issue in CIoT. Component to The study looked at the three areas introduced under the definition of keywords as data privacy, security and trust. There is no doubt that CIoT raised the debate around privacy issues. The implementation of CIoT directs the way personal data is collected, analyzed, used, and protected. Dinev and Hart (2006) describe privacy risk as a measure of the potential loss of private information. However, they acknowledge that consumers sometimes have to disclose personal information to receive certain benefits from service providers. Akturan and Tezcan (2012) define privacy issues as the potential loss of control over personal data. Rose et al. (2015) state that the full potential of CIoT is dependant on approaches that respect people's privacy. The threat to personal privacy can happen at data collection, data storage and data transfer.

- **Data collection** refers to how the sensors obtain the data from the environment and consumers. Sfar, Natalizio, Challal and Chtourou (2018) state that during data collection and transmission, we need to focus on networking issues and technologies such as Radio Frequency Identification (RFID), Wireless Sensor Network (WSN), and mobile connectivity. The question arises as to whether that data collection is violating consumer privacy in one way or the other. Are consumers allowed to consent to data collection or is data just collected discreetly without consumers' knowledge?

- **Data Storage** looks at the collected data in terms of where it is stored. Is it within a particular jurisdiction? Is it essential that the collected data resides locally or otherwise? What are the challenges if the consumers do not know where that data storage is, and do consumers have a right to know?

- **Data transfer** focuses on how data moves between objects, humans and analytical platforms. It also refers to how stakeholders share data amongst themselves and with third parties. Is the way service providers share the data violating privacy regulations such as the Protection of Personal Information Act (POPI Act), the Consumer Protection Act (CPA), the Electronic and Communications Act (ECA), and the Electronic Communications and Transactions Act (ECT Act) in South Africa?

Trust - McKnight, Choudhury and Kacmar (2002) define trust as one's perceptions regarding the integrity and ability of the actant providing the service. The framework addresses trust at three levels, namely consumers and businesses level, smart devices level and network level.

- **Consumers and businesses level:** Trust in consumers alone can be a massive issue for businesses. Humans always want to manipulate the data for some nefarious gains. How can companies endeavour to make sure that you can trust the data from consumers? What checks and balances can businesses put in place to safeguard and trust the accuracy of the data from consumers?

For example, some consumers have used fitness-monitoring devices for the wrong reasons, such as attaching these devices to a dog or cat to accumulate fitness points. While the idea of these wearables is to ensure that people remain active for health purposes, the collected data is not correct, as the entity making the movements is a dog or cat. People turn to use different devices for wrong purposes. Lea (2018) gives examples of the use of CIoT in pets as pet location systems and smart dog doors. However, people always try to circumvent systems or repurpose solutions for other use cases. While this may be wonderful and innovative, it can also be disastrous as incorrect data is collected. Discovery Vitality in the South African context has been battling with the trust issue for a long time now. It is challenging to tell if a person has been exercising or not. Lea (2018) further suggests that consumers experience IoT daily in their personal and work life through their interaction with a Fitbit fitness tracker, an Amazon Echo assistant, or a Google thermostat, among others. According to Li and Wang (2013), IoT technologies affect consumers' behaviour in several aspects of the users' daily life.

- **Smart devices level:** Trust needs to exist at smart devices level when collecting the data. If the device is faulty and thus collects untrustworthy data, the consequences can be dire and even life-threatening. This trust has to exist from data collection up to data storage.

- **Network-level:** We cannot afford to ignore trust at the network level. Network-level trust refers to end-to-end communication between smart things and consumers. What threats exist in networks when things communicate with other things and people? How can we secure the communication paths without compromising performance and consumer experience? Can we trust that the networks do not compromise or allow data alteration and thus misinform consumers or any stakeholder that has an interest in the collected data?

1.7.5 The framework

The conceptual framework assists in analysing privacy threats and challenges while taking into consideration different aspects that affect the overall assemblage of IoT and mobile apps. With the above in mind, an initial framework to develop is, as shown in Figure 1.2:

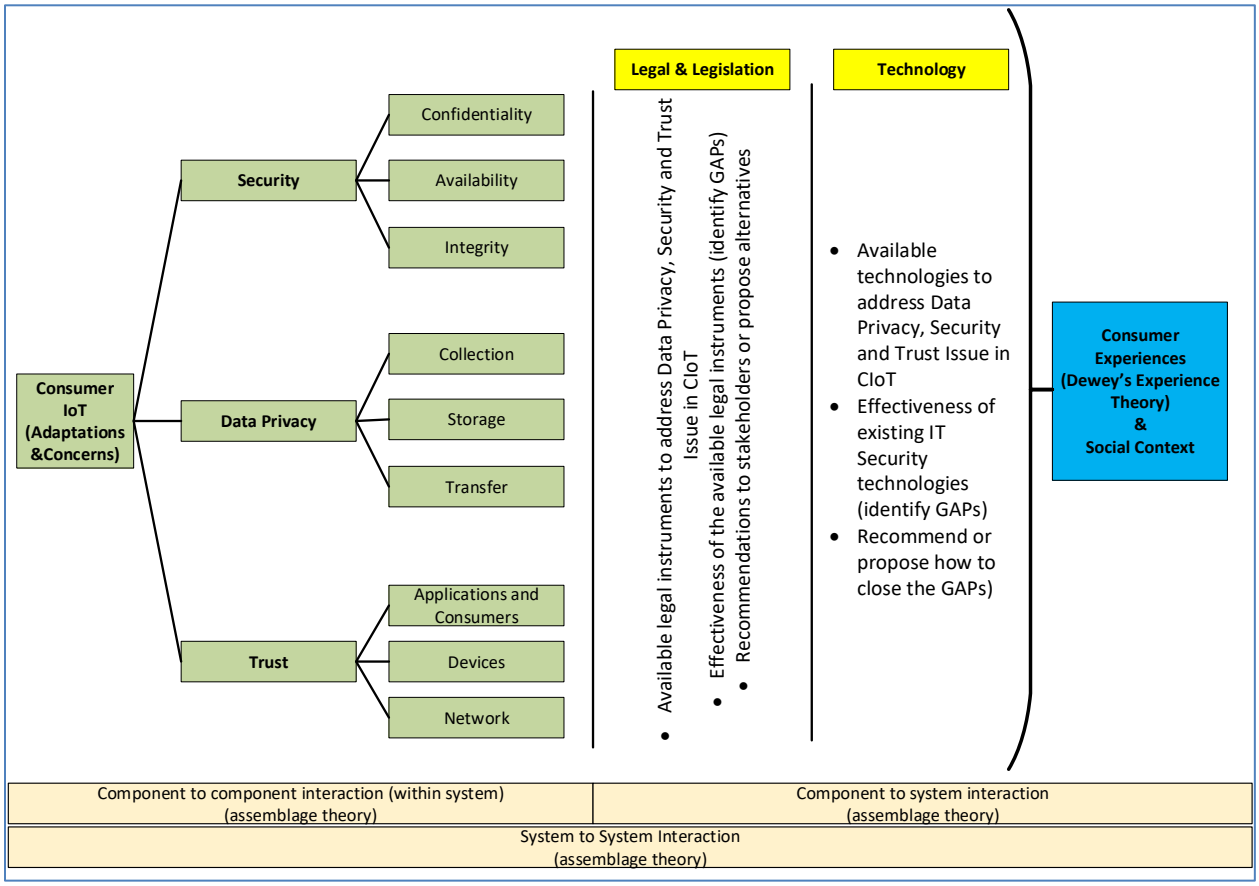


Figure 1.2: Conceptual framework (Researcher)

1.8 Literature review of consumer IoT

Chapter Two covers the literature review in more detail and addresses themes related to CIoT and associated mobile apps. The covered ideas include legal and legislative framework, technological considerations, and layers of the CIoT assemblage. Hashemi,

Faghri, Rausch and Campbell (2016) assert that IoT related applications impose both technical and economic requirements that lead us to conclude that we need to look at IoT applications within an economic, legal and regulatory context. In other words, the technological frameworks are not enough to address the issues of privacy, security and trust.

The legal aspect discusses South African legal instruments that law enforcers may use in dealing with CIoT concerns. The discussed laws are:

- Protection of Personal Information Act 4 of 2013 (POPI Act)
- Consumer Protection Act 68 of 2008 (CPA)
- Independent Communications Authority of South Africa Act 13 of 2000 (ICASA Act)
- Electronic Communications and Transaction Act 25 of 2002 (ECT Act)
- Electronic Communications Act 36 of 2005 (ECA)

The researcher further discussed legal instruments from across the globe. The researcher chose specific jurisdictions based on the level of interactions South Africa has with those jurisdictions. Data sharing happens when doing businesses with the countries discussed. IoT related companies are not exempt the issues that arise from sharing data in platforms that may reside in the discussed foreign lands. The researcher chose some laws across the world based on their relevancy in the study under investigation, and due to South Africa interactions with those countries. The researcher discussed the following international legal instruments in Chapter Two:

- General Data Protection Regulation (GDPR) from the European Union,
- Code of Practice (COP) from the United Kingdom
- California Online Privacy Protection Act of 2003 (CalOPPA), Delaware Online Privacy and Protection Act (DOPPA), California Consumer Privacy Act (CCPA), Internet of Things (IoT) Cybersecurity Improvement Act of 2019 - all from the United States
- Privacy Act (PA) and the Personal Information Protection and Electronic Documents Act (PIPEDA) from Canada

The researcher considered the technical approaches to data privacy, security and trust by discussing existing technologies, design and development aspect, the architectural view, and finally a view of a layered approach in an IoT assemblage. After that, the researcher reviewed in detail the three constructs (data privacy, security and trust) under investigation. Finally, he argued the involvement of various stakeholders in the IoT assemblage, namely smart things, consumers, governments and regulatory bodies, device manufacturers, and application developers.

1.9 Research methodology

Bryman, Becker and Sempik (2008) define research methodology as a systematic process for solving a problem, and thus increasing our understanding of the phenomenon under study. Chapter Three discusses in detail the methodology adopted in this study. The researcher outlines the methodological themes below under the ontological considerations, epistemology, research approach, research design, population and sampling, as well as data collection tools.

1.9.1 Philosophical paradigm

The philosophical paradigm is a belief about how data about a phenomenon should be gathered, analysed and used. The next section introduces the ontological and epistemological approaches in this study. The researcher explained the philosophical paradigm he undertook in detail in Chapter Three.

1.9.1.1 Ontology

Ontology is about the nature of reality. Researchers consider ontology as a starting point of research. From there on, the epistemological and methodological positions can flow logically (Hollway, 2008; Meretoja, 2014). MacIntosh (2009) describes ontology as the image of social reality upon which to base a theory. Ontology has to do with our

assumptions about the make-up of the world and the nature of things. There are two ontological views namely; realism which posits that there is the real world, and constructivism which holds that the real world does not exist but is constructed (Kivunja and Kuyini, 2017; Chilisa and Kawulich, 2012). This study takes on the latter view, which is an ontological view that says that reality is constructed**,** subjective, multiple and relative. The experience of mobile apps users is very diverse and thus have various realities. How smart things interact with humans takes centre stage in the study. The researcher expands on this ontological view in Chapter Three.

1.9.1.2 Epistemology

According to Hussein (2009), ontology describes epistemology as what constitutes valid knowledge and how we obtain it. It has to do with our beliefs about how one might discover knowledge about the world. The term refers to how we know, and the relationship between the knower and what the knower knows. Epistemology is different from ontology (what exists, and the nature of reality) and axiology (values), as well as a methodology (Hollway, 2008; Meretoja, 2014). According to Case and Given (2016), there are two approaches to epistemological assumption, namely: objectivism and interpretivism (Case and Given, 2016; Cowling, 2016). The researcher used interpretivism and explained this epistemological approach in detail in Chapter Three.

1.9.2 Research approach

As per the previous discussion on epistemological assumptions, this research was qualitative. There are many methodological assumptions that the researcher can use in the process of qualitative research (Creswell, 2009). In this study, the researcher used inductive procedure. The researcher based this approach on his own experience in collecting and analysing data. The research is, thus, the product of the values of the researcher. The researcher developed a framework of the underlying structure of experiences or processes that are evident from the raw data.

1.9.3 Research design

According to Bell and Bryman (2007), research design provides a framework for the collection and analysis of data. This research utilized both narrative inquiry methodology and the Delphi method to come up with a structure that we can use in securing and protecting personal and device information. The use of both ways assisted with the triangulation of the research. Many scholars agree on the definition of triangulation as the combination of methodological approaches, theoretical perspectives, data sources, investigators and analysis methods in the study of the same phenomenon (Hussein, 2009; Thurmond, 2001; Jack and Raturi, 2006).

1.9.3.1 Narrative Inquiry

Clandinin (2006) describes narrative inquiry as the study of lived experiences understood narratively. He acknowledges that this is a relatively new method of research. He further mentions that it is a way of studying lived experiences. How do researchers perform narrative inquiry? Moreover, the author states that the method is recursive and reflexive. The process starts by participants telling their stories to field texts to interim text and final research text. The researcher can use different kinds of field texts and analysis to develop a framework. This method highlights ethical matters in the study and shapes new ways of understanding the experiences of consumers. Gottschall (2012) mentions that the narrative is about storytelling, and storytelling is critical for human survival. Sillars and Hallowell (2009) further indicate that anecdotes or stories provide a way of understanding our place in the bigger scheme of things by structuring our understanding of events. The researcher explains the narrative inquiry methodology in detail in Chapter Three.

1.9.3.2 Delphi Technique Method

In one of the methods (Delphi), the researcher selects individuals according to predefined guidelines and asks them to participate in two or more rounds of structured surveys. An example of where researchers use opinion-based methods is when trying to assess customer satisfaction of a specific service over a particular period. The guidelines are strict and direct the research towards a predictable outcome (Sillars and Hallowell, 2009). The researcher expands on the use of the Delphi technique in Chapter Three.

1.9.4 Population and sampling

Bryman (2008) defines a population as the total number of subjects that bear a common characteristic and out of which the researcher can extract a small fraction to serve as participants. For this study, the population consisted of users of mobile apps that the researcher selected through the snowball technique. Luborsky and Rubinstein (1995) compare different types of sampling that researchers can in qualitative research, namely:

- **Convenience (or opportunistic) sampling** - This technique is mainly for a pre-defined population. It uses an open period of recruitment that continues until the researcher achieves a predetermined number of participant. The selection process is on a first-come, first-served basis.
- **Purposeful sampling** – This technique uses participants with predefined traits or conditions. This technique is not about determining the prevalence, incidence, or cause.
- **Quota sampling** – Researchers use this method for selecting several participants to represent the conditions to be studied rather than to serve the proportion of people in the universe. This technique assures the inclusion of people that the convenience or purposeful sampling techniques underrepresent.

- **Snowball sampling** – This is a word-of-mouth technique. The aim is to use participants as sources. In other words, participants recommend others they know who may be eligible for the researcher to use as participants.

In this study, the participants had exposure to mobile apps and smart things. They had a basic appreciation of how the apps interact with objects in the world. In this study, the researcher used snowball sampling (in the case of both narrative inquiry and the Delphi technique) and purposeful sampling (only in the Delphi technique).

Chapter Three covers the detailed processes. The idea is that the participants need to be users of mobile apps for IoT purposes or be experts in the IoT industry. Once the researcher identified one or two participants, he sought referrals to people who are familiar with using mobile apps for IoT purposes. As soon as the researcher reached a saturation point, he discontinued the data collection process.

1.9.5 Data collection tools

Data collection includes many aspects, such as observing and interviewing. These aspects make the researcher and the participants to be in close contact. The researcher interacts with the participants and thus get to know them and their social context (Schneider and Somers, 2006). In data collection, this study used field texts from individuals and groups of people who are familiar with mobile applications and interact with smart things using IoT technology. The participants and the researcher create field texts (usually called data). The researcher's way of inquiring affects what he or she intends to discover. In essence, this implies that the data collection process is selective.

Engaged from a narrative inquiry viewpoint, the researcher collected field texts from individual in-depth interviews, observations and conversations. According to Chou, Tu and Huang (2013), in an interview, the interviewee is the narrator of the story (storyteller), and the interviewer is a guide in this process. Together, the two are collaborators,

composing and constructing a story. The participants hold the power of knowledge because they are the only experts on their lived experience. During the interview process, the researcher offers respectful and interested attention instead of his views. Chou et al. (2013) ascertain that it would be helpful to have questions that guide the storyteller towards the feeling level, and thus making the interview active and interactive. The feelings, actions and interactions bring out most of the meaning in a person's life. The researcher gets to a deeper level of reality in various ways, from specific types of questions to comments to sympathetic and responsive listening.

To use the Delphi method, the researcher sought expert opinion from a group of experts in the field of IoT. The aim was to identify common themes from the experts and reach consensus as far as their view on data privacy, security and trust are concerned. The researcher reached this group through emails and encouraged them through phone calls, as the participants were in various locations.

1.10 Ethical consideration

By its very nature, narrative inquiry is about telling a story about oneself. Telling personal stories may involve telling a story about individual choices and actions, and thus, raising moral and ethical dimensions to the research. This research involved human participants, and the researcher must observe the University of South Africa's (UNISA) policy on research ethics throughout the research stages. The university policy aims to discourage unethical research practice, to make ethics an integral part of the planning and methodology of research, and to protect and promote the rights of research participants finally. The University policy stipulates that the university is committed to (UNISA, 2013):

- maintaining an environment for researchers in which they may be autonomous and ethical in their work
- ensuring that researchers continue with an ethical research practice
- ensuring that the rights and interests of human participants are protected

During the research, participants needed to remain anonymous as part of respecting their privacy and confidentiality. The researcher recognised and protected the dignity, privacy and confidentiality of the participants. After that, the publishing of the research findings was such that it could not harm research participants in any way or form. The researcher reported such results accurately and truthfully. Furthermore, the researcher preserved and protected historical records and study material without revealing the names of the participants. The researcher informed the participants in detail about the purpose of the research. In essence, the researcher was seeking informed consent from all the participants.

1.11 Outline of the chapters

Chapter One (Introduction: setting the scene): – This is the introduction covering the research problem, research objectives and the theoretical argument or justification of the research problem. The researcher covered the background of mobile apps and their relationship with the Internet of Things technology in this chapter. The chapter further covers the scope and objectives as well as key terms that were critical in the research.

Chapter Two (Literature review: consumer internet of things): – This chapter argues different points, comparing, contrasting and critiquing views of prior studies about the security, privacy and trust in CIoT assemblages and associated mobile apps. The researcher clarified the differences between CIoT and IIoT. The chapter further explores the technical approaches to data privacy, security and trust, as well as some existing legal and legislative strategies. This chapter aimed to synthesize findings across prior studies. The current gaps, debates, or shortcomings in the literature provide a further rationale for the study.

Chapter Three (Research methodology): – This chapter is about the research methodology. It covers the ontological assumptions, epistemological assumptions, axiological assumptions and methods. It is in this chapter that the researcher further explains the narrative inquiry and Delphi technique methodologies. He justified why they

were the preferred methods for this research and how he collected research data. The chapter covers participants, instruments, materials and procedures. The research approach and design are part of this chapter, and so are population and sampling methods.

Chapter Four (Data analysis and presentation): - This chapter focuses on presenting the collected data. This chapter gives structure to the collected data from interviews in preparation for interpretations and discussions in the next section. In this chapter, the reader can expect themes that the researcher generated from the collected data. The researcher analysed collected data to seek meaning. Based on the literature review and results of the study, this chapter explores and develops a new framework to address the concerns of data privacy holistically, security and trust.

Chapter Five (Interpretation and discussion) – This chapter focuses on the interpretation of the collected data that the researcher presented in Chapter Four. This chapter further discusses the results and shows how the researcher addressed the research objectives. In essence, this is about interpretation and discussion of the data to find meaning or understanding.

Chapter Six (Summary, conclusion and recommendations) – The last chapter focuses on conclusion and clarity on possible further research. The researcher explores the contribution of the study on consumer IoT to industry and academia as part of the outcome. The researcher concludes by making recommendations based on the conceptual framework.

1.12 Summary

This chapter introduced the study of CIoT and mobile apps technologies while highlighting the challenges of data privacy, security and trust. These challenges are seen as a hindrance to the adaptation if CIoT and thus to economic growth. The rapid adaptation of CIoT can benefit developing countries like South Africa. It can address some of the

societal challenges such as crime, unemployment, environmental issue, to name but a few. While scholars acknowledge the benefits of CIoT, they also warn of the dangers that are associated with this technology as far as data privacy, security and trust are concerned.

The researcher addressed the key definitions in this chapter. It is in this first chapter that the researcher positioned the IoT ecosystem using various theories and further discusses them in Chapter Two. These theories include Dewey's experience theory and assemblage theory. The CIA Triad serves as a good entry point of discussion as it addresses the confidentiality, integrity and availability of data.

The researcher introduced the research methodology used in this study. He uses the narrative inquiry to understand consumers' experiences as they interact with smart things and the Delphi Technique to obtain the point of view of experts on the subject of CIoT.

This chapter concludes by addressing ethical considerations in the study. The researcher observed the University of South Africa's (UNISA) policy on research ethics throughout the research stages. There is an emphasis on the anonymity of participants in the study, and the researcher sought informed consent from all the participants. The next chapter reviews the literature on security, privacy and trust regarding consumer internet of things.

CHAPTER TWO

2 LITERATURE REVIEW: CONSUMER INTERNET OF THINGS

2.1 Introduction

The previous chapter laid the foundation of the study by introducing the research problem, research objectives, and the purpose and objectives of the study. The researcher lay the groundwork that seeks to assist in understanding and analysing how humans, smart things, and other non-human actors or stakeholders interact and how new phenomena emerge because of the interaction. Chapter Two discusses the literature as it relates to CIoT assemblages and the concerns thereof, namely: data privacy, security and trust. The chapter considers existing legal and legislative frameworks, technological considerations, social context and the stakeholders involved in CIoT assemblages.

The literature review is of vital importance in research. Bryman (2016) posits that any research project needs to have a literature review derived from existing literature. Creswell and Creswell (2017) agree by stating that the literature review is for sharing with the reader the findings of prior research that relate closely to the researcher's current study. They further assert that the literature review provides the basis for establishing the significance of the investigation and for benchmarking and comparing the new findings with other results. The expectation is that literature review should provide a summary of existing themes and issues related to the research topic.

2.2 A comparison between consumer IoT and industrial IoT

This research focused on consumer-object assemblage called CIoT and associated mobile apps as opposed to industrial IoT (IIoT). Hoffman and Novak (2017) define consumer experience in CIoT by its emergent properties, capacities, and agentic and communal roles expressed in the interactions.

It is imperative to bring to attention the distinction between CIoT and IIoT. Smutný (2016) highlights that CIoT and IIoT both follow similar architecture but acknowledges that there are some variations. Al-Fuqaha, Guizani, Mohammadi, Aledhari and Ayyash (2015) recognise that the latest developments in RFID, smart sensors, Internet protocols, and communication technologies, generally enable IoT. In this case, they do not differentiate between CIoT and IIoT as both make use of the mentioned technologies. Palattella et al. (2016) mention that CIoT and IIoT share some broad correspondence necessities, such as scalability, lean protocol stack implementations in constrained devices, and benevolence to the internet protocol ecosystem.

However, Palattella et al. (2016) further acknowledge the distinction between CIoT and IIoT and agree with other scholars (Stojmenovic, 2014; Smutný, 2016) that there are some apparent variations on the underlying technologies and business models. For example, they mention that CIoT seeks to improve the quality of people's lives by saving time and money. It involves connecting consumers' electronic devices, their homes, offices, cities and anything belonging to consumers' environments. We present appliances such as refrigerators or fitness sensors as smart. According to Smutný (2016), CIoT is about a group of consumer-oriented applications where data volumes and rates are low. In CIoT, the smart devices and applications that control those devices are not safety-critical. That means, in the case of a system failure or collapse, the life of the consumer is not in danger, and only customer satisfaction is affected. The consumer may experience the inconvenience, but the life of the consumers is not in any way under threat.

Hoffman and Novak (2017) allude that CIoT can change the consumer experience for the better as consumers actively communicate with smart things. The traditional approach of human-centric conceptualization of consumer experience is no longer sufficient to conceptualize consumer experience in the IoT. Smart objects possess their unique properties, capacities and tendencies. In essence, smart objects have their own experiences in interaction with the consumers and with each other. Since the researcher cannot interview smart objects to ascertain their experiences, the researcher is dependent on consumer and experts in IoT.

On the other hand, Palattella et al. (2016) argue that IIoT is machine-oriented, implying machine-machine communication with distributed control. In essence, once implemented, IIoT does not require human intervention. It is when operational technology (OT) and information technology (IT) meet. It allows networked sensors, smart machines, and data analytics to improve business-to-business (B2B) services industries. Such improvements may be from manufacturing to mining to public services. In IIoT, data volumes are very high and hence the term big data. IIoT generally implies machine-to-machine connections, either for application observing or as part of a self-organized system, with a distributed control that does not require human intercession. This kind of monitoring may be in monitoring processes in chemical production plants, production levels, possible breakdowns, and vehicle fleet tracking, to name but a few. In essence, IIoT is about autonomic industrial plants.

Stojmenovic (2014) contends that IoT, in general, is about increased machine-to-machine interactions. They state that it is built on smart devices that have sensors and depend on cloud computing and the network. However, scholars such as Stojmenovic (2014) who generalize IoT to machine-to-machine communication are precisely addressing the IIoT. In CIoT, the consumer is always a participant in the ecosystem. Smutný (2016) ascertains that IIoT has a group of industrial-oriented applications where data volumes and rates are from a sustained to a relatively high level. In IIoT, devices are the machines that operate in industrial, energy, medical or transportation domains.

Moreover, applications in IIoT are safety and mission-critical. That means when something goes wrong, or system fails, the consequences are dire, and could significantly affect the economy or the lives of people. Palattella et al. (2016) highlight that IIoT evolves from a broad base of systems employing machine-to-machine communications for control process automation and monitoring. In this case, IIoT is the aftereffect of the integration of hardwired and often detached islands, usually dependent on semi-proprietary protocols and architectures via the internet. Such a combination amplifies the capability of isolated industrial plants by augmenting their flexibility and manageability and uncovering the chance to deploy new services.

Palattella et al. (2016) stress that the communication requirements of IIoT and CIoT can be different, as far as reliability, latency, inertness, throughput, security and privacy are concerned. CIoT communications are usually machine-to-consumer instead of machine-to-machine as is the case with IIoT. In CIoT, desirable features of networked things are low power consumption, ease of installation, integration and maintenance.

CIoT related applications impose both technical and economic requirements that lead us to conclude that CIoT applications must be within an economic, legal and regulatory context. In other words, the technological frameworks are not enough to address the issues of privacy, security and trust. CIoT applications should achieve a balance of authority between technology, legislation and the social world (Pilkington, 2016; Hashemi et al., 2016). It is for this reason that the literature review explored both the legal and regulatory approaches, as well as the technical approaches to CIoT, among other things. The literature review further discussed different legislative frameworks from different parts of the world to assess how they can contribute to the integrated structure in the South African context. The chapter also argues other theories that helped the researcher explain the CIoT ecosystem and how these theories help in addressing legal and technological challenges of CIoT as far as they relate to data privacy, security and trust. Table 2-1 summarises the differences between IoT and CIoT.

Table 2-1: Difference between IIoT and CIoT (Researcher)

IIoT	CIoT
Heavy Machinery	Wearables
Transportation	Phones and mobile apps
Machine oriented	Consumer-oriented applications
Mostly machine-to-machine interactions	Mostly machine-to-consumer interactions
Automation	Appliances
Used in factories	Home and offices monitoring
Healthcare at Industrial scale	Personal Health
Failure can cost lives	Failure causes inconvenience
Object-object assemblage	Consumer-object assemblage
Improves productivity in factories	Improving the quality of people's lives by saving time and money
Data volumes are high	Data volumes and rates are low.
systems and software that control the machine are safety-critical	The smart devices and applications that control them are not safety-critical
Business-to-business (B2B) services	Business-to-consumer (B2C) services

2.3 Legal and legislative frameworks on CIoT

Roos (2006) state that the main aim of privacy or protection legal instruments is to safeguard personal privacy by regulating the processing of personal data. Such legislations seek to empower people to participate and influence the processing of information about themselves. It would be useful to embed legal and regulatory challenges into constitutional frameworks and human rights. Weber (2010) argues that there is a need for an independent fundamental right of confidentiality and integrity related to info-technical systems. There is a need for a framework at a national and international

level to address all underlying issues. This framework should apply to every object on earth from its becoming to its destruction. Data protection and privacy need communication strategies that establish a sound stage for dialogue between lawmakers, non-governmental organizations, public interest groups and the private sector. Without proper legislation, CIoT becomes impractical and hard to use efficiently. The implementation of IoT architecture and the use of RFID poses several legal and regulatory challenges. The fundamental questions of the agenda are as follows:

- Do we need international or national laws that can monitor the use of CIoT?
- How will such laws affect the South African environment?
- Are existing laws and legislations sufficient to deal with the CIoT issues, or is there a need for new legal instruments?

O'Connor, Rowan, Lynch and Heavin (2017) mention that the informed consent process is becoming a challenge with the emergence of IoT as service providers may collect data without consumers being aware. Consumers of IoT need to be fully aware of what they are consenting to when they register an account with such technological artefacts. CIoT needs to have a framework driven by regulatory bodies to address data privacy, security and trust issues. Legislatures enact laws or acts, and thus legislators are automatic stakeholders when dealing with CIoT challenges. Peppet (2014) acknowledges that scholars and regulators have not given attention to PII issues raised by IoT.

Rose et al. (2015) point out that IoT assemblages and the devices or components of the assemblages raise new regulatory and legal questions as well as amplifies existing legal issues around the internet. The rapid changes in CIoT more often than not outpace the ability of the associated policy, legal, and regulatory structures to adapt. For instance, there are issues around data flowing across borders. We need to address the problems that occur when devices collect data one jurisdiction and transmit it to another jurisdiction — the two jurisdictions most likely different laws for data protection. In addition, the data collected by CIoT devices are susceptible to misuse and thus can potentially cause discriminatory outcomes for some consumers. These unfair outcomes may be from a race, age, gender, and even economic perspective.

Rose et al. (2015) further mention that problems may arise because of conflicting interests between law enforcers. The conflicting interests might be about enforcement surveillance and civil rights, data retention and destruction policies, legal liability for unintended uses, and security breaches or privacy lapses. These legal and regulatory challenges are vast and complex. Despite the broad scope and complexity, there is a dire need for a holistic and integrated framework that promote principles of consumer safety and security, consumers' ability to connect, innovate, share, choose, and trust the CIoT technology.

According to Zimmeck, Wang, Zou, Iyengar, Liu, Schaub et al. (2017), mobile apps have to satisfy various privacy requirements. Apps publishers are often obligated to provide a privacy policy and notify users of their apps' privacy practices. They state that there is a need to have a scalable system to help analyze and predict Android apps' compliance with privacy requirements. Peppet (2014) comments that a lack of attention by scholars and regulators in addressing personal information when it comes to IoT has left the door open for IoT companies to do as they please. For example, IoT service providers define "personal information" and "PII" in a variety of ways in privacy policies and terms of use. He proposes that regulators should first issue guidance to IoT companies concerning the definition and treatment of PII in their privacy policies and their security practices. The proposed framework in this research is for IoT developers, providers, regulators, privacy activists, application publishers and app store owners. These stakeholders may use the proposed holistic framework in their internal assessments of privacy requirement compliance.

In their analysis of free apps, Zimmeck et al. (2017) found that 71% of apps analysed did not have a privacy policy. The applications that had privacy policies had some level of inconsistencies concerning what the apps' policies stated and what the code of the app performed. The authors advise that apps publishers need to identify possible discrepancies before they become prevalent. CIoT service providers often provide mobile apps for free as part of the overall solution. Regulators can benefit from a system that helps them identify potential inconsistencies. The service providers can benefit in their

software development process. Developers may find it challenging to understand privacy requirements and thus end violating privacy laws without knowing. In such cases, as much as the developers had no malicious intentions, they would not want to be on the wrong side of the law. Zimmeck et al. (2017) suggest that writing policies in natural language is the de-facto standard and warn that those policies are often long and difficult to read. Few consumers ever read them, and regulators lack the resources to review them systematically. Massey, Eisenstein, Antón and Swire (2013) evaluated 2,061 policies and focused on their readability and suitability for identifying privacy protections and vulnerabilities from a requirements engineering perspective. They do not look at the legal relevancy part of it. Some first world countries such as the United Kingdom and the United States have started to take action around regulation of the IoT industry specifically.

2.3.1 South Africa

South Africa has some laws that seek to protect consumers, and the researcher explored the extent to which these laws apply to the consumers of IoT. The five most appropriate legislative framework relating to the protection of consumers in South Africa are the:

- Protection of Personal Information Act 4 of 2013 (POPI Act),
- Consumer Protection Act 68 of 2008 (CPA),
- Independent Communications Authority of South Africa Act 13 of 2000 (ICASA Act)
- Electronic Communications and Transaction Act 25 of 2002 (ECT Act)
- Electronic Communications Act 36 of 2005 (ECA)

2.3.1.1 Protection of Personal Information Act

The POPI Act exists to guarantee that all South African institutions responsibly behave themselves when collecting, processing, storing and sharing other people's information. The Act ensures this by holding the institutions accountable should they abuse or compromise people's data in any way. Katuu and Ngoepe (2015) acknowledge that South

Africa's legal and regulatory environment has a long history that comes with its complexity. They mention the fact that public institutions in South Africa have to comply with several legal and regulatory provisions that relate to the management of records. How can these statutory and regulatory provisions be used when it comes to data privacy, security and trust in mobile apps and IoT?

The enactment POPI Act considers personal information valuable and therefore aims to bestow upon the people certain rights concerning their data. The owner of the data should be able to exercise control over their personal information (De Bruyn, 2014). The following summarizes the aim of the Act:

- when and how a person decides to share his or her data (requires consumer consent)
- the type and degree of data the person chooses to share (must be collected for legitimate reasons)
- transparency, responsibility and accountability on how the person's information will be utilized (restricted to the purpose) and warning if or when the information is used for the wrong reasons
- providing the person access to their data and the right to have the personal data removed and destroyed should the person wish to do so
- who can access the personal data, that is, there must be sufficient measures and controls set up to track access and prevent unauthorised people, even inside a similar organization, from accessing their data
- how and where personal data is stored (there must be satisfactory measures and controls set up to shield private data from theft, or being undermined)
- the integrity and accuracy of personal data (for example, personal data must be captured correctly once collected, the institution must look after the personal information in a responsible manner)

The South African POPI Act, Canadian PIPEDA and the European GDPR are data protection laws that make provision for accountability as a principle. These laws give people control over how businesses collect and process their information. The South

African government created the POPI Act to promote the constitutional right to privacy by safeguarding PII. The Act tries to guarantee that all South African institutions behave responsibly when collecting, processing, storing, and sharing another entity's personal information by holding them accountable, should they abuse or compromise that entity's personal information in any way.

Even though the authorities enacted the POPI Act in 2013, it is only coming into effect in 2020. The enforcement of the law delayed since to allow the establishment of the regulatory bodies (Staunton, Adams, Anderson, Croxton, Kamuya, Munene et al., 2020). Table 2-2 below compares the POPI Act to international laws on privacy discussed later in this section.

Table 2-2: Comparing the POPI Act to other international laws (Botha, Grobler, Hahn and Eloff, 2017)

Country	Act	PoPI Principles								Other Areas					
		Accountability	Processing Limitation	Purpose Specification	Further Processing Limitation	Information Quality	Openness	Security Safeguards	Data Subject Participation	DPO Required	Breach Notification	Cross-border Data Transfer Limitations	Electronic Marketing	Online Privacy	Enacted Year
South Africa	PoPI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		2013
Australia	PA		✓	✓		✓	✓	✓	✓	✓		✓			1988
Canada	PA / PIPEDA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	2000
Europe	EU DPD		✓	✓	✓	✓	✓	✓	✓	✓		✓			1995
Europe	GDPR	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	2016
UK	DPA		✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	2000
USA	*		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	*

The researcher summarized the eight POPI Act principles in Table 2-3.

Table 2-3: POPI Act principles

	PoPI Principle	Description
1	Accountability	The party in question, which means the individual or entity processing the data, must guarantee that they adhere to all the eight principles
2	Processing Limitation	The processing of the data should happen lawfully or legally.
3	Purpose Specification	There should be a lawful reason for collecting the data, and the subject should be aware of this reason
4	Further Processing Limitation	Any further processing of the data must be aligned with the first reason for collecting it.
5	Information Quality	The data must be complete, accurate and not deluding. If need be, the data may be updated while considering the original reason for collecting the data.
6	Openness	Transparency should exist, which means the Information Regulator must be advised before any data handling happens. The processing of data ought to be noted in a register, and the data subject ought to be told that information was gathered about them.
7	Security Safeguards	The trustworthiness of collected personal data ought to be kept up.
8	Data Subject Participation	The data subject has the right to solicit and to be given free of charge any data that the party in question may have.

2.3.1.2 Consumer Protection Act

The protection of consumers is of vital importance in any market. South Africa enacted the CPA to deal with the need to protect consumers (GOV.ZA, 2009). When consumers of IoT suffer financial losses, or identity theft because of improper business practices, the laws of the country need to protect them. Carlin, Gervais and Manso (2010) state that improper business practices may include habits like misleading information, advertising, direct marketing, use of inferior products and unclear instructions on how to use the services. These practices apply to any business venture in the supply chain of delivering the service. In CIoT, the service providers may over-promise regarding what the service is capable of doing or its ability to provide security concerning consumers' information. The providers may also use consumers' information for advertising and marketing purposes without the consent of the consumers. The use of inferior devices that the regulator like ICASA or SABS has not approved poses a threat to data privacy and security of the consumers. Inferior products may also come with unclear instructions on how to use the product or service. All these may be detrimental to the consumers, and thus the law needs to protect the consumers against businesses that focus on profit at the expense of the consumers.

Is CPA enough to protect consumers of IoT in South Africa? According to Jacobs, Stoop and Van Niekerk (2010), the Act currently gives a broad structure for consumer protection. It expects to create, enhance and protect the rights of the consumer while eliminating unethical suppliers and improper business practices. The Act has codified certain areas of the common law regarding consumer rights and the Act now governs certain unfair business practices that were previously unregulated. The United Nations Guidelines for Consumer Protection (UNGCP), adopted in 1985 and revised in 1999, proposed a list of objectives described as 'legitimate needs'(UNCTAD, 2016):

- right to be heard
- right to information
- right to safety
- right to choose

- right to consumer education
- right to consumer redress
- freedom to form consumer groups
- promotion of sustainable consumption patterns
- and development of the economic interests of consumers

A few of these objectives seem to have found their origins in human rights — for example, the right to safety, which echoes the Universal Declaration of Human Rights. Ukwueze (2016) argues that there is a need to elevate human rights to consumer rights. A worry for human weakness is at the centre of expanding resonance of calls for a robust framework for consumer protection. While all these declarations were born before the existence of IoT, they remain applicable in our days. Their applicability is based on the premise that the protection of consumer information is not just about protecting human life, but also for maintaining human dignity. Some big corporates can easily take advantage of consumers' data, and thus, the laws that can protect consumers against big corporates are of the utmost importance.

Ukwueze (2016) suggests that even though the Bill of Rights in the Constitution of the Republic of South Africa, Act 108 of 1996 does not explicitly mention consumer rights (RSA, 1996), some of the fundamental consumer rights in the CPA can be viewed as extensions of human rights (GOV.ZA, 2009). Ukwueze (2016)'s argument is based on the premise that both human rights and consumer rights rest on similar interests, namely equality, justice and solidarity. Those rights are not strictly constitutional rights since the constitution does not guarantee them. However, those are still enforceable by law. The CPA defines the term 'consumer' concerning a person that consumes particular goods or services and has entered into a transaction with the supplier (GOV.ZA, 2009). The supplier would have to market to such a person, and the person entered into a deal with a supplier. This definition is broad to cover other stakeholders involved in the CIoT space. The researcher is of the view that the CPA and the POPI Act are too broad and subject to various interpretations.

Ukwueze (2016) states that the goal of the law in consumer protection is to prevent harm or injury to and provide redress for the consumer where he or she suffers damage or injury in his or her relationship with the producer or supplier of goods and services. In South Africa, the CPA derive from the International Bill of Rights and cover the rights contained in UNGCP. The CPA recognises, in more specific terms, the fundamental rights of consumers as follows (GOV.ZA, 2009; Jacobs et al., 2010):

- Right to equality in the consumer market and protection against discriminatory marketing practices; Right to privacy;
- Right to choose;
- Right to disclosure of information;
- Right to fair and responsible marketing;
- Right to fair and honest dealing;
- Right to reasonable, just and sensible terms and conditions;
- Right to reasonable worth, high quality and security; and
- Right to accountability by suppliers.

Customer rights are about the people using safe products, services, reasonable exchange of goods and services, and access to justice. These rights focus on the upkeep of human pride and prosperity in the marketplace. Imbalance of bargaining power decreases the consumer's capacity to negotiate through fair market conditions and undermines their autonomy. Big businesses do not generally negotiate on equal terms. In this manner, we can presume that consumer rights encapsulate the three principal qualities of human rights namely universality and full recognition, improvement of individual well-being and protection against powerful governments or groups, which constitute the ingredients for the substantive tests for the realisation of human rights. We need to recognise that consumer rights are human rights.

2.3.1.3 Independent Communications Authority of South Africa's enacted legislations

According to the Independent Communications Authority of South Africa (ICASA), referred to as the "Authority" by law, their primary responsibilities relate to licensing, consumer protection and telecommunication numbering. ICASA's mandate is to perform a consumer protection role and to advance the interests of consumers of electronic communications in general. This mandate is articulated in the ICASA Amendment Act No 3 of 2006 (GOV.ZA, 2006). However, the question arises as to the extent to which this law can protect the consumers of IoT. According to Solutions (2012), ICASA has not, in general, been useful in the role of protecting consumers.

ICASA legislation empowers ICASA to grant licences, monitor licensee compliance with licence terms and conditions, develop regulations, plan and manage the radio frequency spectrum, and protect consumers (GOV.ZA, 2006). In addition to the ICASA Act is the Electronic Communications Act 36 of 2005. Section 35 (1) of this Act states that (GOV.ZA, 2005),

> *"No person may use, supply, offer for sale or lease or hire any electronic communications equipment or electronic communications facility, including radio apparatus, used or to be used in connection with the provision of electronic communications, unless such equipment, electronic communications facility or radio apparatus has, subject to subsection (2), been approved by the Authority".*

Both the ECA and ECT Act fall under the ICASA mandate. However, Solutions (2012) states that ECA is pro-competitive legislation, and the ECA is not for protecting consumers but for ensuring that there is fair competition amongst service providers and that South African networks use only approved devices. The researcher explains the content of the ECA here to clarify how it differs from the ECT Act. The ECA states that the Authority must authorise all wireless technologies. That means all devices that operate in CIoT on the South African market need to undergo "Type Approval" from the Authority. The ECA defines Type Approval as a process through which the Authority

authorises equipment or a device or system to use in South Africa or imported into South Africa. The process involves verification of the equipment's compliance with the applicable standards and other regulatory requirements (GOV.ZA, 2005). CIoT devices that have undergone this verification may help in curbing some of the challenges of CIoT. However, many hobbyists in the market import devices without following the process of “Type Approval”. These unapproved devices still connect to the rest of the internet.

The Authority works with established technical standards with which the device must conform. These standards may be international, regional and national. The Authority makes a list of these standards in the Technical Regulations defined in the Type Approval Regulations (GOV.ZA, 2005). In 2016, the Authority signed a memorandum of understanding with the South African Bureau of Standards (SABS) to collaborate regarding the Type Approval Framework. The ECA Act states that any device utilized or to be utilized regarding the provision of electronic communications correspondences except if unequivocally absolved by the Authority is liable to Type Approval by the Authority. The Authority should provide the Type Approval Certificate only to South African registered companies. The following stakeholders in CIoT can apply to the Authority for Type Approval:

- Manufacturers
- Importers
- Distributors

Therefore, we should not confuse the ECA with the ECT Act. There is a clear distinction in content between the ECA and the ECT Act. The ECA focuses more on competition, and the ECT Act focuses on the consumer-supplier relationship. The ECT Act includes the essential elements related to the study on data privacy. The ECT Act looks at the devices that may be used for communication purposes across different competitors. The chapter on consumer protection on the ECT Act states that the principle of collecting personal information as follows (GOV.ZA, 2002):

- A data controller must have the consent of the data subject for the collection, gathering, processing or disclosure of any personal data on that data subject

- A data controller may not electronically ask for, collect, examine, process or store individual data on a data subject, which is no longer required
- A data controller must have the consent of the data subject for the collection, processing or disclosure of any personal data on that data subject
- The data controller must disclose to the data subject in writing the particular reason for which any personal information is being requested, collected, collated, processed or stored
- The data controller may not utilize the personal information data for some other reason than the disclosed purpose without the written authorization of the data subject
- The data controller must keep a record of personal information for whatever length of time that the personal information is utilized for and the purpose for which the personal information was collected
- A data controller may not disclose any of the personal information held by it to an outsider, except if required by law or explicitly approved by the data subject
- The data controller must delete or destroy personal information is out of date
- A party controlling personal information may utilize that personal information to incorporate profiles for statistical purposes and may openly exchange with such profiles and measurable knowledge, as long as the profiles or statistical information cannot be connected to a particular data subject by an outsider

In addition to the provision of collecting personal information, the ECT Act seeks to protect the consumer when transacting with the service provider. Some of the rules that seek to protect the consumer are as follow (GOV.ZA, 2002):

- A customer has a right to drop any transaction exchange and credit agreement for the supply of goods or services inside seven days after the date of the receipt of the products or services without reason or penalties.
- An entity that sends unsolicited commercial communications to consumers must provide the consumer with the option to cancel the subscription to the mailing list

- An entity that sends unsolicited commercial communications to a consumer despite having received a warning that such interchanges are unwelcome is blameworthy of an offence and subject, on conviction to the punishments.
- A consumer may complain with the Consumer Affairs Committee in respect of any non-compliance with the provisions of the law by a supplier.

Other regions around the world have been hard at work trying to catch up with technologies and devising new laws to manage the challenges that come with technological advancements. The researcher chose the regions that have actively taken action in regulating their online technological developments. The researcher further looked at the investments from these regions to South Africa. For example, Ncube (2006) state that the EU is the largest source of investment for South Africa and accounts for almost half of South Africa's total foreign trade

2.3.2 International privacy legislation

South Africa developed most of its legislations following some of the first world's approaches. The next subsection discusses some of the international laws enacted in various countries to deal with rights to privacy.

2.3.2.1 European Union – General Data Protection Regulation

While the General Data Protection Regulation (GDPR) is not specific to IoT, there are significant clauses that apply to IoT. There are many similarities between the South African PoPI Act and the EU GDPR. Many scholars and literature (Botha et al., 2017; De Bruyn, 2014; SouthAfrica, 2013; Staunton et al., 2020) agree that South Africa developed the POPI Act with a lot of input from the GDPR. The European Commission raised some concerns concerning data privacy, security and trust issues related to RFID and IoT (Da Xu, He and Li, 2014). The implementation of IoT architecture and the utilization of RFID poses various legal and regulatory difficulties. It is because of such concerns that the commission invited member states in 2009 to provide direction on the design and

operation of RFID applications in a legitimate, moral, socially and politically acceptable way, respecting the right to privacy and guaranteeing protection of personal data (Weber, 2010). The recommendation was about the implementation of privacy and data protection standards in applications bolstered by RFID. It outlined the measures that EU member states need to take in the deployment of RFID application to guarantee that national enactment is in agreement with the EU Data Protection Directive (DPD). According to Birnhack (2008), Europe had DPD from 1995. The implementation of the DPD took place in 2000 to ensure that the industry and the relevant civil society can collaboratively develop a framework for privacy and data protection impact assessments (PIA) (Weber, 2015). The objectives of the PIA were to identify the implications of the application of privacy and data protection. Apps that might raise security threats need to be submitted by member states and document the consequences they may have to the public (Weber, 2010).

Following the 2009 recommendation and the latest requirements of the EU data regulation legislation, this directive underwent revision in 2015 to come up with the GDPR, which came into force in May 2018. The DPD defined personal data as data such as names, photos, email addresses, phone numbers, addresses, and own identification numbers (social security, bank account, etc.). On the opposite side, the GDPR defines personal data as any information that others could use, on its own or in conjunction with other data, to identify a person. Such data includes IP addresses, mobile device identifiers, geolocation and biometric data (e.g. fingerprints, retina scans). The GDPR additionally covers data identified with a person's physical, psychological, hereditary, mental, economic, cultural, or social identity. The most significant change in the GDPR is the meaning of personal data. The GDPR reflects changes in technology and the ways that organizations collect data about people. Overall, businesses see the changes as a good step for privacy but bad for existing marketing and sales techniques. Profiling, or building up a preview of a person's inclinations utilizing purchase history is no longer acceptable under the GDPR except if the person concerned has unequivocally agreed.

The GDPR tries to address current difficulties identified with personal data protection and to harmonise data protection across the EU. It seeks to benefit companies by offering consistency in data protection activities and liabilities across the EU countries and empower progressively coordinated EU-wide data protection policies. Tikkinen-Piri, Rohunen and Markkula (2018) ascertain that GDPR requires a lot of money and human resources to implement and train employees. The authors allude that businesses need guidance to support them in this transition, and an integrated framework will assist these companies in complying, especially when they are involved in consumer IoT in one way or another. Businesses have been caught off-guard as far as these changes are concerned and lack the awareness of the necessities and the GDPR's coercive measures. South Africa deals with a lot of companies from Europe, and thus those companies must understand and comply with the GDPR when dealing with data management and usage practices in the age of CIoT.

The European Union wanted to discontinue default passwords for IoT devices through a new technical specification named TS 103 645 (ETSI, 2019). The specs called for device manufacturers to ban the utilization of default passwords for consumer devices that connect to the internet, and to make it easy for consumers to delete their data. There are various incidents in which system vulnerabilities compromised IoT devices, and the most eminent one was the Mirai botnet in 2016. Researchers concur that the full surface area of IoT represents a cybersecurity risk because of its amorphous nature, with different connected devices communicating through a largely unsecured wireless protocol.

While the above initiatives are commendable, the European Commission has been facilitating the embracement of IoT over the last few years. The new IoT initiative by the commission is more specific to the technology and aims to realize the full potential of IoT in Europe. The commission intends doing this by adopting a set of supporting policy actions and launching a series of relevant initiatives. In March 2015, the commission found the Alliance for Internet of Things Innovation (AIOTI) (ENISA, 2017). This body aims to create an innovative and industry-driven European IoT ecosystem. The commission intends to work very closely with all IoT stakeholders on establishing a

competitive IoT market and new business models to benefit the citizens of Europe and businesses.

2.3.2.2 The United Kingdom Laws

The United Kingdom government is one of the first governments to be specific in addressing IoT issues. In October 2018, they passed the IoT voluntary Code of Practice (COP) for consumer IoT that endeavoured to arrange all best practices in one place. Besides, the COP requires that IoT device manufacturers must provide a point of contact so that consumer know who to contact in cases where they need to enquire about the security of their devices. There is also vulnerability disclosure, whereby manufacturers need to state the minimum length of time for which the device will receive security updates. The vulnerability disclosure aims to inform consumers about the length of time it is considered safe to use a device. After the initial base period, the device would turn into a ticking time bomb, fit for being misused by hackers. Moreover, they presented another draft law that requires certain cybersecurity features to be incorporated with IoT products and marked on the package.

The UK government is also trying different label designs for IoT security. They want a compulsory labelling scheme that would tell consumers exactly how secure their smart devices genuinely are. When the service provider affirms the final label, the onus would be on the retailers to ensure that there is a proper conveyance of the message to the consumers. The retailers would have only to sell smart devices that have security labels. These different iterations of IoT security laws allude to a fundamental concept of "secure by design" that is turning out to be progressively standard. What this implies in practice is that security ought to be something that is incorporated into the product long before the production phase.

Conversely, in the present digital culture, it appears as though security features are grafted on at the end rather than designed into the product from the very beginning. By the time a product reaches a production phase, it would have reached a point of no return

concerning security. Before COP, the UK adopted the Data Protection Act (DPA) in 1998. However, the implementation of both the UK DPA and the EU DPD happened in 2000.

2.3.2.3 American laws on privacy

Peppet (2014) suggests that California's Office of Privacy Protection leads among the states in setting out recommended practices on privacy policies. The California Online Privacy Protection Act of 2003 (CalOPPA) requires that companies that operate an online service and collect PII must post a privacy policy, through sensibly open methods for making the privacy policy available to online consumers. Zimmeck et al. (2017) include Delaware Online Privacy and Protection Act (DOPPA) and state that both CalOPPA and DOPPA require online services that collect PII to post a policy. The policy must distinguish the categories of PII gathered and the kind of external stakeholders with whom the organization shares data. The guidelines from both acts require companies to include in their privacy policies information of how they collect personal information, the type of personal information they gather, how they use and share such information with others, and how they secure the data. Botha, Eloff and Swart (2015) define PII as any data that can be used to identify a specific individual. This definition is broad and creates security and privacy challenges, and hence the specific and stringent safeguards for it are spelt out in regulations such as the GDPR in Europe and the POPI Act in South Africa.

Zimmeck et al. (2017) are worried about the policies around mobile apps and mention that there is no commonly relevant government resolution demanding privacy policies for apps. They express that California and Delaware enacted comprehensive online privacy legislation that effectively serves as a national minimum privacy threshold given that app publishers usually do not provide state-specific app versions or exclude California or Delaware residents. Peppet (2014) states that companies dealing with IoT trigger CalOPPA's requirement to have a privacy policy. Such companies are in one way or another, maintaining or operating an online service. The companies need to disclose the types of PII collected and the categories of third parties with whom they share that PII.

According to Zimmeck et al. (2017), CalOPPA and DOPPA further demand that privacy policies describe the process through which service providers notify people of policy changes. They also mention that the Children's Online Privacy Protection Act of 1998 (COPPA) makes policies compulsory for apps directed to children. While COPPA requires the description of access, edit, and deletion rights, in both CalOPPA and DOPPA, such rights are optional. In addition to CalOPPA, the California state signed into law the California Consumer Privacy Act (CCPA) in June 2018, which took effect in January 2020. The CCPA gives a unique insight into the trend towards data protection throughout the world and into how that trend is influencing laws inside the United States (Palmieri III, 2020). However, Palmieri III (2020) is critical of the CCPA and states that it contains a myriad of uncertainties, and the authorities passed the law hastily. Despite the criticism, it is a ground-breaking law which will have ramifications throughout the United States.

In addition to all the privacy-related laws in California, it became the first state to pass an IoT security law, which came into effect on 01 January 2020. It is the first IoT-specific security law in the United States. The IoT Security law and the CCPA seek to put new responsibilities and restrictions on companies for privacy and data security. The IoT security law requires all IoT devices sold in California should be equipped with reasonable security measures such as the following:

- No use of default passwords on IoT devices. That means all IoT devices should have unique passwords
- Devices should have certain protections that prevent consumers from switching them back to factory-ready default settings

Congress has also been hard at work after the 2016 botnets attacks. The United States Senate and House of Representatives introduced the Internet of Things (IoT) Cybersecurity Improvement Act of 2019 (Brown, Dawson and Seessel, 2019). According to Warner, Gardner, Wyden and Daines (2017), the Act seeks to make sure the federal government does not buy devices that criminals can hack easily. The legislation does not include security standards for IoT companies across the board. The law is for the companies that sell to the federal government. The federal government is a huge

customer. The legislation hopes that by improving security standards for the federal government, the criteria would improve for the entire IoT market.

Furthermore, the IoT Cybersecurity Improvement Act seeks to establish standards for federal government agencies that purchase IoT devices for use by the federal government. The proposed law would call on the National Institute of Standards and Technology (NIST) to develop standards that address secure development, identity management, patching, and configuration of IoT devices. The NIST would also guide the federal government on policies and procedures about IoT device security vulnerabilities and the resolution of such exposures. The guide would cover reporting, coordination, publishing, and receipt of information (Warner et al., 2017; ENISA, 2017). These requirements are such that IoT devices,

- do not contain known security vulnerabilities or defects
- rely on software or firmware components capable of accepting authenticated and trusted updates from the vendor
- rely only on non-deprecated industry-standard protocols and technologies for specific functions
- do not include fixed or hard-coded credentials

Brown et al. (2019) highlight that the IoT Cybersecurity Improvement Act of 2019 is different from California's SB 327 that lawmakers passed in September 2018. California's law requires explicit safety efforts that IoT device manufacturers need to obey. The IoT Cybersecurity Improvement Act of 2019 requires that there should be no default passwords, and consumers should create their passwords. Whenever passed, the federal IoT security bill would require recommendations from the NIST on security standards that the central government ought to follow. The NIST would likewise review that policy like clockwork, as per the law. All IoT merchants that sell to the US government would also have a vulnerability disclosure policy so that government authorities can learn when the devices they are utilizing are open to cyberattacks. The government introduced a similar enactment in 2017. The 2017 rendition, in any case, included explicit prerequisites such

as password management and software updates which are absent in the 2019 law (Warner et al., 2017; Fowler, Goel, Hodges and Miller, 2019).

California's new law determines the security commitments of manufacturers of IoT devices. A manufacturer may be a company that manufactures or agrees with someone else to manufacturer IoT devices sold or offered for sale in California. Therefore, the law will apply to manufacturers outside of California if they want to sell their items in California. Under the new law, the manufacturer of an IoT device must equip the device with a sensible security feature that is (Brown et al., 2019),

- appropriate to the device's nature and function
- applicable to the data that the device may gather, contain, or transmit
- designed to secure the device and any of its data from unapproved access, pulverization, use, disclosure, or alteration

Brown et al. (2019) criticize California's new law to be sweeping in scope. However, the authors acknowledge that there are a few protections and exceptions. (Clayton, Evans, Hazel and Rothstein, 2019) recommend that in light of the breadth of the law and the specific nature of the exemptions, manufacturers may need to insure themselves against products liability for products that manufacturers wish to sell in California. Manufacturers also need to seek clarity on which products will be subject to the new law and thus ensure that sensible security features are in place. Alternatively, Clayton et al. (2019) advise that manufacturers develop expanded or reinforced exclusionary language.

2.3.2.4 Canada and Australia

Canada has two federal laws, namely, the Privacy Act (PA) and the Personal Information Protection and Electronic Documents Act (PIPEDA). The PA covers personal information-handling practises of federal government departments and agencies. On the other hand, the PIPEDA is for the Canadian federally regulated private sector only (Bryman, Bell, Mills and Yue, 2011). Both the PA and PIPEDA govern electronic marketing in Canada. In

addition, there is Canada's Anti-Spam Legislation (CASL). Having so many legislations to address PII might come with challenges.

Another point worth noting outside North America and Europe is that of Australia. Botha et al. (2017) allude that data protection in Australia is at present a blend of Federal and State or Territory enactment. Each territory has its data protection legislation applying to state government agencies. Australia permits the cross-border transfer of data, but the sending agency or organisation remains primarily accountable for that personal information.

2.4 Technological considerations

This section discusses existing technologies that work with and influences IoT. These technologies may contribute negatively or positively to the concerns of data privacy, security and trust.

2.4.1 Existing technologies

The fulfilment of customer privacy requirements can be a daunting task. More often than not, we go on with our daily lives without thinking about data privacy, security and trust issues. Several technologies exist that seek to achieve information privacy goals. The technological approach explores technological steps that stakeholders can take to protect consumer data.

Another technology that is worth exploring while developing the framework is the blockchain technology. Crosby, Pattanayak, Verma and Kalyanaraman (2016) define blockchain as a distributed database of records. This distributed database of records consists of public ledgers of all transactions or digital events that the system has executed and shared among participating parties. Zyskind and Nathan (2015), state that the blockchain technology or distributed ledger technologies come with promises to express

and establish shared trust in information created and exchanged by smart things and people. While blockchain applications may ascribe all authority to the blockchain, IoT applications should achieve a balance of power. The economic, legal and regulatory context extends beyond the blockchain technology.

Interacting devices in the IoT assemblage reside at the edges, and this is where IoT data is generated and acted upon (Ouaddah, Abou Elkalam and Ait Ouahman, 2016). Ensuring that information is trustworthy is hard enough when a central authority orchestrates device configuration, data collection and cleaning, and data dissemination. However, distributed networks like those using the blockchain technology do not rely upon a central authority.

Biswas and Muthukkumarasamy (2016) propose a security framework based on blockchain technology that allows communication between entities in a smart city without compromising privacy and security. Figure 2.1 shows some entities or building blocks that make up a smart city.

Figure 2.1: Building blocks or entities that make up a smart city (Zigurat, 2019)

Biswas and Muthukkumarasamy (2016) conclude that the main advantage of using blockchain is that it is resilient against many threats. In addition to the resilience against the risk, they ascertain that it provides several unique features such as improved

reliability, better fault tolerance capability, faster and efficient operation, and scalability. The resilience is in its distributed nature. Figure 2.2 shows how blockchain achieves the resilience from many threats.

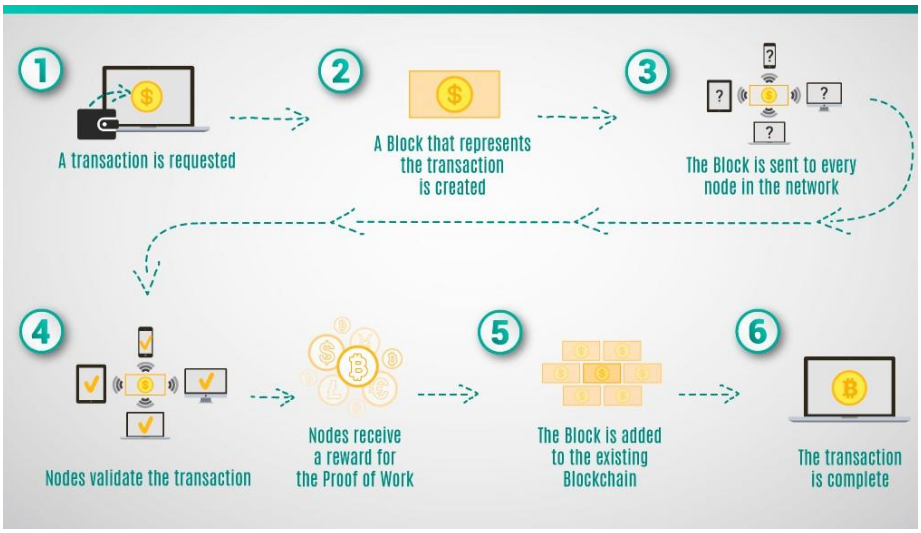


Figure 2.2: The workings of Blockchain technology (Lastovetska, 2019)

The integration of blockchain technology with devices in an IoT ecosystem should create a common platform where all machines would be able to communicate securely in a distributed environment and thus curb security threats and privacy. This security framework covers four layers, namely, an interface layer, database layer, communication layer and the physical layer. Technicity is an essential basis for the development of rules protecting privacy objectives. Several varied points can be taken into account, namely (Weber, 2010):

- the complexity of the tag (active and passive, rewritable, processing and sensor provided products),
- the complexity of background devices (reader or other linked media) and the maximum reading range which is designed primarily to cover transparency demands

2.4.2 Design and development considerations

O'Connor et al. (2017) mention that designers and developers of IoT should consider an integrated framework with practical approaches when designing and developing IoT for data collection and data sharing. Rose et al. (2015) suggest that as a matter of principle, developers, designers, and all stakeholders of IoT devices and systems must guarantee they do not expose consumers to potential harm. Such an obligation means that all stakeholders need to address the data privacy, security and trust issues from a technical perspective, in addition to regulatory frameworks, as they contribute in the development of the CIoT assemblage. A collaborative approach between the stakeholders to data privacy, security and trust are needed to develop effective and appropriate solutions that are well suited to the scale and complexity of the issues.

Babar et al. (2011) propose a hardware and software design methodology that can help designers and developers to deliver more secure devices. They suggest that the concept of security architecture in IoT should be about utilizing security mechanisms and protocols effectively. The CIoT assemblage can be attacked from any layer of the system, including the physical or device layer and application (software) layer. A cost-effective design uses a mixture of hardware and software to accomplish overall security goals. The level of security within the device varies depending on the nature of the protected content and kind of application.

The starting point is a design that takes data privacy, security and trust into consideration from the requirements gathering to maintenance following the software development life cycle. From a technical point of view, Babar et al. (2011) mention the following as the key features of the security framework and architecture:

- **Lightweight cryptography:** Upgraded Cryptographic algorithms and equipment design for low power, memory and processing necessities. The IoT industry needs to work extra hard to create lightweight cryptographic algorithms that can work inside the limits of a specific electronic device. The fundamental nature of a large

number of electronic devices in CIoT makes them unequipped to process current cryptographic algorithms, and hence the requirements for lightweight cryptographic algorithms. Lightweight cryptography requires fewer resources from the devices and take less effort and time to finish their fundamental procedures. Utilizing expensive heavyweight weight solutions for each little IoT device would likewise make the expense of devices unfeasible to implement. Lightweight cryptography would thus work better to verify the delicate information transmissions happening each second on the IoT.

- **Physical security:** Trusted Platform Module (TPM) considers the vulnerabilities of the electronic equipment at a physical level. TPM protects your information with an algorithm that integrates into the hardware device. It gives a more elevated level of security than software alone and shields personal data from thieves, malware and hackers. This protection is particularly significant in IoT devices to safeguard the CIoT assemblages. TPM is broadly acknowledged as the most secure technique for ensuring the safety of the data residing in electronic devices. The design ought to give physical protection to secret keys by keeping the parts like secure ROM (Random Access Memory), which is dealing with the secret keys, inside the protected SoC (System on Chip).
- **Standardized security protocols:** This is about the development of standardized protocols which are both lightweights concerning communication and cryptographic computations. The standardization of protocols is to achieve consensus between different stakeholders of a CIoT assemblage. These stakeholders may include device manufacturers, software developers, and network providers.
- **Secure operating systems:** Rich operating systems with a reliable and stable kernel, guarantee a safe communication inside the processor by giving a safe runtime execution condition, secure booting, protected content, among other things. The Secure Bootloader ought to guarantee that the device boots up with the original operating system OS or firmware with right process privileges. Secure ROM, secure runtime execution condition, a secure memory management unit is the prime focus for inbuilt security. Additionally, the operating system with

fundamental security functionalities, secure kernel interface and compatible standardized security protocols for IoT framework contribute towards the security design of IoT.

- **Future application Areas:** It is essential to understand areas that may form part of the assemblage in the future. If service providers envisage future applications, they can take appropriate security measure in the present and not be caught by surprise later on. This area is about understanding the technical, economic, social context of a given application area, to create security solutions which are appropriate and acceptable.
- **Secure Storage:** Personal information may reside in the cloud and the devices. Some of the information may be cached, in RAM or ROM, and even in secondary storage. Regardless of where the data resides, its protection is vital as it may be susceptible.

2.4.3 The architecture of consumer IoT

This part of the research addresses the elements and architectures that have been developed by various scholars. Figure 2.3 below summarizes the high-level design of IoT functions and lays the groundwork of the CIoT structure:

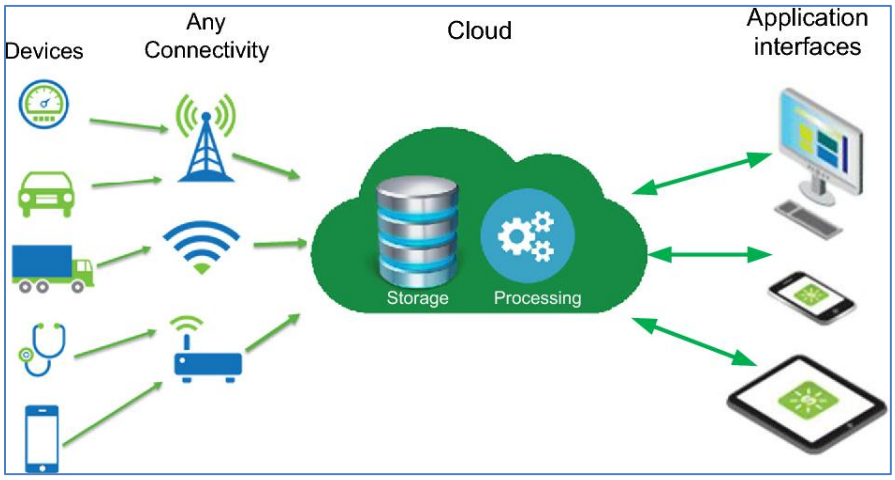


Figure 2.3: Architecture of how IoT functions (Tomovic, Yoshigoe, Maljevic and Radusinovic, 2017)

The study discussed several types of possible attacks in an IoT ecosystem, and the framework incorporates possible attacks. There are several potential ways that a hacker can access features or data on a connected device. Subashini and Kavitha (2011) identify three main target hacking points, namely: the device, the cloud infrastructure, and the network.

Another way of looking at a CIoT assemblage is in a layered format. The security framework summarized in Figure 2.4 covers four layers proposed by Biswas and Muthukkumarasamy (2016), namely, interface layer, database layer, communication layer and the physical layer.

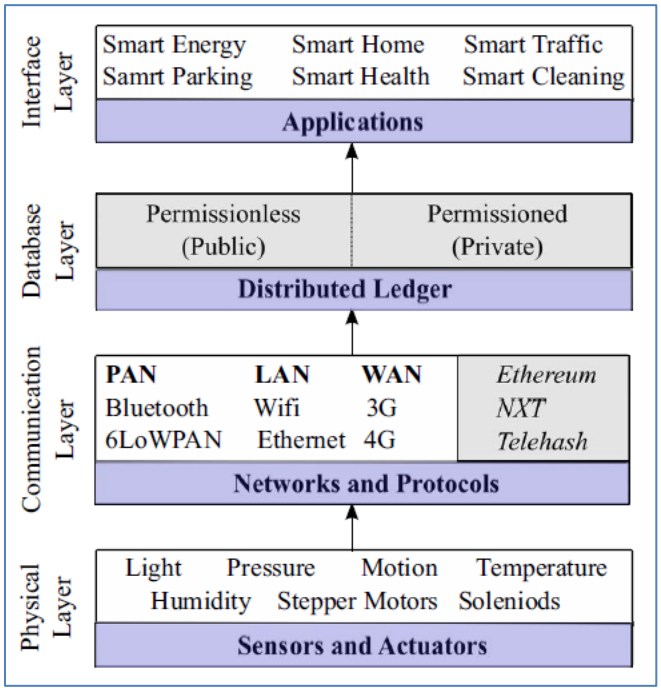


Figure 2.4: Security framework (Biswas and Muthukkumarasamy, 2016)

The next section considers the layered approach used in this study. This study looks at three layers, namely, the application layer, the device or physical layer, and the network layer.

2.4.4 A layered approach to the architecture

Much research is being done to provide a reliable well-defined security architecture that can ensure the confidentiality of data security and privacy. Most scholars have approached IoT security frameworks from a technical point of view using multiple layers. Babar et al. (2011) mention possible attacks that can happen in an IoT assemblage and classify them according to the following; physical attacks, software attacks, network attacks, side-channel attacks and cryptanalysis attacks. Since mobile apps are a type of software, interacting with the physical devices over a network, it is no doubt that these attacks can come in many forms within the IoT ecosystem.

Zhang and Qu (2013) propose a security framework using four layers, namely, perception layer, network layer, middleware layer and application layer. On the other hand, Biswas and Muthukkumarasamy (2016) propose a security framework based on blockchain technology that allows communication between entities in a smart city without compromising privacy and security. The latter scholars' framework is also based on four layers, namely; interface layer, database layer, communication layer and the physical layer. Tiwary et al. (2018) ascertain that the following are essential elements required to build an IoT ecosystem:

- Hardware components such as sensors and actuators
- Middleware components such as a database for storage and data analytical tools
- Visualization through different applications

The technical approaches taken by different scholars have mobile apps in at least one of the layers. Some scholars call the layer where mobile apps exist an application layer (Zhang and Qu, 2013). Others refer to it as an interface layer (Biswas and Muthukkumarasamy, 2016). The researcher discussed the layered approach considered in this research below:

2.4.4.1 Applications and consumers layer

Some scholars introduce another layer and call it the middleware layer (Zhang and Qu, 2013). In this research, the researcher views the middle-ware layer and the application layer as one layer. The applications and consumers are actors of the same ontological footing in this research and thus operate at the same level. Biswas and Muthukkumarasamy (2016) refer to the application layer as the interface layer. According to Zhang and Qu (2013), this layer realizes various practical applications of IoT based on the needs of consumers in different types of industries such as Smart Home, Smart Environment, Smart Transportation and Smart Hospital.

Zhang and Qu (2013) further state that this layer consists of the information processing system that takes automated actions based on the results of processed data and links the system with the database, which provides storage capabilities to the collected data. At the application layer, there is the job of acquiring, storing, analysing and processing of data. This layer is service-oriented and ensures the same service type between the connected devices. In addition to mobile apps, this layer also includes data storage technologies like cloud computing, ubiquitous computing, intelligent processing and mega databases. Tiwary et al. (2018) mention visualization part of the CIoT assemblage as the mobile apps used by consumers to access the analyzed data. The visualization part is at the application layer of the CIoT system. In some cases, consumers use a different mobile app for viewing analyzed data, and another one for communicating and controlling smart devices. The security challenges of this layer include Unauthorized Access, DoS Attack, Malicious Insider, Spear-Phishing Attack and Sniffing Attack.

As the exchange of data happens between different entities like databases and applications, it is exposed to all kinds of attacks before it gets to the consumers of the information. Security threats can be from within the layer through mainly unauthorized access, theft of data, the supply of fake data, worms and viruses. Pomponiu (2012) mentions that CIoT service providers use Access Control Management Privacy protection to improve security in the application layer.

Software Attacks at the application layer are a significant source of security vulnerabilities. Software attacks take advantage of execution vulnerabilities in the system through its communication interface. This sort of attack incorporates exploiting buffer overflows, and utilizing Trojan horse programs and viruses to inject malicious code into the system on purpose (Babar et al., 2011). Software attacks can happen in any layer of the IoT since all layers have an element of software in them. Zhang and Qu (2013) state that the application layer is susceptible to unauthorized access, DoS attack, malicious insider attack, spear-phishing attack, and sniffing attack.

2.4.4.2 Devices layer

This layer is sometimes called the perception layer or even the physical layer and has the primary function of identifying objects and collecting information (Zhang and Qu, 2013). This layer comprises the hardware that makes an IoT device and includes the sensors and the networking infrastructure. According to Zhang and Qu (2013), this layer consists of different kinds of data sensors like RFID, barcodes or any other sensor network. Zhang and Qu (2013), further highlight the risks associated with the physical or perception layer as unauthorized access to the tags, tag cloning, eavesdropping, spoofing, and RF jamming.

While we acknowledge that information gathering was once a human only phenomenon, it has become a norm for smart objects to gather information on their own without any human input. Such a collection of information is possible in CIoT because smart things come with sensors that collect the data. Some of the physical objects and sensor devices in the physical layer are two-dimensional code tags and code readers, RFIDs, cameras, GPS modules, and all sorts of sensors. Depending on the type of sensors, the information can be about location, temperature, vibration humidity or chemical changes in the air.

The security of the device layer is a challenge because devices at this layer, for the most part, do not have enough memory and computational capacity for comprehensive security

technology (Pomponiu, 2012). Babar et al. (2011) assert that physical attacks are the attacks where the hardware components are tampered with. Some examples mentioned by these scholars are de-packaging of chip, layout reconstruction, micro-probing, and particle beam techniques. Chen, Chang, Jin, Ren, Li and Li (2011) state that attacks at the physical layer usually happens when there is a disruption in object identification through MAC addresses of devices and jamming of networks that connect sensor nodes. When this happens, data collection cannot be efficient. Pomponiu (2012) alleges that applying intrusion detection and wireless encryption mechanisms at this layer can improve security.

Babar et al. (2011) further mention attacks such as side-channel attacks that depend on "side-channel Information" that can be recovered from the encryption device that is neither the plaintext to be encoded nor the ciphertext resulting the encryption procedure. Encryption devices create timing information that is effectively quantifiable, radiation of various sorts, power consumption statistics, amongst other things. Side-channel attacks make use of some or all of this information to recover the key the device is using. These attached are possible due to the logical operations that have physical characteristics that depend on the input data. Examples of side-channel information are timing attacks, power analysis attacks, fault analysis attacks, electromagnetic attacks, and environmental attacks.

2.4.4.3 Network layer

Security threats can also be from the network layer by altering the data destination and source information (Chen et al., 2011). The reason for this layer is to transmit data from the perception layer to any information storage and processing system. Such transmission is through communication networks such as the internet or any reliable network. The Network layer consists of the WSN, which transmits the data from the sensors to any destination with reliability. The related security issues in the network layer include Sybil attack, sinkhole attack, sleep deprivation attack, DoS attack, malicious code injection and man-in-the-middle attack (Zhang and Qu, 2013).

The network layer is very mature since it has been around for some time and has been researched thoroughly and documented. The network layer consists of infrastructure that facilitates the connection of things through different technologies such as 2G, 3G, Bluetooth, infrared depending upon the sensor devices (Khan, Khan, Zaheer and Khan, 2012). This layer includes many protocols that govern how the information and data are lined up for transfer so that it can be exchanged between endpoints in the layers or while in transit through different networks. The attacks from the network layer can target the sensor and actuator nodes and alter their ability to collect and share data, change the destination of information, modify actual record or information source, adjust the data itself or block the connections between the perception layer and the application layer, hence a complete breakdown of the service. Some of the threats in this layer include flooding and selective forwarding.

Flooding starts from the network layer yet focuses on the storage and processing abilities of the devices in the perception layer. Because the devices in this layer do not have a lot of memory or computational aptitudes, it does not take a lot of bandwidth to accomplish flooding in a network of simple nodes. Selective-forwarding is the point at which an intermediary node transmits particular data packets while blocking or dropping other packets. For this situation, security can be improved by access security to guarantee that data and data routes are accessed by the approved, authorized and authenticated entities. Encryption of data and the network-intrusion-detection system should always be in place as data is transmitted (Chen et al., 2011; Pomponiu, 2012). Babar et al. (2011) mention that wireless communications systems are vulnerable to network security attacks because of the broadcast nature of the transmission medium. They classify attacks as active and passive attacks, and they state that examples of passive attacks are monitoring and eavesdropping, traffic analysis, camouflage adversaries.

On the other hand, they mentioned active attacks like DoS attacks, node subversion, node malfunction, node capture, node outage, message corruption, false node and routing attacks. Zhang and Qu (2013), mention Sybil attack, sinkhole attack, sleep

deprivation attack, DoS attack and malicious code injection. The scholars above do not delve deeper into the mobile apps security challenges but barely mention that the apps are at the application or interface layer. Each layer of the IoT ecosystem is susceptible to cybercriminals in one way or the other.

2.5 Data privacy issues

This section discusses the issue related to data privacy in CIoT. The chapter also looks at how data collection, storage and transfer affect the problems of data privacy.

2.5.1 Privacy overview

Privacy is a significant concern for consumers when adopting new technology and has a substantial influence on the adoption of technology. Akturan and Tezcan (2012) define privacy issues as the potential loss of control over personal information. Alghamdi and Beloff (2014) say that it is of paramount importance that consumers feel safe about their privacy when interacting with systems such as CIoT. Rose et al. (2015) state that the full potential of CIoT relies upon procedures that respect personal privacy decisions over a wide range of desires. The data streams and consumer specificity afforded by CIoT devices can unlock incredible and unique value to consumers of IoT. However, concerns about privacy and potential harms might hold back the full adoption of CIoT. This stance implies privacy rights and regard for consumer privacy expectations are integral to ensuring consumer confidence CIoT. Diamantopoulou et al. (2020) state some consumers are not aware of the risks associated with personal information disclosure.

Peppet (2014) uses the phrase personal identifiable information (PII) and refers to PII as any information of any type that can identify a person. That information may include information such as the person’s name and surname, email addresses, gender, age, any other information that can point to the consumer that subscribes for the CIoT service. Personal data covers the already known information such as name, age, gender,

nationality and more. In addition to the known information, individual data includes data generated by the sensors in response to human desires. For example, we may be having desires to monitor our homes or our health using CIoT solutions, and the information generated by the sensors is personal. In this example, the information generated by sensors in the house shows our preferences, patterns and can allow one to predict future individual behaviours. Such data is still personal as it is related to the environment or the place where the person interacts with smart things and thus can inform and monitor behavioural patterns of the consumer interacting with smart devices. We can group the data as follows:

- contact details type information,
- demographic information,
- historical information,
- biometric information,
- private and confidential correspondence
- personal opinions and views about an individual made by another individual

Helberger (2016) points out that profiling and targeting are usually associated with data protection laws and privacy. Consumer laws need to play an essential role in protecting the legitimate interests of consumers, and guaranteeing a fair balance between consumers, providers of smart things and services, advertisers, insurance companies and other stakeholders. CIoT amplifies concerns about the potential for increased surveillance and tracking, difficulty in being able to opt-out of specific data collection, and the strength of aggregating IoT data streams to paint detailed digital portraits of consumers. While these are significant challenges, they are not insurmountable. Rose et al. (2015) assert that to take advantage of the IoT opportunities; there should be strategies developed to respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technology and services.

The fulfilment of customer privacy requirements is quite tricky. More often than not, we go on with our daily lives without thinking about personal data privacy issues. Cloud computing and the network epitomizes the importance of trusting data. As much as

providers of cloud service bring the narrative we have nothing to worry about when our data is in the cloud, it is essential to understand where the data resides if we are concerned about privacy. Can the information be leaked from that location? In South Africa, the legal aspect of privacy is taken care of by the POPI Act. The lawmakers created this legislation to promote the constitutional right to privacy in South Africa by safeguarding PII. The Act respects the right to privacy of customers and employees and also acknowledges the need for businesses to collect and use personal information (Botha et al., 2015). What does data collection entail?

Consumers need to have the right to privacy and data protection. There needs to be a balance between advancing technologies for the betterment of humanity and the right to privacy and consumer data protection. In South Africa, consumer privacy and data protection use a multi-faceted approach. Firstly, the right to privacy is enshrined in the Constitution. There are also provisions through various legal instruments that deal with privacy and data protection. The multiple legal instruments can converge and through mutual interactions serve to strengthen consumer privacy protection in systems like the CIoT assemblage.

Privacy is a topic of concern in the digital age. The issues of confidentiality and privacy are numerous and complex. There has to be a multidisciplinary approach between technology and legislations. Europe seems to prefer the use of the term “data protection” while the United Stated use “data privacy”, or “information privacy” (Palmieri III, 2020; Botha, Grobler, Hahn and Eloff, 2017; ETSI, 2019; Birnhack, 2008; Tikkinen-Piri et al., 2018). This research used data privacy and data protection interchangeably. The concerns raised by consumers of IoT, scholars and experts show that the focus on safeguarding consumers’ information is of utmost importance. It is essential to regulate the processing of personal information and thus to protect the privacy of consumers and their interests.

2.5.2 Collection

Sfar et al. (2018) state that data collection refers to how the sensors obtain the data from the environment and consumers. Perera, Ranjan, Wang, Khan and Zomaya (2015) suggest that collecting data through IoT solutions and analysing it on a large-scale can be of significant value to consumers and businesses. Furthermore, the authors state that collecting and analysing that data can make a substantial impact on society by increasing productivity and diminishing wastage.

Existing technologies and laws are not enough to support a privacy guaranteed data management life cycle. From the time the data is captured by the sensors embedded in IoT solutions to the point where there is the extraction of knowledge, and permanently and securely deleting raw data, consumer privacy needs to be protected and enforced. If we can address the data management life cycle, the IoT solutions can gain the confidence of the consumers. It is through strict laws and regulations that we can solve the technological limitations. These laws and regulations should include harsh and severe penalties for offenders and misusers. Is data collection violating consumer privacy in one way or the other? Are consumers allowed to consent to data collection or is data just collected discreetly without consumers' knowledge?

2.5.3 Storage

IoT technology generates big data, and this data needs to be stored somewhere. Al-Fuqaha et al. (2015) ascertain that big data needs smart and efficient storage. The authors further allude that connected devices need mechanisms to store, process and retrieve data. After smart devices have collected data, the data can be stored anywhere in the world. Data storage looks at the collected data in terms of where it is stored. Is it within a specific jurisdiction? Is it essential that the collected data resides locally or otherwise? What are the challenges if we do not know the data storage, and do consumers have a right to know such information?

Mary and Amalarethinam (2017) assert that cloud storage needs physical, logical and access control policies. Mahesh, Kumar, Ramasubbareddy and Swetha (2020) state that the use of smart device will continue to grow for a long time to come, and thus generating more data to be stored in cloud storages. The authors allude that storing more and more data in cloud storage facilities negatively affects the performance of the storage system. CIoT service providers need to keep in mind the criticalness of storage systems in performing their functions optimally such as improving the utilization of the storage, protecting the stored data, and eliminating redundant data. Zhao, Rong, Jaatun and Sandnes (2010) raise some concerns on cloud storage related to fault tolerance and service availability. Their concerns relate to system failures, or when a cloud service provider cease doing business. This is a problem when CIoT providers depend on one cloud service provider. To avoid this, CIoT providers need the capability of migrating from one provider to another.

Mary and Amalarethinam (2017) further state that the cloud offers typically vast space to store data. However, they are quick to warn that in cloud storage, data storage security is of greatest concern. Sultan, Varadharajan, Zhou and Barbhuiya (2020) state that there is a lot of reluctance to store data in the cloud when the information is sensitive. This is especially true in the health industry. They further argue that consumers lose control over their data once they choose to store it in the cloud. Mary and Amalarethinam (2017) discuss that consumers outsource the storage service because of their flexible, efficient and seamless services. Sultan et al. (2020) state that public cloud storage is popular with individuals and organizations. They mention some of the examples as Microsoft Azure Storage Service, Amazon S3, and Google Cloud Storage. Developers of CIoT systems make use of these cloud services. There are many advantages of using these public cloud providers. One example relates to saving on investments costs of building their storage. Another benefit is in accessing ubiquitous data through the Internet without worrying about management and maintenance of the outsourced data. There are increased concerns for data security and privacy when CIoT providers outsource data storage services to cloud providers. Data is normally stored around the world in distributed

geographical areas. This makes it impossible for data owners or consumers to be certain where their information reside. While the researchers acknowledges the benefits of cloud storage, the security and privacy of the data stored in the cloud remain a concern.

When IoT devices collect sensitive information, such information may be stored anywhere in the world. The health industry has a lot of sensitive patient information that they keep. The cloud service providers may misuse such data. For example, service providers may sell patient information to medical insurance companies. Rao and Vurukonda (2016) assert that cloud service providers have full of control over the data stored in their servers around the world. These providers can extract, modify, copy, destroy or even sell personal information. These concerns threaten personal information privacy. Xu, Hunt, Kwon, Georgiev, Shmatikov and Witchel (2017) ascertain that cloud providers store consumers' data such as photos and contacts, and make this data available to other mobile apps. The authors warn about the complexity of the data and that some underlying information that may lend in the hand of cybercriminals. For example, a collection of photos may have tags with the consumer's notes.

Xu et al. (2017) worry about the adequacy of protection of information in cloud storage. They allude that existing platforms do not have adequate support for mobile apps' data management. They make an example of Dropbox on Android storing files in public storage and thus giving up all the necessary data protection. Sultan et al. (2020) state that the confidentiality of outsourced data needs preservation to avoid any entity like service providers from accessing data without proper authorization. Access to information in public clouds requires suitable access control mechanisms and policies. The policies need to restrict any person or entity from accessing data other than those allowed by the data owners.

2.5.4 Transfer

Mary and Amalarethinam (2017) state that as soon as a consumer outsources the data to the cloud, there is a possibility to attack the data in transit. The authors suggest that when the data is in transit, it should be in either encrypted format or masked format. Data transfers focus on how the transmission of data happens between objects, humans and analytical platforms. It also refers to how stakeholders share data with other stakeholders or third parties. Is the way that shareholder share data violating privacy regulations such as the POPI Act in South Africa? Several technologies exist that can achieve information privacy goals during the transfer process. The technological approach explored technological steps that CIoT service providers can take to protect consumer data.

Weber (2010) highlights privacy-enhancing technologies (PET) such as virtual private networks (VPN), transport layer security (TLS), DNS security extensions (DNSSEC), onion routing and private information retrieval (PIR) systems as part of the technological approaches that can CIoT service providers can use during data transfer. These technologies form part of the proposed framework and tackle the technology part of the structure.

Rewagad and Pawar (2013) are of the view that to induce trust when transferring data, the system should be able to perform authentication, verification and encrypted data transfer, and thus maintaining data confidentiality. The authors mention eavesdropping, tampering, man-in-the-middle attack, and identity spoofing as some of the undesirable incidents that may happen to data in transit. They summarize these as follows.

- **Eavesdropping** - Zhang and Qu (2013) agree with Rewagad and Pawar (2013) and all state eavesdropping as a severe concern for data in transit. For eavesdropping to happen, the attacker gains access in the data path and gains access to monitor and read the messages. This risks associated with the physical or perception layer.

- **Tampering** - Atzori, Iera and Morabito (2010) agrees with Rewagad and Pawar (2013) in that data tampering can happen when the data is in transit. In this type of attack, the attacker may alter information that is transiting to the cloud storage. The same may happen once the data is in storage. When data tampering happens during either transmission or at the destination, there is a compromise in the integrity of the data. A system such as a CIoT assemblage should be able to catch the threat of data tampering to avoid any potential damage to the consumers.
- **Man-in-the-Middle Attack** - Zhang and Qu (2013) mention that this type of attack is common in the network layer. Data in transit happens at the network layer too. Rewagad and Pawar (2013) state that this type of attack occurs when an attacker infiltrates the communication channel to monitor the communication and modify the messages for malicious purposes
- **Identity Spoofing** – This attack happens when an attacker impersonates the users as the originator of the message to gain access on a network. This occurs when the data is in transit.

2.6 Security issues

This section discusses security concerns by first examining the overview of the issues related to security. As a foundation to security issues, the chapter looks at the CIA Triad, namely confidentiality, integrity and availability.

2.6.1 Security overview

While building the embedded security framework for IoT, Babar et al. (2011) suggest that we look at all the trade-offs between performance, cost, and security. More often than not, higher security typically means lower performance. Babar et al. (2011) further propose a hardware-software based security architecture for IoT that seeks to find the best trade-off between cost and efficiency or security and performance. They also argue that embedded security framework should consider the following things:

- **Environment factor:** this is in connection with the environment in which the devices operate. Designers need to determine the assumptions, threats, vulnerabilities, attacks and required policies for secure functioning of the CIoT ecosystem.
- **Security objectives:** There is a great need to determine the intention of the device's security. We need to consider the data or operation it needs to protect and against which threats.
- **Requirements:** We need to be able to determine functional security requirements from the beginning.

In the real world, more often than not, the three concepts of performance, cost and security are usually directly at odds with one another. If performance increases, so do the price. On the other hand, the lower the costs, the lower the security and performance. Finally, implementing higher security means that performance decreases. The security triad is part of security in IT, and thus it deserves some level of discussion when dealing with security in CIoT.

The Security Triad is also known as the CIA Triad, whereby the CIA stands for Confidentiality, Integrity and Availability. An IoT ecosystem needs to ensure proper identity authentication mechanisms and provide confidentiality about the data. The Security triad is a recognized model for the improvement of security mechanisms, and it executes the security by utilizing the three areas, which are data confidentiality, integrity and availability. A compromise of any of these three areas could cause severe issues to the system, and thus they must be accounted for (Farooq et al., 2015). The diagram below depicts the CIA Triad,

Figure 2.5: CIA Triad (Purcell, 2018)

Al-Momani et al. (2016) define security as the extent to which a person believes that using a particular application will be risk-free. Berdykhanova, Dehghantanha and Hariraj (2010) mention that activities such as online transactions are critical for consumers. Many scholars agree that security is among the issues that prevent customers from adopting IoT services (Lee and Lee, 2015; Babar et al., 2010). Kowatsch and Maass (2012) state that security is among the factors that affect the intention and the willingness to provide personal information for IoT services. Coughlan, Brown, Mortier, Houghton, Goulden and Lawson (2012) found that in the UK, security is an essential factor that influences the adoption of IoT in the country. Data from the sensors may be tampered with, stolen, deleted, dropped, or transmitted insecurely, allowing access by unauthorized parties. These concerns have an effect on the adoption of CIoT and on intentions to use IoT.

Babar et al. (2011) state the aim of considering security from design to implementation, and from manufacturer to consumption is to detect vulnerabilities throughout the lifecycle of the system. The design methodology should cater to the embedment of proper security majors. To do this, the service provider should discover the sources and the reasons for the vulnerabilities. Security experts designed the CIA model to guide policies for information security. While the experts consider this a core factor in IT security, it has a limited view of safety and ignores other important factors. For example, while availability serves to make sure that one does not lose access to resources needed to provide

information when needed, thinking about information security in itself does not guarantee that someone else has not used your hardware resources without authorization.

2.6.2 Confidentiality

Data confidentiality links to the privacy issues in that it seeks to address the confidence levels of the consumers about the privacy of sensitive information. Service providers achieve this using a different mechanism, and these mechanisms include the following (Farooq et al., 2015):

- Data encryption – This is when the system converts data into ciphertext structure, which makes it hard for users to access without appropriate approvals.
- Two-step verification, giving authentication by two dependent components and permits the access only when both components pass the authentication test.
- Biometric verification in which every person is uniquely identifiable. For the IoT based devices, it ensures that the sensor nodes of the sensor networks do not reveal their data to the neighbouring nodes. Similarly, the tags do not transmit their data to an unauthorized reader.

Abbasi, Memon, Memon, Syed and Alshboul (2017) state that since CIoT works on sensing, tracking and connecting everyday life objects used by humans, this adds more concerns regarding security, privacy and information leakage. CIoT also produces a large amount of personal information and hence creates the need for providing confidentiality and privacy. It is for these reasons that we require secure mechanisms for data collection and data access. These mechanisms should determine when and to what extent data should be collected. Some of the data collected, stored and analysed include sensitive details about consumers.

2.6.3 Integrity

Farooq et al. (2015) feel that cybercriminals can change data during the communication process. In addition to the human factors, they assert that data factors that are beyond human control, such as the crash of a server or an electromagnetic disturbance can also cause data alteration. Tchernykh, Schwiegelsohn, Talbi and Babenko (2016) mention that integrity involves maintaining the consistency, accuracy, and trustworthiness of information so that unauthorized people do not change the information. IoT systems are highly data-driven and assuring the integrity of the data and assuring that the system is resilient to data anomalies is a necessity.

There are existing methods that providers of CIoT can use to ensure the accuracy and originality of data such as Checksum and Cyclic Redundancy Check (CRC), which are simple error detector mechanisms for a portion of data. Sometimes data needs backing up, and so it needs continuous synchronizing and version control.

Atzori et al. (2010), refers to data integrity as the protection of user information from external interference and cybercriminals during transmission and reception. Many tracking methods help in such a way that the system can catch the threat of data tampering. Abbasi et al. (2017) acknowledge that data integrity is a significant issue in any data-centric environment. The authors mention that the devices that sense must gather and share only data essential to perform the required operation. The devices should not keep or share the data indefinitely and unnecessarily. The collection and sharing of data from sensors must employ the scale of integrity meaningfully with some standard procedures and rules. Smart cities depend on reliable and accurate data. Appropriate measures must ensure that data is accurate and free from manipulation.

2.6.4 Availability

Aldossary and Allen (2016) highlight the importance of system and data availability. The authors suggest that some organizations need their computer IoT systems to be available all the time due to the critical services they provide. If an attacker uses all available resources, others cannot use those resources, which leads to attacks such as DoS. People who need to access those resources may be blocked, or the system becomes too slow.

When we talk about data availability, we refer to the ability to ensure that data is accessible at all times, that is, when and where needed in an organization. Such a requirement applies to consumers concerning personal information. Farooq et al. (2015) posit that data must always be available to the consumers whenever they need it. This data availability requirement is equally valid to consumers of IoT. The availability of data ensures the immediate access of an authorized party to their information both under normal conditions and under unfavourable conditions. The organization usually avoid attacks like denial-of-service by introducing firewalls to ensure that data is available at all times. It is also critical to prevent bottlenecks that prevent the flow of information. Organizations dealing with CIoT should make sure these measures are implemented as any attack compromises both the organization and the consumers as far as data availability, among other things, is concerned. Furthermore, organizations should make sure that the CIoT system has redundancy and failover backup methods.

Abbasi et al. (2017) emphasize that the availability of IoT services must be ensured at all times due to the critical nature of their application. If CIoT services are not available for whatever reason, there will be a decrease in overall performance and an increase in the risk of being attacked by hackers. Access to data and the way of collecting and sharing it is critical, and security solutions must avoid adverse effects on availability. Therefore, when we talk about availability, we refer to both system availability and data availability. To help prevent system-level failure, Aldossary and Allen (2016) propose a high

availability and integrity layer (HAIL). The HAIL technology seeks to address the threat caused by a service provider being unavailable by distributing data across many cloud providers to keep their service available all the time. The architecture leverages multiple cloud service providers. The inspiration for HAIL is from a redundant array of independent disks (RAID), which is reliable storage made from unreliable storage. Tchernykh et al. (2016) suggest that service availability depends on the robustness of the hardware, hardware repairs, and maintaining a correctly functioning operating system environment, system upgrades, and preventing the occurrence of bottlenecks. Tchernykh et al. (2016) mention that redundancy, failover, RAID and other methods; can mitigate consequences when hardware failures occur.

2.7 Trust Issues

This section focuses on trust issues. The issues of trust can be between all stakeholders, between stakeholders and components, and between components of the CIoT assemblage. It is of paramount importance for trust to exist at all levels for progressive functioning of the CIoT assemblage.

2.7.1 Trust overview

Trust is an essential feature of both social and economic interactions in which uncertainty exists. It supports consumers to overcome perceived risks and insecurities. Trust is effective in reducing uncertainty and risks by supporting safety perceptions. It is a complex construct composed of multiple dimensions. The research approaches perceived technology trust (PTT) as the degree of subjective probability to which the consumer believes that the new technology usage is reliable and trustworthy. Literature in IoT technology (Gao and Bai, 2014; Al-Momani et al., 2016; Coughlan et al., 2012) supports the argument that trust in a system or technology influences adoption behaviour.

Trust is about a person's perceptions regarding the integrity and ability of another person or another system that provides a service (McKnight et al., 2002). Integrity is one of the three variables in a security triad. However, trust goes beyond what is described in the security triad and thus deserves its special attention. When Tchernykh et al. (2016) discuss trust, they emphasize that unauthorized people can alter the data. It is hard to argue whether a system is trustable or not because there are no existing metrics to measure this. A matrix is useful, and designers, developers, integrators and regulators, among other stakeholders, can use it. Chen et al. (2015) state the three trust metrics as honesty, cooperativeness, and community interest.

Chen et al. (2015) state that honesty represents whether or not an element of an IoT system is honest. For example, is any of the objects having malicious codes embedded in them? From the consumers of an IoT service, the malicious code represents dishonesty concerning what the system is supposed to do. Malicious code is not only dangerous to the consumers but also other elements and stakeholders of an IoT assemblage. Such a code can severely disrupt the operations of the whole system, and thus service continuity. When trust is broken in the system, other things such as data integrity are affected. The issue of data integrity discussed earlier is a trust concern that focuses on the quality of the data that is generated by or fed into an IoT system. The quality of the information flowing between devices and from sensors will directly impact whether an IoT system is fit-for-purpose. Data is the "blood" flowing through IoT systems.

There is a lot of interaction in any CIoT assemblage, and each element or stakeholder relies on others. Chen et al. (2015) state that the willingness or ability of objects and stakeholders to cooperate represent the level of trustworthiness. Certain objects can trust other things more than other objects. For example, if an object communicates using a standard protocol such as Internet Protocol, it may easily gain the trust of other things that use proprietary protocols such as Zigbee.

A CIoT assemblage has an interest in the overall system to perform optimally. Chen et al. (2015) mention a community-interest trust as representing whether or not different

elements have the same social communities or similar capabilities. The authors allude that when two parts have high community interest, they increase their chances of optimal interaction, resulting in better performance of the assemblage.

Relevant stakeholders of CIoT should consider the trust concerns during IoT system development and throughout the operation. There is a lot of data that components of the assemblage generate and process in an IoT assemblage. IoT systems are likely to have a dynamic and rapidly changing dataflow and workflow. There may be numerous inputs from a variety of sources such as sensors, external databases or clouds, and other external subsystems. The potential for the generation of vast amounts of data over time renders IoT systems potential “big data” generators. The possibility of not being able to guarantee the integrity of excessive amounts of data or even process that data is a trustworthiness concern.

Consumers’ trust in the system may influence their satisfaction and continuance intention. Li, Hess and Valacich (2008) allude that trust in the assemblage influences consumers' adoption decisions. Li et al. (2008) agree and state that trust is an essential predictor of technology usage and a fundamental construct for understanding consumers’ perceptions of technology.

Trust may be compromised at many levels, namely; consumer level, device level and network level. CIoT improves efficiency, analytics, intelligence, and decision-making. These beneficial attributes of CIoT are achievable only if the data collected is trustworthy. Ali et al. (2018) argue that in data transparency, there is an inherent need for trust and a lack of absolute confidence. Yan, Zhang and Vasilakos (2014) state that trust is about a declaration of holistic credential information or disclosure of relevant information, often decentralized across a network of actors and objects. They say that trust is complicated and is influenced by many measurable and non-measurable properties. A healthy relationship exists between trust and security since ensuring system security and user safety is a necessity to gain confidence. Trust covers a more significant scope than security in that it covers goodness, strength, reliability, availability, ability and other

characters of an entity. In addition, a strong relationship exists between trust and privacy discussed above as it touches on the strength of an object to determine the release and disclosure of information. The release and disclosure of information cover whether, when, and to whom the entity should release or disclose the information about itself. A trustworthy digital system should preserve its users' privacy, which is one of the ways to gain user trust. The framework addresses trust at the levels of consumers' level, smart devices' level and network level.

2.7.2 Consumer-level

Trust in consumers alone can be a huge issue; humans always want to manipulate the data for some nefarious gains. For example, some consumers have used fitness monitoring devices for the wrong reasons to accumulate points whereby they put these devices in dogs or cats. The purpose of having these wearables is to ensure that people remain active for health purposes. However, the collected data is not correct, as the active entity is a dog or cat. In South Africa, companies like Discovery, through their Vitality Health program, have been battling with the trust issue for a long time because it is challenging to tell if a person, a dog, or some other entity has been exercising or not.

How can organizations that collect CIoT related data trust that the collected data is credible? Organizations should endeavour to make sure that the data collected from consumers and devices is trustworthy. What checks and balances are in place to safeguard and trust the accuracy of the data from consumers?

Consumer trust in CIoT grows based on the reliability of the system. For example, if one was to leave home forgetting to switch off the stove, geyser or control anything remotely, the CIoT assemblage needs to be able to help the consumer at all times. If the system reports that one has successfully turned off the stove, it has to be like that. That is how trust is built – the system has to be reliable. However, if the consumer reaches home and discovers that the system did not switch off the stove as per expectation, the trust is

broken. This broken trust is between the CIoT system and the consumer. Sometimes the trust can be broken between a specific device and the CIoT system, or just between a device and the consumer. For the consumer to trust a system, that system has to be reliable at all times. There may be a need for reliability assessments of the system. Can the system handle anomalous events and data?

Usability is critical from a consumer perspective. Usability is a trust concern that deals with whether consumers understand how to use the devices that they can access. The question is on the user-friendliness of the IoT devices, mobile apps or other display modes, and the ability to learn how to make use of the overall system. This is an important attribute to consider for CIoT adaptation. The user interface need not be tightly constrained by limited display size and functionality. Some user interfaces such as in smart home devices are more often than not limited to a small set of onboard features like LED status indicators and a few buttons and a broader set of display and control parameters accessible remotely via a computer or mobile device. Usability and other trust concerns to which usability is intimately tied have significant implications for user trust.

2.7.3 Smart devices level

All stakeholders that have an interest in the collected data need to trust the devices that collect the data. If the equipment is faulty and thus collects untrustworthy data, the consequences can be dire and even life-threatening. Default credentials are still widely used, and this exacerbates the issue of trust. Criminals may counterfeit IoT devices. Trust has to exist from data collection up to the data storage. Ouaddah et al. (2016) mention those interacting devices that make up IoT reside at the edges. IoT data generation and action thereof happens at the edges. They allude that there are often no secure physical perimeters where the raw sensing of the physical world takes place such as on rooftops and geysers, in our gardens, inside our car engines and on solar panels.

The threats to IoT devices are an essential concern because they are hard to remediate and fix. The existence of IoT botnets has been a known fact since 2008. However, the world did not realize the extent of the danger they pose until the second half of 2016. One of the methods that can be looked at to build trust is the certification of the devices used in CIoT assemblage. The ability of heterogeneous “things” to interoperate and integrate creates a different tension related to emergent behaviours. Heterogeneity will almost definitely create emergent behaviours that will enable new and unknown security vulnerabilities as well as affect other concerns such as reliability and performance. Ownership and control are trust concerns that occur when much of the functionality within an IoT system originates from third-party vendors.

More often than not, we do not know what is happening inside third party devices. If we do not know the internal workings of a third party device, it can lead to security threats from the device in question. These devices are neither observable nor transparent and can contain malicious Trojan behaviours. Consumers of IoT can only hope and trust that there is no malicious intent by the third-party providers. When CIoT adopters start understanding the magnitude of losing access to these acquired functions, they will recognize criticalness of trust in IoT systems.

There is also a trust concern between hardware and software components. Will they always work well with each other? Interoperability can be a challenge in a system with heterogeneous devices. The devices or parts of the devices should be swappable to satisfy new system requirements. After that, these devices should be able to continue communicating without breaking the trust that existed before swapping a specific device or component of a device. That means trust relates to integration, interoperability, compatibility and composability. Each of these has an impact on IoT trust. It may be helpful to have an evaluation for each of these properties of new devices or components of a device entering the system before being part of the assemblage.

There need to be functional requirements all the time stating what a system shall do as well as contrary provisions saying what a system shall not do. These requirements should

not be a hindrance for a CIoT system to learn new things. Machine learning should somewhat improve functional needs instead of introducing contrary elements. System maintenance should happen as frequently as necessary to make sure the system is not doing what it is not supposed to be doing in the background.

Heterogeneity brings the problem of predictability. It is not easy to predict how devices will interact with each other. While machine learning is a good thing in making the devices smarter, it may pose new challenges in that it may be hard to predict the outcome of the system. For example, some devices in the system may be overloaded because of more and more data and processing power happening locally on a smart device. The design of the device in question may have lower RAM (Random Access Memory) and CPU (Central Processing Unit), but new information and processing demand extra resources. If this is not addressed, it may crash the entire CIoT assemblage.

2.7.4 Network and storage level

It would be suicidal to ignore trust at the network level. Network-level trust refers to end-to-end communication between smart things and consumers. What are the threats to these networks? How one can secure that communication path without compromising performance and consumer experience? Can the network be trusted in order not to compromise or allow data alteration and thus misinform consumers or any stakeholder that has an interest in the collected data? Do consumers always know what smart devices are doing? If we consider a voice response technology such as smart speakers, Amazon Alexa or Google Assistant, do consumers know who else may be listening? Are these sounds stored somewhere and linked to the consumer?

The network helps in synchronizing the CIoT system, especially as far as redundancy and backup are concerned. It is because of networks that we have distributed computing systems. Such systems have different computations and events occurring concurrently. There can be several computations and functions, such as data transfers happening

simultaneously. These computations and activities need some degree of synchronization and thus need a timing mechanism that applies to all computations and events.

The conventional internet has a TCP/IP protocol suite with HTML for websites running over TCP/IP. There are standardized port numbers and globally concurred web domain names that enable steady and consistent operations, paying little heed to the hardware producer. A similar structure has not reached out to IoT devices since they mainly do not have the processing power to help it. This lack of structure has enabled many new protocol families, causing countless potential interactions among different versions of software and hardware from a wide range of sources. These interactions are inclined to security and reliability issues.

Chen et al. (2011) allude that the data exchange happens throughout the ecosystem, and unauthorized access exposes it to data theft, the supply of fake data and viruses. They further mention that at the network layer level, data related to destination and source is easy to alter and thus compromises the privacy of consumers of IoT. To limit this, Pomponiu (2012) mentions the importance of using access control management at the application level. Since mobile apps operate at the application level, developers of mobile apps have to take due diligence during the development process in as far as access control management is concerned. However, since the mobile apps are just an element of a broader IoT ecosystem, other layers of the IoT ecosystem may be used as entry points of attack and thus renders access control management at application level lacking in terms of security. We need a holistic and integrated security framework that considers all layers of the IoT ecosystem from a technological, social, and legal and legislation point of view. In developing the framework, the researcher took cognisance of the make-up of a CIoT assemblage and the stakeholders involved in the assemblage.

Sivarajah, Kamal, Irani and Weerakkody (2017) ascertain that IoT comes together because of the sensors and machines connecting. That is to say, the real value that IoT creates is at the intersection of gathering data and leveraging it. The information that the sensors collect is not worth very much if there is no infrastructure in place to analyse it in

real-time. Sadeghi, Wachsmann and Waidner (2015) argue that cloud-based applications are the key to using leveraged data. They further say that IoT does not function without cloud-based applications to interpret and transmit the data coming from all these sensors. Want, Schilit and Jenson (2015) agree and state that the cloud is what enables the apps to go to work for you anytime, anywhere. This research argues against centralized cloud-based applications and proposes the distributed ledger architecture from a technical, socio-economic and legal point of view. From a technical point of view, the distributed ledger approach builds from other scholars such as Biswas and Muthukkumarasamy (2016), Qu, Tao and Yuan (2018), Ali et al. (2018), Zyskind and Nathan (2015) and Ferrag, Derdour, Mukherjee, Derhab, Maglaras and Janicke (2018).

Katuu and Ngoepe (2015) mention that the cloud-computing model offers public institutions several benefits such as scalability, cost savings and enhanced security. Marciano, Lemieux, Hedges, Esteva, Underwood, Kurtz et al. (2018) mention that social and industrial trends inform the production and consumption of digital records. Darzentas, Hazzard, Brown, Flintham and Benford (2016) ascertain that smart things or objects may acquire precious digital files throughout their lifetimes. In addition to that, they say that this may enhance their value, meaning and utility. The challenge on CIoT is about what the consumers' data reveals about them.

Consequently, this revelation raises the question of data ownership and how data sharing happens and with whom. While the focus of the scholars mentioned above is on archived digital records in general, we need to think about what happens to digital information, including digital files, when interacting with mobile apps and IoT. When it comes to the sensors, they are always part of the devices and thus help the devices to be smart (Stojmenovic and Wen, 2014). This kind of ecosystem allows everything in our lives to be smart.

Tiwary et al. (2018) state that each of the devices used in CIoT requires a unique identification for communication. This identification helps in controlling and accessing remote devices via the internet. Each object or device is embedded with sensors and

continuously sense the data based on the context. The context may be sensing humidity, temperature, sound levels, amount of air pollution, and motion. The sensors send the sensed data from smart devices to the database through the communication technologies.

Tiwary et al. (2018) further mention that the smart devices used in CIoT produce a large amount of data, and this data has to be stored in the storage device. Once the data is stored, it has to be analyzed to extract meaningful information. This analysis is done by an analytical tool which incorporates an intelligent algorithm that extracts the useful information from raw data. They further state that a centralized infrastructure is required to support both storage and analytical tools. However, this research disputes the use of centralized architectures as they introduce a single point of failure when the centralized environment is under attack.

Bojanova and Voas (2017) state that the amount of data generated by an IoT assemblage can easily overwhelm the ability of network to handle the workflow and dataflow needed to achieve the goal of the assemblage. All stakeholders need to have trust that large amount of data will not overwhelm the network and thus causing unnecessary inconveniences.

Abbasi et al. (2017) mention that mobile devices of IoT infrastructure must be secured against attacks because these nodes may be the most natural victims of the attack and can effortlessly provide a gateway to an adversary to get into the system for malicious activity. This gateway provides an attacker with the facility to disrupt whole IoT operations considerably. Mollah, Azad and Vasilakos (2017) note that to protect data confidentiality and privacy, and there is a need to ensure the security of mobile device storages. Furthermore, they propose two ways to provide mobile device storage namely;

- using encryption of data and securing the encryption key by using the Trusted Platform Module which is installed in a stand-alone chip on a mobile device, and
- using cloud services by consumers to store all data within it.

Tiwary et al. (2018) agree with the latter approach and propose centralized architectures. However, a centralized approach introduces a single point of failure, and personal data may be compromised even more in this architecture. Ensuring that information is trustworthy is hard enough when a central authority orchestrates device configuration, data collection and cleaning, and data dissemination. However, distributed networks like those using the blockchain technology do not rely upon a central authority.

To eliminate the single point of failure, some scholars (Pilkington, 2016; Hashemi et al., 2016) propose a blockchain architecture in dealing with trust issues from a network architecture point of view. They argue that blockchain applications ascribe all authority to the blockchain. However, in reality, trust extends beyond the devices that are part of a blockchain. Crosby et al. (2016) define blockchain as a distributed database of records. These are sometimes called public ledger of all transactions or digital events that have been executed and shared among participating parties. Zyskind and Nathan (2015) state that the blockchain technology or distributed ledger technologies come with promises to express and establish shared trust in information created and exchanged by smart things and people.

Biswas and Muthukkumarasamy (2016) conclude that the main advantage of using blockchain is that it is resilient against many threats. In addition to the resistant against the risk, they state that it provides several unique features such as improved reliability, better fault tolerance capability, faster and efficient operation, and scalability. The integration of blockchain technology with devices in an IoT ecosystem can create a common platform where all devices would be able to communicate securely in a distributed environment and thus curb security threats and privacy.

2.8 IoT and mobile apps in the South African environment

The IoT ecosystem comes from the development of the internet, mobile devices, mobile applications, near field technologies (such as Wi-Fi and Bluetooth) and communication networks. Mobile apps are part of the Consumer IoT ecosystem because consumers of

IoT generally use them to interact with smart things. The South African environment experiences a high level of crime. There have been many initiatives around community safety using IoT technology. Dlodlo et al. (2015) mention that one of the major tasks of the South African government is to reduce crime levels on a year-to-year basis. The authors state that the use of ICT, in general, is crucial in finding crime-related solutions. South Africa can use CIoT in the fight against crime.

Mvelase, Dlamini, Dludla and Sithole (2015) state that mobile devices are one of the most essential and affordable tools to access data. They design a framework architecture that integrates smart wearable mobile devices and cloud computing in healthcare. They ascertain that, in the current dispensation in South Africa, cloud computing is used widely for security and easy access to data. Mobile apps used in IoT make use of the cloud computing technology and thus the security and data privacy issues and challenges that are inherent in cloud computing pose similar problems in IoT and mobile apps. Cloud storage also comes with the challenges of privacy, security, anonymity, telecommunication capacity, government surveillance, reliability, liability and more. When building cloud storage, service providers need to think of all these issues since medical records are susceptible. There are many ethical issues, rights to care, and rights to privacy regarding medical records. Service providers need to build cloud storage to efficiently manage explosive data growth and significantly improve the performance of file serving applications. The cloud storages' design has to be extremely scalable, flexible, and cost-efficient. These cloud storages deliver excellent performance and modular storage infrastructure to accommodate significant storage growth.

The next section of the study discusses the responsibility of the identified stakeholders, namely; smart things or objects, individual consumers and non-consumers, government and regulatory bodies, application developers, and device manufacturers. Just as it is essential to understand the architecture of CIoT assemblages to deal with the challenges that come with it, it is also necessary to understand the stakeholders involved in the assemblage and how they influence the challenges of data privacy, security and trust.

2.9 Consumer IoT stakeholder responsibility

Different stakeholders affect what happens in the CIoT assemblage in one way or the other. Some stakeholders may unintentionally elevate the risk levels of the CIoT. For example, consumers may ignore the security of the device by using default passwords or even removing the password altogether, or manufacturers may manufacture devices that are sub-standard and do not follow any open standards, or cloud providers may store CIoT data in a server without any security features. All these and other examples of stakeholders' roles warrant our discussion on stakeholders' responsibility. It is because of these various stakeholders that the CIoT assemblage or ecosystem can be complicated. Many scholars (DeLanda, 2006; Harman, 2008; Hoffman and Novak, 2017; Buchanan, 2015; Hoffman and Novak, 2015) agree that the concept of communication is critical to understanding assemblages. The stakeholders continually interact and become something more than individual entities. The consumer is a vital and necessary component of CIoT. Interactivity is crucial as it is the glue that holds the assemblage together. Without interaction, there is no smart systems or a CIoT assemblage, but people, products and other stakeholders.

DeLanda (2016) ascertains that assemblages emerge and change over time, and the nature of the components' interaction with each other can change over time. In addition, the elements of CIoT vary and can be added to or removed from an existing CIoT. These changes in the assemblage happen because of interactions between humans and nonhuman smart objects, and between the objects themselves. For example, the camera in the smart home system cannot collect and store data without interacting with a Network Video Recorder (NVR). The owner of this smart home cannot make sense of the data unless there is a connection to an analytical system. The assemblage cannot trigger an alarm unless there is a further connection to an alarm controller that also connects to the siren. The ongoing interactions define the properties and capacities of the assemblage.

In their research on assemblage theory, Hoffman and Novak (2017) ascertain that different aspects of the interaction between consumers and objects produce different

experiences. These diverse experiences emerge because of repeated and multiple interactions. Novak and Hoffman (2019) expand on the notion of experiences and argue that these experiences are positive and enabling, and some are negative and constraining. Sauer (2017) alleges that broader societal influences, such as privacy and legal considerations, can shape consumers and objects experiences. Other forces are in advertising and marketing, which also touch privacy or personal information, and even human rights domains (Hoffman and Novak, 2017). Müller (2015) discusses the assemblage theory and suggests that various scholars have applied the concepts of assemblage theory in different fields. This study uses the concept of assemblage theory in CIoT.

The assemblage theory allows us to examine how new capacities of complex systems like CIoT translate into consumer experience of these systems. The assemblage theory considers external associations. The researcher discussed various external associations or interactions as a way of finding meaning in the responsibility of multiple stakeholders. These external associations can be between CIoT ecosystem, legislators, policymakers, device manufacturers, applications developers and other organizations. The researcher further used the assemblage theory to find meaning due to the theory's consideration of external associations. Consumers affect smart things and smart things affect consumers. Hoffman and Novak (2015) posit that it is through ongoing interaction of components that new capacities can emerge. The authors further state that these constant interactions make assemblages not to be static, but dynamic and in continuous nonlinear change.

Consumers experience CIoT in different ways depending on experiences from the past, their interests and the envisaged outcome. Dewey's experience theory (Dewey, 1984; Clandinin and Connelly, 2000) looks at personal and social (interaction); past, present, and future (continuity); and place (situation). Consumers are the only ones who can relate their experiences as they interact with mobile apps and devices. The consumers can further narrate their past and present experiences, as well as how they intend to do things differently in future. Finally, consumers can provide context or situations as to where they feel it is worth using IoT and mobile apps. At the heart of Dewey's theory is the sense of

fluidity in storytelling. The fluidity is about moving from the past to the present, and the future (Wang, 2017). This fluidity, as can be seen later in the research, takes interpretivism as a philosophical position within an epistemological stance. In other words, we will treat reality as being fluid and knowledge as subjective due to the very nature of storytelling.

There is agreement among scholars that interaction is necessary for consumer experience to occur. Communication or interaction may be direct or indirect. In IoT, the application layer objects may not be interacting directly with the physical layer components but there some interaction via the network layer. Consumers of IoT may not be directly communicating with the sensors but via a mobile application. De Keyser, Schepers and Konuş (2015) incorporate interaction in defining consumer experience as comprised of the cognitive, emotional, physical, sensorial, and social elements that mark the customer's direct or indirect communication with a set of actors. Interaction is a prerequisite building block from which experience originates.

Silverio-Fernández et al. (2018) ascertain that in CIoT, smart devices to interact with consumers by design. There is a certain level of interaction with the consumer, whereby the device collects or provides data to the consumer. Harwood, Dooley, Scott and Joiner (2014) explain that a smart device allows consumers to ubiquitously conduct activities such as emailing, texting, gaming, internet browsing, social networking and making phone calls; all these activities are specifically designed for a consumer. Miller (2015) suggests that IoT is all about the interconnection of devices, to the point where some devices might never interact directly with consumers and only interact with other devices. Stojanovic, Falconer, Isaacs, Blackwood, Gilmour, Kiezebrink et al. (2017) imply that the interaction can happen with consumers or within the smart devices.

The IoT ecosystem has several stakeholders that need discussing to assist in the development of the framework. Perera et al. (2015) ascertain that all stakeholders have the responsibility to secure the infrastructure, the data collection and transfer process, as well as the people using the devices. The stakeholders include the following:

- Smart Things or Objects
- Individual consumers and non-consumers
- Government and Regulatory bodies
- Application developers
- Device manufacturers

2.9.1 Smart things or devices

It is no doubt that IoT comes alive with connected smart things. The key is to make sure that there is interoperability of these smart things, including their seamless integration with applications and services. The internet-enabled devices collect data at the edges of the CIoT assemblage. Device manufacturers develop these devices to autonomously perform specific tasks and send the information to a centralized place for data processing purposes. In CIoT, there is connectivity that allows previously unrelated objects or things and products to work together as assemblages through a process of ongoing interaction. As these interactions take place, new properties and capacities emerge that have the potential to expand what consumers and smart things can do, and what can be done to and for them. The various assemblages affect various consumers and objects in different ways.

Day in, day out, billions of smart devices are being connected. Smart devices in IoT are always lightweight and have less energy and memory. IoT transforms real-world objects into smart objects. Due to the low-cost price of processors and wireless cards, almost anything can be part of the IoT, from wearable devices (such as smart wrist straps and smartwatches) to a giant vehicle (such as a train or aeroplane). The development of the IoT has created a large number of devices, such as sensors, interconnected and interoperable devices for data collection and exchange. Lea (2018) makes examples of the following CIoT use cases in a smart home: smart irrigation, smart garage doors, smart locks, smart lights, smart thermostats, and smart security.

According to the assemblage theory (DeLanda, 2016; Hoffman and Novak, 2017), smart things are one of the stakeholders that need to be given attention in the CIoT assemblage as they can affect and be affected. These smart things can operate interactively and autonomously, or they can self-govern. This study addresses the concept of smart things or devices within the paradigm of the CIoT. What is the role of smart things or devices in a CIoT assemblage?

Silverio-Fernández et al. (2018) propose three pillars that make a device or object smart, namely autonomy, context-aware and connectivity. In other words, by adding these features, we can make a device smart. For example, if a sofa gets a sensor (context-awareness) that detect when you sit on it, and then processes that information (autonomous computing) and sends it to a central local via a network (device connectivity), the couch has just become smart. Miller (2015) points out that most things connected to the IoT assemblage are simple devices that scholars sometimes refer to as smart devices. However, he warns that these devices are not necessarily smart unless they join other connected devices. That means a device on its own or in isolation is not smart, and has to be interacting with other devices. In essence, we can say the device has the responsibility to interact in the assemblage.

Silverio-Fernández et al. (2018) emphasize that as much as the final aim may be to provide services to the consumer, the interaction should be with other devices and humans. This study is not concerned about whether the communication is with other devices or with humans as it assumes humans and devices to be on the same ontological footing. As long as the devices can affect humans and humans affect them, it means there is a two-way interaction. Stojkoska and Trivodaliev (2017) conclude that a smart device has a responsibility to communicate and compute. Ray (2018) points out that those smart devices can dynamically adapt to the changing contexts and take actions based on their operating conditions. In other words, smart things should be self-configuring and interoperable, having unique identities and being able to communicate and exchange data with other devices and systems. The definition of smart things excludes the consumers, and thus this paper extends the definition to include consumers as part of the

interaction. The next sections discussed the three attributes that make the things smart namely autonomy, connectivity and context-aware.

2.9.1.1 Autonomy

Autonomy refers to the situation whereby the device performs tasks autonomously without the direct command of the user. Zhang, Mao, Rau, Choe, Bela and Wang (2013) explore the autonomy of smartphones (a smart device) and point out the multitasking scenarios whereby the smartphone has processing capacity and to perform tasks in the background. Najjar and Amer (2016) use the term smart device for a control system used in engine cars that autonomously perform tasks. Smart devices can independently send information over a network to a centralized database or analytical system. Schleich, Faure and Klobasa (2017) make mention of their intention to use smart meters by measuring the information through sensors and send such information through a network autonomously. Vazquez-Fernandez and Gonzalez-Jimenez (2016) discuss the processing of biometric data in a mobile device for face recognition. They highlight that this is done independently by such a smart device.

2.9.1.2 Connectivity

A smart device needs some form of connectivity to interact with other devices, databases, analytical platforms and with humans. Connectivity helps with data sharing and accessing services from the internet. Cheng and Mitomo (2017) posit that a smart device always needs communication capabilities. Many other scholars (Madakam, Lake, Lake and Lake, 2015; Tiwary et al., 2018) agree on that IoT relies on connecting many devices to the internet and some control centre, between human-to-human, human-to-things, and things-to-things. There are many technologies used to connect things to the internet and each other. IoT devices may connect to the internet and each other via RFID, Near Field Communication (NFC), Ethernet connection, WiFi connection, ultra-wide bandwidth(UWB), GSM, WiMAX, 2G, 3G, 4G and Long Term Evolution-Advanced (LTE-A), ZigBee gateway, Bluetooth, Z-wave, Sigfox and many others. Tiwary et al. (2018)

further state that if we put sensors and actuators on objects and then add network connectivity, many different smart devices are possible. Consumers use smartphones equipped with mobile apps to communicate with other smart things, and communication can happen using any of the technologies listed above. The next subsection summarizes some of the connectivity technologies mentioned used in IoT deployments:

Traditional Cellular and Cellular LPWA - Cellular technologies **(**2G/3G/4G) were initially designed for consumer and business voice and data services. These mobile networks were traditionally used for wide area networks. From around 2020 onwards, 5G networks will also start to be commercially available, bringing improved capabilities to address both massive and critical communication use cases. In South Africa, mobile network operators are Vodacom, MTN, Cell and Telkom Mobile. Wang, Lin, Adhikary, Grovlen, Sui, Blankenship et al. (2017) mention that NB-IoT is an IoT technology specified in Release 13 of the 3GPP in June 2016. NB-IoT can coexist with GSM (global system for mobile communications) and LTE (long-term evolution) under licensed frequency bands. Mekki, Bajic, Chaxel and Meyer (2019) state that NB-IoT offers the advantage of maximum payload length. NB-IoT and LTE-M are backed by major mobile operators such as Vodacom, MTN, Cell C and Telkom Mobile in South Africa, offering standardized connectivity with global reach.

Proprietary LPWA – Sigfox and LoRa are some of the proprietary LPWA technologies used in IoT. Irmak and Bozdal (2017) state that Sigfox announced having built its first IoT based telecommunication network in 2015. The authors allude that Sigfox is an LPWAN network that offers an end-to-end IoT connectivity solution. Sigfox deploys its proprietary base stations equipped with cognitive software-defined radios and connects them to the back end servers using an IP-based network. Sigfox (operated by Sqwuidnet in South Africa), may address certain niche segments. Mekki et al. (2019) further state that LoRa is a physical layer technology that modulates the signals in small frequencies using a proprietary spread spectrum technique. According to Northstream (2018) analysis, they recommend Lora deploying IoT in widely spaced areas, and have NB-IoT and LTE-M as

complement technologies. LoRa's dynamic and open ecosystem is ideal for private networks with customized deployment.

Short Range Technologies (WiFi, **Zigbee, Bluetooth)** - Traditionally, the IoT landscape or rather the machine-to-machine (M2M) communication has been dominated by radio technologies such as ZigBee, Bluetooth and Wi-Fi for short-range local area networks. Wi-Fi's use was for consumers in local area networks, and now some devices come equipped with Wi-Fi modules.

RFID - Another technology worth mentioning that date back to the 1980s is RFID technology (Palattella, Dohler, Grieco, Rizzo, Torsner, Engel et al., 2016). Mathaba, Dlodlo, Williams and Adigun (2011) mention that RFID tags come in two types. They can either be passive or active, and this is dependent on their supply of electrical power. Active RFID has its won power source, such as having an in-built direct current battery. Active tags - These active tags send a stronger signal, and RFID tag readers can read them from a distance. Because of the in-built source of power, they are usually bulky and expensive. It is possible for them to either transmit a signal only when in range or continuously.

On the other hand, passive RFID tags get their power from a signal of an external RFID reader. These usually are reasonably small and cheap when compared to active tags. Mathaba et al. (2011) are of the view that South Africa as a developing country is expected to prefer the more affordable tags. However, this view falls short of explaining the functionalities of each tag. There is no merit in choosing a more affordable tag if it is not fit for purpose.

Northstream (2018) posit that there is no single technology ideally suited to serve all IoT use cases. Most technologies co-exist and complete each other to perform a specific purpose. Figure 2.6 shows the main connectivity technologies for IoT.

Considerations	Traditional Cellular			Cellular LPWA		Proprietary LPWA			Short Range		
	2G	3G	4G	LTE-M	NB-IoT	SigFox	LoRa	Ingenu	Wi-Fi low power	ZigBee 3.0	Bluetooth LE
Outdoor coverage	>10km	>10km	>10km	>10km	>15km	>15km	>10km	>15km	<1km	<300m	<100m
Indoor coverage	High	Medium	Medium	Medium	High	High	High	Very low	Very high	Medium	Low
Energy efficiency	2-5 years	<10 days	<10 days	>10 years	>10 years	10-20 years	10-20 years	10-20 years	6-12 months	6-12 months	6-12 months
Typical uplink data rate	50 kbps	1 Mbps	10 Mbps	1 Mbps	20 kbps	100 bps	25 kbps	50 kbps	1 Mbps	250 kbps	1 Mbps
Bidirectional communication	Yes	Yes	Yes	Yes	Yes	Limited downlink	Yes in Class A	Yes	Yes	Yes	Yes
Mobility	Very high	Very high	Very high	Very high	High	Very low	Low	Medium	Medium	Low	Very low
Localization	Yes	Yes	Yes	Yes	n/a	No	Limited accuracy	n/a	Yes	Yes	yes
QoS & security	Very high	Very high	Very high	Very high	High	Very low	Low	Low	Medium	Medium	Medium
Connectivity cost	Medium	High	Very high	High	Medium	Very Low	Low	Low	Medium	Medium	Medium
Scalability	High	High	High	High	Very high	High	High	High	Low	Low	Very low
Future proofness	Medium	Medium	Very high	High	Very high	Low	High	Low	Medium	High	High
Global reach & interoperability	Very high	Very high	Very high	High	High	Medium	Low	Very low	Low	Medium	High

Figure 2.6: Main connectivity technologies for IoT (Northstream, 2018)

Selecting the most suitable connectivity technology is one of the critical decisions when deploying IoT. Every use case has specific needs, which translate into certain technology requirements that determine the choice of the most suitable connectivity technology. This is equally true when selecting the tags to use. The tags to need to perform the required tasks optimally.

Northstream (2018) state that for applications that require high data rate, the most suitable technology options are either LTE, Wi-Fi or BLE, depending on the scope of the IoT deployments. The author state that choosing connectivity technology is less evident for local short-range applications, and often the interfaces and implementation of platform and application layers become more crucial. Mekki et al. (2019) allude that NB-IoT provides the advantage of very high scalability than Sigfox and LoRa. For service providers to deploy CIoT in South Africa, they need first to understand the requirements and choose various technologies that are fit for purpose.

2.9.1.3 Context-awareness

Smart devices come in many different forms and have various built-in sensors that make them context-aware. That may include devices as cameras, microphones, accelerometers, GPS modules, light sensors, humidity testers and many others. Silverio-Fernández et al. (2018) mention that the fundamental thought behind context-awareness is the ability of smart devices to perceive information from the environment through sensors. These sensors can be in cameras, accelerators, microphones and GPPS modules. The smart devices can use the data from sensors to make autonomous decisions or to help consumers to make better decisions. Zhang et al. (2013) discuss the use of sensors with a smart device when talking about smart devices for photography or video recording. Husnjak, Perakovic and Jovovic (2014) address context-awareness of a smart device with a particular focus on human voice recognition. Hoffman and Novak (2017) propose a conceptual framework that is based on assemblage theory and object-oriented ontology. Their proposed framework looks at how the consumer experience and object experience emerge in the IoT. The next section looks at the consumers of IoT as one of the stakeholders.

2.9.2 Individual consumers and non-consumers

After all the interactions have happened amongst CIoT components, and with external entities, CIoT affects the consumer experiences in one way or the other. Many consumers of technology are not aware of the underlying security risks and privacy issues, nor their rights as consumers. This research seeks to make consumers aware that they need to look for products or services that are secure and privacy-respecting by design. They have a responsibility to protect themselves from malicious intentions. Legislations like the POPI Act seek to achieve the right to privacy of consumers. Consumers have the right to know how smart devices collect their data, how that personal data is used, who accesses it, and how the service providers will protect and store the collected data.

Consumers attitude on IoT inform levels of investments now and in the future. This study unpacks how the positions have been changing over time through the storytelling by the consumers. Through storytelling, the consumers were able to articulate their stories, voice and their future intentions regarding the use of CIoT. In 2016, The Edelman Trust Barometer showed that there exist a exists a gap between the technology industry's perception of performance and the things consumers find most important (Edelman, 2016). In the Edelman survey, consumers highlighted the area of importance as a technology that protects consumer data, ensures quality control and keep people safe. Therefore, consumers have a role to play in providing feedback on issues that matter most and hence on the adaptation of new technology. Consumers keep a close watch on how markets develop and how technologies affect their lives.

Dewey's theory of experience (Dewey, 1984) posits that if there is always an interaction between the actors (humans and smart things), continuous changes are bound to happen. As the CIoT smart components (equipped with machine learning capabilities) interact, they affect each other as well as the consumers. Perera et al. (2015) suggest that individual stakeholders can be both IoT product consumers and non-consumers. Most of the exiting IoT solutions focus on consumers. However, these IoT solutions also affect non-consumers. Lea (2018) makes examples of the use of wearables as health and movement trackers and smart clothing. Some wearables pose a threat to the people who wear them and to the people around them.

An example is a product called Google Glass that poses a threat to people within the viewpoint. It is the responsibility of the IoT device owner to be sensitive to the other people around him or her. The consumer needs to consider how his or her devices affect others. Figure 2.7 shows examples of body parts that can make use of wearables.

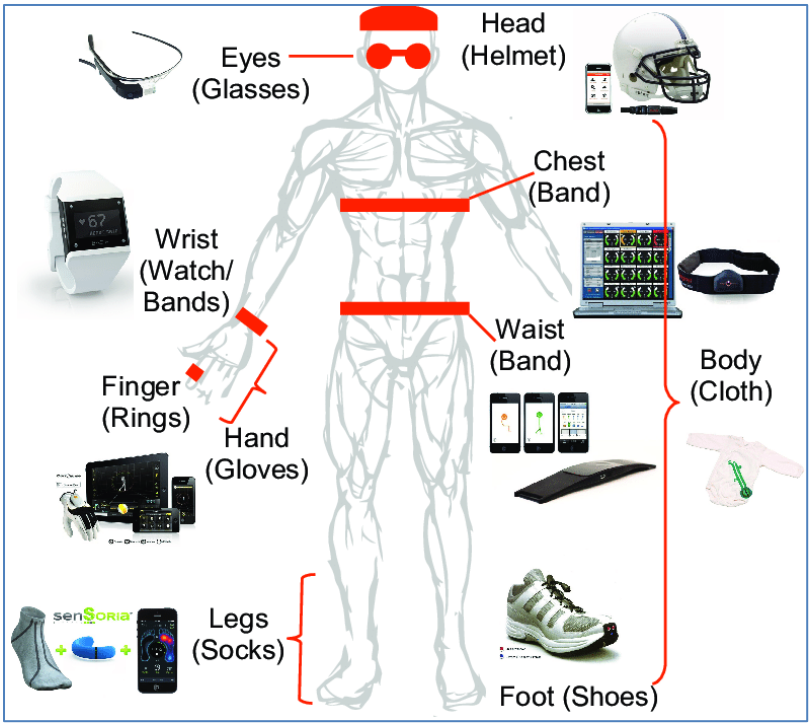


Figure 2.7: Examples of body parts that can use wearables (Perera, 2017)

In addition, when consumers install the IoT devices such as CCTV cameras and other sensors in private homes, office environments, or apartment complexes, it is essential to notify the non-consumers of the nature of the solution deployed and related information. Hoffman and Novak (2017) focus on how CIoT is presenting new opportunities to consumers and how they have the potential to revolutionize the consumer experience. They ascertain that smart objects possess their unique capacities and their kinds of experiences in interaction with the consumer and each other.

2.9.3 Government and regulatory bodies

Perera et al. (2015) suggest that government or independent regulatory bodies must lead and enforce standardization and legal efforts. For example, South Africa has agencies like the Independent Communications Authority of South Africa as discussed earlier that act as a watchdog of the telecommunications, broadcasting and postal industries. One of its mandates is to receive complaints from the consumers about services provided by

telecommunications, broadcasting and postal licensees (GOV.ZA, 2006). The government or other independent regulatory bodies enact laws that deal with CIoT. The section on legal framework discussed the requirements such as the Protection of Personal Information Act 4 of 2013 (POPI Act), Consumer Protection Act 68 of 2008 (CPA), and the Electronic Communications Act 36 of 2005 (ECA), and the Electronic Communications and Transactions Act 25 of 2002 (ECT Act).

Standardization efforts should most likely have a certification process and a technology development process. A specific body should oversee the standardization and certification processes in one way or another. However, the standardization efforts should not be a hindrance to innovation but should ensure interoperability among different IoT solutions, and fair marketplace and competition. Standardization of data transfer and storage will reduce the entry barriers to the IoT market place.

Some of the areas of standardization would be in communication, encryption, user consenting mechanisms and storage. The process of standardization and certification should not be left to individual companies as this hinders interoperability. Today, on the internet, some form or certificate authority model is using digital certificates, and so the certification mechanism for IoT can follow a similar mechanism. To be effective, the IoT certification model needs to cover hardware products and software services.

2.9.4 Device manufacturers

Device manufacturers are essential stakeholders in the IoT assemblage, and they need to embed privacy-preserving techniques into their devices. They have a responsibility to develop devices that are safe for consumption. Embedding a privacy-preserving technology, in the beginning, ensures that there is a high level of security throughout the data flow within the CIoT assemblage. These manufacturers must address the following as part of privacy-preserving, security and trust techniques (Perera et al., 2015):

- Upgrade or patch the firmware and software by pushing them over the air with minimum consumer intervention
- Implement secure storage, data deletion, and control access mechanisms at the firmware level
- Inform consumers about the type of data that is collected by the devices
- Explain the kind of data processing that will be employed, how and when data would be extracted out of the devices
- Provide the necessary control for the consumers to disable any hardware components
- Provide a programming interface for third-party developers to acquire data from the devices

2.9.5 IoT cloud services and platform providers

Most of the CIoT solutions connect to a cloud-based solution. The cloud portion is responsible for providing advanced data analysis support for the local software platforms. When we refer to standardization and certification, cloud providers need to comply with them. It is also essential for the cloud providers to use common standards so that consumers can have a choice on the provider to use. The cloud provider needs to comply with the POPI Act, the GDPR and other legislation that seek to give power to the consumers about their data. It is the responsibility of the cloud providers to make sure that they tick all the boxes and comply with the law, failing which may result in hefty fines as stipulated in the regulations such as the POPI Act and the GDPR. Some of the providers store data and analytical platforms outside of South Africa, and this may be a challenge for the consumer. Perera et al. (2015) posit that while consumers make use of cloud providers, they must be free and able to delete and move data from one provider to another over time. These standards should not be country-specific but should span across all geographies in the world.

2.9.6 Application developers

Just like device manufacturers, application developers have the responsibility to produce applications that are safe and do not contain any malware. As part of the standardization and certification, they need to follow strict processes as required by the relevant standardization body. They also need to have their apps certified. Perera et al. (2015) point out that developers have a responsibility to ensure that they present clear and accurate information to the users to acquire explicit user consent. They mention some of the critical information that application developers need to state when asking the consumer to consent. These are:

- The task that the application performs
- The information that the app needs to do the tasks
- The hardware and software that the sensors utilized
- The procedures and techniques that the application used to aggregate and analyse the data
- The kind of information that the app will determine by processing the data

Perera et al. (2015) suggest that acquiring consumer consent should be a continuous and ongoing process. In essence, the application developers must continuously allow the users to withdraw, grant, or change their consent. Also, they argue that consumers must have full access to the data collected by IoT devices.

2.10 Summary

This chapter reviewed prior literature in CIoT. It starts by making a comparison between consumer IoT and industrial IoT to set the scene in the exploration of CIoT. After that, it reviewed the legislation and legal frameworks that influence CIoT at an international level before focusing on the South African context. The researcher discussed the South African POPI Act about CIoT, as well as international regulations. The next exploration was on the technological considerations from a design level and development point of view.

Furthermore, the researcher discussed different architectures in CIoT, including the layered approach to the design. The idea of explaining the structures was to understand the most vulnerable layers or elements of the CIoT assemblages concerning data privacy, security and stakeholders trust. The chapter closed by digging deeper into each stakeholder that is involved in the CIoT assemblage. The next section discusses the research methodology applied in this study.

CHAPTER THREE
3 RESEARCH METHODOLOGY

3.1 Introduction

The literature review in Chapter Two on CIoT indicated the importance of approaching the challenges from the legal and technical point of view. It further highlighted the importance of looking at all layers of the CIoT assemblage in developing a framework to deal with data privacy, security and trust challenges. These approaches provide the underlying principles of the research methodology for this research and give both depth and breadth, while also shaping the design, strategy and techniques used in this research. This chapter presents sections that contribute to the description of the research methodology and define the scope and limitations of the research design adopted in the study. Kothari (2004) describes the research methodology as a way to solve the research problem systematically. It provides researchers with the necessary ammunition to choose methods, materials and scientific tools relevant for the issue selected.

The chapter presents the philosophical assumptions underpinning this research in more detail. This chapter aims to describe the research process or various stages of the study, such as the selection of participants, data collection process and data analysis process. Finally, the chapter discusses the role of the researcher in qualitative research concerning reflexivity. Alvesson and Sköldberg (2017) define reflexivity as involving a self-conscious awareness of the relationship between the researcher and “other”. It is a process of continuous self-analysis. This process is when the researcher reflects more deeply on the experiences encountered when doing the research. Figure 3.1 illustrates the research methodology applied in this study.

The research methodology is defined by Bryman (2008) as a systematic process of solving a problem to increase our understanding of the phenomenon being studied. The methodological themes are the ontological considerations, epistemology, research approach, research design, population and sampling, as well as data collection tools. This

systematic approach provides information concerning the method that the researcher used in undertaking the research and the justification of using a specific strategy. Figure 3.1 summarizes the steps that the researcher took in the study.

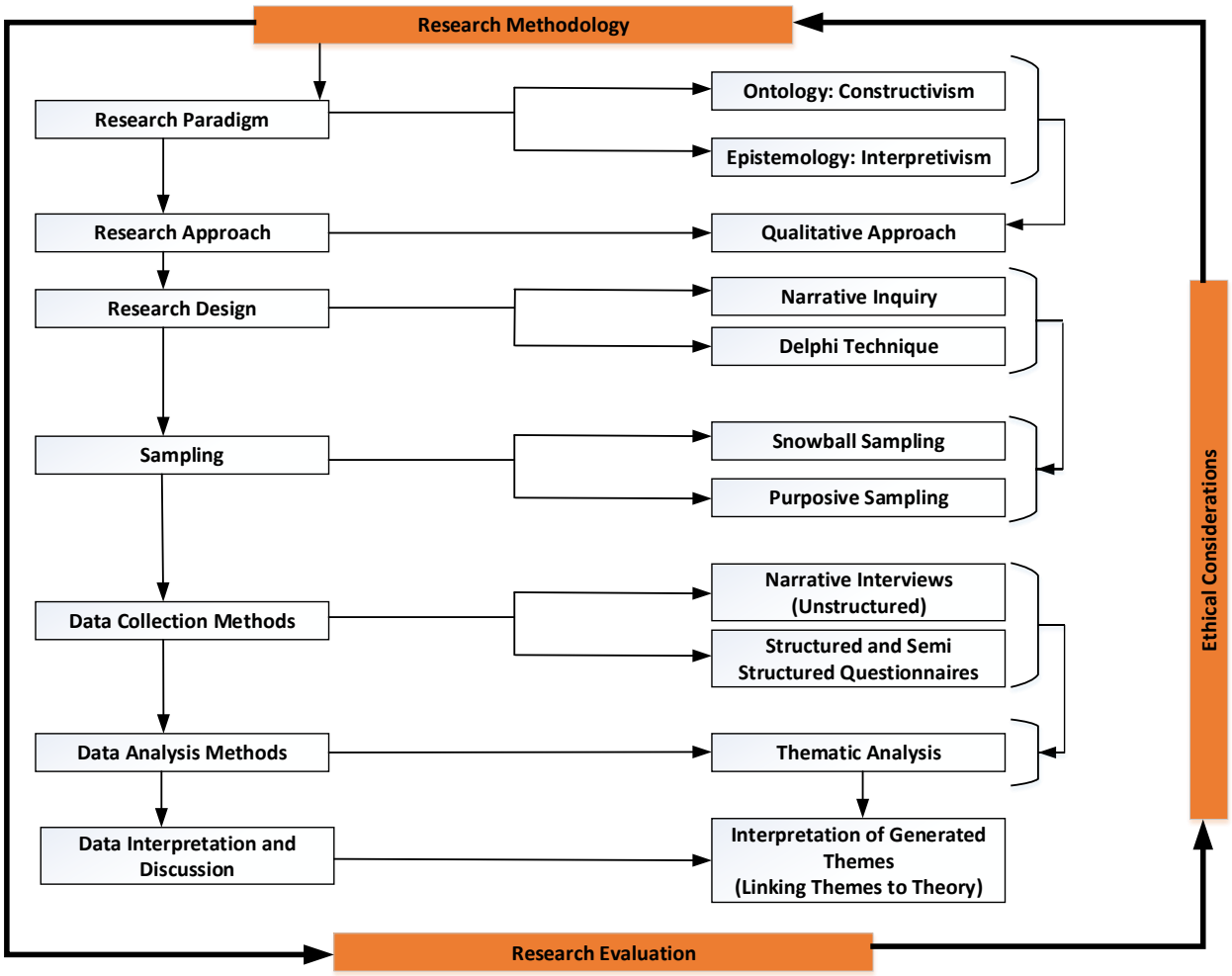


Figure 3.1: Research methodology map for the study (Researcher 2019)

3.2 Philosophical paradigm

This section discusses the philosophical assumptions used in the study, namely ontological, epistemological and axiological assumptions.

3.2.1 Ontology

Ontology is where the research begins and is about the nature of reality. After that, one's epistemological and methodological positions can logically follow (Hollway, 2008; Meretoja, 2014). Pierre (2012) describes ontology as the branch of metaphysics dealing with the nature of being or how one views reality. MacIntosh (2009) indicates that the ontological view is all about what constitutes reality and how we understand existence. He further describes it as the image of social reality upon which the researcher bases a theory. Ontology is about our assumptions about the make-up of the world and the nature of things. There are two ontological views namely; realism which posits that there is the real world, and constructivism which holds that the real world does not exist (Kivunja and Kuyini, 2017; Chilisa and Kawulich, 2012). This study takes the latter – an ontological view that says the reality is constructed, subjective, multiple and relative. The experience of mobile apps users is very diverse and thus having various realities. How smart things interact with humans takes centre stage in the research.

Salgado and Hermans (2009) ascertain that researchers sometimes use constructivism and subjectivism interchangeably. They state that constructivism is an ontological position asserting that the social phenomenon is in constant construction or revision. The social actors are continually accomplishing the meaning of the social aspect. Bryman (2008) alleges that in social constructivism, there is no single reality. If we take users of mobile apps and culture as examples, constructivism infers the continuous change, updating and rejuvenating the existing social structures (Bryman et al., 2008). Dewey's theory of experience (Dewey, 1984) states that there is always an interaction between the actors, and thus continuous changes are bound to happen.

3.2.2 Epistemology

Hussein (2009) describes epistemology as what constitutes valid knowledge and how we obtain it. It has to do with our convictions about how one may find new knowledge about the world. The term alludes to how we know things and the connection between the knower and the known. It is not quite the same as metaphysics or more specifically ontology (what exists, and the idea of the real world) and axiology (values), as well as a methodology (Hollway, 2008; Meretoja, 2014). There are two ways of approaching the epistemological assumption, namely: objectivism and interpretivism (Case and Given, 2016; Cowling, 2016). The research paradigm for problem solving in this research is interpretivism.

Bryman et al. (2008) contend that interpretivism is qualitative and subjective. In essence, there is no single reality in this approach. Cowling (2016) argued that interpretivism is also known as post-positivism. It is a term given to a different epistemology to that of positivism. It is concerned with the theory and method of the interpretation of human action. McQueen (2002) states that the interpretive researchers look for techniques that empower them to comprehend in detail the relationships that people have with their environment. In this study, the researcher sought to understand the part played by those people and other stakeholders in making a social fabric of which they are part. As humans interact with smart things more and more, there exists a relationship as the interaction continues to happen. As much as smart things need to trust each other in communication, humans need to trust smart things too.

The positivist seeks to explain human behaviour while on the other hand; the interpretive seeks to understand human behaviour. This research thus aims to understand (interpretivism) the conduct of actors in a CIoT ecosystem, be it smart things or humans. This section explores the interpretive stance in the field of CIoT. This understanding is critical if we are to develop a framework because of consumers' experiences in using mobile apps for IoT purposes. The researcher seeks to analyse and understand the social

dynamics rather than just “measuring” them. Measuring social dynamics is more in retrospect and reactive. Understanding social dynamics takes a more pro-active approach and seeks to curb privacy and security threats before they happen.

Creswell (2009) posits that there is a connection between interpretivism and qualitative methods of research. He further indicates that researchers use qualitative research to explore and understand individuals or groups, and the meanings of a social or human problem. This exploration helped the researcher in understanding the experiences of people in the age of mobile apps and the internet of things. It also helped in understanding all actors in the CIoT ecosystem and how each contributes to curbing data privacy, security and trust issues. It is about getting insight and in-depth information. Following the nature of the interpretive paradigm, this research further seeks to analyse the experiences of mobile app users when consuming the internet of things.

The researcher used storytelling or narrative enquiry to achieve this understanding. Voegtle, Spaulding and Katherine (2006) mention that in a qualitative approach, the researcher conducts the studies a naturalistic setting. In this case, the researcher asked broad research questions designed to explore, interpret, or understand the social context.

The researcher examined the interpretive paradigm through storytelling or narrative enquiry. Voegtle et al. (2006) mention that in a qualitative approach, the studies happen in a naturalistic setting. What is more naturalistic to humans than storytelling? In narrative inquiry, the researcher asks expansive research inquiries intended to investigate, decipher, or comprehend the social context. The choice of participants is through non-arbitrary techniques dependent on whether the people have data fundamental to the exploration questions. In this study, the participants had exposure to mobile apps and a basic appreciation of how the apps interact with things in the world.

3.2.3 Axiological assumptions

According to Yilmaz (2013), axiological assumptions look at the roles of values with two possible axiological assumptions. Firstly, there is an approach whereby the inquiry is objective and thus value free. That means the use of rigorous procedures eliminates the values and biases of the researcher. This subjective, value-free and unbiased view is the positivist or conventional view. Secondly, there is an approach that assumes the inquiry is value-bound. That means the values are inherent in the context of the study, and thus the researcher's values affect the investigation. This influence by the researcher is the constructivist view.

3.3 Research Approach

As per the previous discussion on epistemological assumptions, this research will be qualitative. The researcher can use many methodological assumptions in the process of qualitative research (Creswell, 2009). Qualitative or subjective research is interpretive as in the researcher is keen on how he interprets, understands and experience the social world. The researcher was adaptable and delicate to the social setting inside which he collected the information. Jennifer (2002) mentions that subjective research is about delivering all-encompassing understandings of rich, logical and detailed information. Creswell and Creswell (2017) state that qualitative research is about engaging participants in a natural setting. This engagement is in contrast to research that happens in a lab environment. In this investigation, the researcher picked the qualitative research philosophy since this approach braces a comprehension and interpretation of meaning and intentions fundamental the interaction of people.

Denzin and Lincoln (2011) posit that qualitative research requires the researcher to turn into the exploration instrument. Additionally, it incorporates room for a description of the researcher's own biases and ideological inclinations. Qualitative research includes informed consent decisions and is receptive to moral or ethical concerns. In qualitative

research, more often than not, the aim is exploratory and descriptive rather than explanatory. The expressive nature of qualitative research achieves two things. Firstly, it enables the researcher to describe or give a portrayal of the experiences of the participants. Secondly, it empowers the readers to comprehend the meaning and significance of the experience, the distinct nature of the issue and the impact thereof. The researcher considered qualitative research reasonable for this study as one of the motivations behind this study was to explore the narratives of consumers of IoT in as far as they relate to data privacy, security and trust. The researcher did not present the findings as absolute truth but as a way of constructing meaning.

The researcher drew on assemblage theory and Dewey's philosophy of experience to inform certain aspects of this study within a broader social constructivist paradigm. According to Denzin and Lincoln (2011), the nature of the research questions and the subject under investigation determines the research methodology or strategy.

3.4 Research design

According to Bell and Bryman (2007), research design provides a framework for the collection and analysis of data. The research strategy adopted for the design was to interview consumers of IoT using narrative inquiry methodology as well as interview experts using the Delphi Technique. The primary data collection techniques used in this research study were unstructured interviews and participant observation (in the case of narrative inquiry) and questionnaires, semi-structured interviews (in the case of the Delphi Technique). The researcher conducted the fieldwork during the period from February 2019 to August 2019.

This research utilized both narrative inquiry methodology and the Delphi method to explore and come up with a framework to guide various stakeholders in securing and protecting personal and devices information. The use of both ways assisted with the triangulation of the research. Many scholars agree on the definition of triangulation as the combination of methodological approaches, theoretical perspectives, data sources,

investigators and analysis methods in the study of the same phenomenon (Hussein, 2009; Thurmond, 2001; Jack and Raturi, 2006). The research design further covers the reasons for selecting data sources, data collection and analysis.

3.4.1 Narrative inquiry

The use of narrative inquiry is central in understanding consumers' experiences as they interact with things. Clandinin (2006) describes narrative inquiry as the study of lived experiences followed narratively. Gottschall (2012) acknowledges that the narrative is about storytelling and storytelling is critical for human survival. Sillars and Hallowell (2009) further indicate that anecdotes or stories provide a way of understanding our place in the bigger scheme of things by structuring our understanding of events. This method increases awareness of the role storytelling plays in shaping social phenomena. To get the most out of storytelling, the interviewer or researcher needs to be tactful in asking the questions. The next section discusses how the researcher designed the interviews and the process he followed to get the most out of the conversations. The interviewer needs to cultivate a high degree of interpersonal skills and be analytical.

Scârneci-Domnişoru (2013) alludes that the narrative inquiry has created new ways of approaching research topics and subjects that had less intricate guides and without predefined-answer surveys. It allows the participants to have greater freedom to express themselves. The researcher spent time in data analysis so that the research findings could reflect how participants constructed meaning. The researcher was conscious of presenting his personal experiences. He tried his best to remain aware of his own biases and experiences.

3.4.1.1 Narrative interviews

Interviews are great tools that researchers can use to collect data in qualitative research. Scârneci-Domnişoru (2013) posits that in qualitative research, narrative interviews are

instruments for data collection. The narrative technique does not impose strict guidelines on the participants but instead encourages them to be the ones who decide what and how to recount. The interviews are unstructured, experiences recounted, opinions are detailed, and ideas explained. While the researcher used the Delphi Technique in the second part of data collection, the research started with the narrative inquiry. The narrative inquiry approach seeks to get emerging behaviour through stories of participants. The idea was to explore and analyse the experiences of IoT consumers as they use mobile apps to interact with things.

Jovchelovitch and Bauer (2000) assert that narrative interviews should be in an environment that provides a setting that encourages and stimulates an interviewee to freely narrate their story about some significant event in their life and social context. When people adopt IoT for their everyday use, their lives are affected in one way or the other. For example, they can monitor their health, save on electricity and water, among other things. The interviewee or participant narrates the story as to how their lives have changed and how the CIoT concerns affect them if they do. The basic idea of narrative inquiry is to reconstruct social events from the perspective of participants as directly as possible.

Muylaert, Sarubbi Jr, Gallo, Neto and Reis (2014) allege that narrative interviews are unstructured tools, in-depth with specific features, which emerge from the life stories of participants and the situational context. Scârneci-Domnişoru (2013) mention that a single question, called a generative question, needs to be prepared before entering the field and this question generates the story by stimulating the participants to speak. The participant needs to unveil experiences by recounting them. The participant decides on what is essential to recount with no influence from the interviewer or researcher. The generative question is normally longer with several sentence.

The researcher or interviewer need to tell the participants that he has enough time to listen to their stories, that he is interested in every detail of the story, that the question

does not have any restrictions on topics. The generative question for this research is as follows:

> *"I want you to tell me how experiences of how your life has changed for the better or worse since you installed the system whereby you control certain things via your smartphone. I want you to tell me about all the things you can control and get more information from while using your smartphone or tablet. Think about your life before having such a system (past), your current situation (present) and your behavioural intentions (future) as if it were a novel. I want you to tell me about your concerns and benefits. There is no need to rush and so please give me details because I am interested in everything important to you. I will no longer ask questions henceforth. I will only take notes on the things I would like to ask you about later. If we do not have time today, maybe in the second interview."*

The interviewer needs to encourage the interviewee during the process, as narrative interviewing is not typical for the participant. The interviewer needs to show that he or she is interested in the story. The interviewer may use encouraging gestures and comments such as "interesting", "wow", and many more. The encouragement ensures the interviewee that the interviewer is concentrating on what the interviewee has to say. It is essential to pose inquiries that will help individuals to recount tales about their encounters in their manner and from their point of view, recalling how it felt at the time. The interview begins with asking one open question. The interviewer can ask subsequent questions only once the interviewee has finished their story.

3.4.1.2 Data collection tools – narrative inquiry

Data collection techniques include interviewing and observing the participants, and thus bringing the researcher and participants together. The researcher takes an interactive role whereby he or she gets to know the participants and the social context in which they live (Schneider and Somers, 2006). Denzin and Lincoln (2011) express that utilizing interviews as a technique for information assortment helps the researcher to gain a more

profound comprehension of the participants' constructions through dialogue and through the language they use in building the various talks. Studies recognize that culture determines communication practices.

In data collection, this study used field texts from individuals who are familiar with using mobile apps to interact with smart things using IoT technology. The participants and the researcher create the field texts to present aspects of the experience. The way that the researcher inquires influences what he or she intends to discover and hence the data collection process is selective. The particular intrigue or lack of engagement of the researcher and members shape the field texts. Drawn in with a narrative inquiry perspective, the researcher gathered field texts from the consumers of IoT technologies through in-depth interviews, perceptions or observations, and discussions or conversations.

As per Chou et al. (2013), in an interview, the interviewee is the storyteller, and the questioner is a guide in this procedure. The two together are partners, forming and developing or constructing a story. The participants hold the power of knowledge since they are the only specialists in their lived experiences. During the interview, the interviewer offers conscious and intrigued consideration rather than his perspectives. Douglas (1985) contends that the most accommodating inquiries would be those that guide the storyteller towards the inclination level. The researcher can find a deeper level of reality in different manners, from specific kinds of inquiries to remarks to thoughtful and responsive listening.

3.4.1.3 Data collection process – narrative inquiry

This process of narrative inquiry is about conducting open-ended interviews. Denzin and Lincoln (2011) contend that unstructured interviews permit the researcher to comprehend the multifaceted nature of the circumstance without forcing any earlier order. Scârneci-Domnişoru (2013) mentions that this is one of the many data collection technique can be used in qualitative research, yielding rich, complex data and leave the subjects in control

of the interview. The narrative dialogue exploits the participants' expertise to express themselves verbally. Narrative data has become indispensable in comprehending past encounters and occasions. The participants' point by point and striking depictions cannot be gotten to as proficiently with other research strategies and procedures. The following sections lay out a defence for choosing specific approaches and techniques.

3.4.1.4 Justification of using the narrative inquiry

How is narrative inquiry different from traditional opinion-based inquiry? While there are many opinions-based research techniques, there are four primary research methods for obtaining views, namely Staticized Group Techniques (SGT), Focus Group, Delphi and Nominal Group Technique (NGT). Narrative inquiry is a new one that is now part of the list. There are many similarities between these methods, but there are also subtle differences. Furthermore, there are also many variations or alternative techniques of these methods. However, none of them considers meanings that people ascribe to their experiences, as does the narrative inquiry method. Supposition or research that is based on opinions, for the most part, include designing an experiment and after that collecting the data. For this sort of research, they are usually arbitrary and subjective, following the ordinal or interval type. Surveys are an effective method for evaluating data from a sample group and testing feelings or inclinations. (Sillars and Hallowell, 2009).

The first reason for using narrative inquiry is from the premise that IoT, mobile apps and the consumers of these technologies make up a complex social system. The researcher used the process of narrative enquiry to understand the patterns that exist within a complex social system. The second reason is that people are natural storytellers and make meaning from the stories they tell to other people. The different experiences and stories bring a new coherent narrative that makes sense to us. This new coherent narrative has direct implications in our decision-making process in the future. The researcher sought to understand how consumers of IoT and users of mobile apps view privacy, security and trust with the hope that the methodology that emerges helps in limiting cybercriminal activities through mobile apps and the IoT technology.

Most studies that use opinion-based methods make use of surveys and structured interviews. The input from the respondents is by nature, subjective, and the researcher aggregates the results. In the Staticized Group Technique, the researcher uses surveys when the instructions and objectives are clear. In this method, the researcher creates a survey form for input purposes. The researcher, however, uses unstructured interviews when the goals of the study are complex or intricate and hard to explain succinctly using the questionnaire forms.

When analysing the field texts, the researcher considered the participants' past and present experiences. The situation or place also needs to be interpreted in a transcript or in field texts. To do this, the researcher needs to search in the participant's landscape for specific situations that give meaning to the narrative. For example, this may be the participant's physical places or the sequence of the sites and the impact these places have on shaping their experiences.

The three commonplaces of narrative inquiry (temporality, sociality, and place) serve as a framework that contributes to the theoretical framework that the researcher developed. Commonplaces are dimensions which need exploration when undertaking a narrative enquiry (Clandinin and Huber, 2002). Attending to experience through investigations into all three commonplaces is, in part, what distinguishes storytelling research from opinion-based evaluative questionnaires. Narrative inquiry can identify patterns of behaviour that are not visible. It is almost impossible to identify those patterns and thoughts using traditional models of investigation. The study sought to find meaning to the philosophy of experiences in a personal and social context from consumers of IoT. Through participating in commonplaces, narrative inquirers can study the complexity of the relational composition of people’s lived experiences both inside and outside of an inquiry and, as well, to imagine the future possibilities.

Continuity or temporality is essential to narrative research. To help this, while investigating the transcript or field texts for information, the researcher needs to think about the participants' past and present encounters. The circumstance or place should also be dissected in a transcript or field texts. To do this, the researcher needs to scan in the participant's scene for specific circumstances that offer significance to the story. For instance, this might be the participant's physical place or the sequence of the places and the impact these places have on shaping their experiences. Since the aim is to find meaning to the philosophy of experience in a personal and social context when it comes to consumers of IoT that use mobile apps, the narrative enquiry can identify hidden patterns of behaviour and thoughts that researchers cannot identify using traditional models of investigation.

Creswell and Poth (2017) posit that narrative inquiry is an open-ended inquiry that seeks to understand the participants' experiences rather than one that seeks measurable and observable data where the research questions are specific and narrow. Ziebland, Coulter, Calabrese and Locock (2013) allude that narrative interviewing is an approach get to the bottom of people’s stories and their experiences. This approach is in contrast to semi-structured and structured techniques that tend to focus on specific topics introduced by the researcher.

Unstructured interviews elicit precious, detailed materials that the researcher can use in qualitative analysis. In an informal conversation, the researcher has a list of topics that they want the respondent to address. Jovchelovitch and Bauer (2000) allude that the motivation for narrative interviewing is due to the critique of the question-response schema of most interviews. In the question-response mode, the interviewer is imposing structures in a threefold-sense:

- By selecting the theme and the topics
- By ordering the questions
- By wording the issues in his or her language

Jovchelovitch and Bauer (2000) mention that to evoke a less forced and in this manner increasingly 'legitimate' rendering of the participant's viewpoint, the impact of the interviewer ought to be negligible, and the setting masterminded to accomplish this limiting of the interviewer's effect. The rules of engagement in narrative interviewing confine the interviewer. The authors further allude that the narration schema substitutes the question-answer schema that defines most interview situations. The hidden presupposition is that the tales uncover the point of view of the interviewee, whereby the participant is utilizing their natural language in the portrayal of occasions. Nonetheless, it would be naive to claim that the narration is without structure. The narrator officially organizes the story. The storytelling follows a self-generating schema. Whoever recounts a decent story consents to the fundamental principles of narrating. The paradox of the narrative is that the constraints of the implicit rules liberate the narration.

3.4.1.5 Preparing the interview

According to Jovchelovitch and Bauer (2000), preparing for narrative interviewing requires investing time, and a preliminary understanding of the main event is necessary both to clarify the gaps that the interview seek to fill and to accomplish a convincing formulation of the initial central topic designed to trigger a self-sustainable narration. The researcher needs to clarify the context of the investigation in broad terms to the participant. Informed consent is necessary, and so the participant must be asked for permission to record the interview. The recordings assist in the proper analysis that happens in Chapter Five.

How do researchers do this? Clandinin (2006) alludes that the narrative method is a recursive, reflexive process. The process moves from the field to field texts (data) to interim and finally research texts. Commonplaces of temporality, sociality and place create a conceptual framework within which the researcher uses different kinds of field texts and various analyses. Narrative inquiry highlights ethical matters as well as shapes new theoretical understandings of people’s experiences. The narrative interview has three phases:

- Narrative phase: The researcher asks a single, carefully constructive narrative question, and the participant responds freely without intrusion from the researcher.
- Narrative follow-up: The researcher asks an additional question to gather more information if necessary.
- Optional second interview: The researcher asks more structured questions to reveal specific data.

In this study, the researcher used interviews to collect data. The next section discussed the phases that the researcher underwent during the interview process.

Phase 1 (main narration): In this phase, the interviewer poses a single, carefully constructed, introductory, narrative question and then remains silent for an extended period. This question aims to inform the interviewee about the focus of the interview. Jovchelovitch and Bauer (2000) allude that when the narration starts, it must not be interrupted until the interviewee pauses and signals the end of the story. When the interviewee has finished, the interviewer may ask a question like: is there anything else? During the narration, the interviewer abstains from any comment other than non-verbal signals of attentive listening and explicit encouragement to continue the narrative.

Phase 2 (questioning phase): The questions that the researcher ask in the second 'session' of the interview are still entirely participant focussed, following strictly the order of the topics freely associated by the narrator. Jovchelovitch and Bauer (2000) say that the interviewer needs to allow the narration to come to a 'natural' end and after that, opens the questioning phase. They say that the questioning phase should not start unless the interviewer has sufficiently probed the end of the main narrative. This phase aims to clarify events like 'what happened before, or after, or then?' The aim is not to be reasoning about the events. It is not yet the time to justify or rationalize, and so the follow-up questions should guard against this. The sole purpose of the questioning phase is to elicit new and additional material beyond the self-generating schema of the story.

Phase 3 (concluding talk): Fehér (2011) ascertain that this is an optional phase. If the interviewer feels that more, non-narrative material is needed, they can conduct a second interview. This time a semi-structured, in-depth discussion is necessary. Jovchelovitch and Bauer (2000) point out that some juicy information may come up after the end of the interview after the researcher has switched off the recording. The extra information may come out because of a relaxed mood leading to exciting discussions in the form of small-talk. This contextual information proves in many cases to be very important for the interpretation of the data, and it can be crucial for a contextual understanding of the participants' accounts. During this phase, the interviewer may use why-questions and may serve as an entry point to the analysis in Chapter Five. It is also the phase whereby the interviewer rates the level of trust or mistrust they command in the eyes of the participant. It is essential information for the interpretation of the narration in its context. It is advisable to have a notebook so that the interviewer does not miss this vital information. The researcher can thus summarize the contents of the small-talk immediately after the interview.

3.4.2 Delphi technique method

The following section deals with the tools applies when using the Delphi technique to collect data, the process thereof, the justification of using the Delphi technique and finally, how the researcher selected the participants.

3.4.2.1 Data collection tools – Delphi technique

In the second part of data collection, the researcher used the Delphi technique method as a data collection tool whereby experts on IoT shared their opinions. The researcher sent emails to a selected group of people whom he considered experts in the IoT field. The aim of using this technique was to seek expert opinion or knowledge to understand a phenomenon under study in greater depth. Hsu and Sandford (2007) allege that the Delphi technique is a widely used and accepted method for gathering data from

respondents within their domain of expertise. They allude that this method is useful when exploring or exposing underlying assumptions or information, leading to different judgments. The idea is to get information that may generate a consensus on the part of the respondents. In essence, the technique is a group communication process, which aims to achieve a convergence of opinion on a specific real-world issue. After the researcher gathered all the information, he correlated the different views on the topic under study.

Skulmoski, Hartman and Krahn (2007) say that the number of rounds that the researcher may use varies depending on the purpose of the research. Most scholars suggest that a three iteration Delphi is sufficient for most analysis (Torrecilla-Salinas, De Troyer, Escalona and Mejías, 2019; Davidson, 2013; Avella, 2016). They point out that three iterations are often sufficient to reach a consensus. Hsu and Sandford (2007) acknowledge that conducting a Delphi study can be time-consuming, mainly when the instrument of a Delphi study consists of many statements. Also, the participants need to dedicate blocks of time to complete the questionnaires, which can be time-consuming. The Delphi method can be an effective and efficient method appropriate for CIoT if the researcher follows and implements rigorous design considerations. This study was very rigorous in designing the questions in all rounds. The researcher dedicated a total of five months to the data collection process.

3.4.2.2 Data collection process – Delphi technique

According to Hsu and Sandford (2007), the feedback process in the Delphi method allows and encourages the selected Delphi participants to reassess their initial judgments about the information provided in previous iterations. Thus, in a Delphi study, the participants can change or modify the results of earlier iterations regarding specific statements in later iterations based on their ability to review and assess the comments and feedback provided by the other Delphi participants. The researcher explained the objectives of the research to the participants as “to identify consumer-related issues in the Internet of Things such as data privacy, security and trust, determine a strategy to assess them,

analyse the technical approaches and analyse the legislative frameworks that may exist in South Africa". Furthermore, the researcher explained the participants' involvement and all the stages involved once they agree to be part of the research. Skulmoski et al. (2007) propose the following process in the use of the Delphi method and the researcher considered these steps in this study:

1. **Developing the research question** – The researcher developed the research question based on his industry experience and thus contributed to his interest in are of his research. The researcher works in the ICT space and works with CIoT related products and services. He found existing theoretical gaps due to conducting a literature review. He saw the gaps that exist when it comes to the CIoT and thus saw it fit to address the differences related to data privacy, security and trust.

2. **Designing the research** – Once the researcher had developed a feasible research question, he created the study from a macro to a micro perspective. This design stage is typically when the researcher determines the research method if it will be qualitative or quantitative. The researcher ordinarily selects the Delphi method if he or she wants to collect the judgments of experts in a group decision-making setting. The Delphi process allows for both qualitative and quantitative methods. In this case, the researcher chose a qualitative approach because he was concerned with how people interpret, understand, experience or produce the CIoT assemblage. The qualitative method allows data generation that is flexible and sensitive to the social context in which data is generated. The researcher explained the three rounds involved in the Delphi process to the participants.

3. **Research sample** – The selection of subjects or participants is critical in Delphi research. This criticality is because expert opinions determine the output of the study. How do we assess expertise? Adler and Ziglio (1996) propose four requirements to meet to consider a participant an expert, namely:

a. *Knowledge and experience with the issues under investigation.* The researcher has access to the experts as he works in the field and interacts with many experts in CIoT.
b. *Capacity and willingness to participate.* The researcher approached the participant who showed commitment to the whole research process. He briefed the participants that they would have to answer questions more than once until all participants reach a consensus. He used only the participant who was willing and could contribute to the research.
c. *Sufficient time to participate in the Delphi research.* The researcher informed the participants that the process might be time-consuming, and thus he chose the participants on their willingness to be part of the process until the end.
d. *Effective communication skills.* Since the participants were professionals in their field, their communications skills were also critical. The researcher requested the participants to avoid the use of jargon and industry-specific abbreviations so that the researcher could interpret the information quickly.

4. **Developing Delphi round one questionnaire** – The researcher was careful and attentive when preparing the initial broad question. We cannot overemphasize that if the participants do not understand the problem or question, they may provide inappropriate answers or even worse, become frustrated. The researcher designed round one to obtain your personal opinion relating to a critical issue in CIoT. The researcher explained that this round has some general open-ended questions that required the participants to answer. Respondents were encouraged to be as broad and detailed as possible. The researcher noted the deadline for every participant to respond in the questionnaire, and he used the three questions below in the first round:
    a. In your opinion, what are risk or issues that come with the adoption of the internet of things by consumers? If you can, give examples.
    b. With the risks or issues in mind, in your opinion, what is the role of regulators, smart device manufacturers, application developers and

consumers, in curbing the problems and risks in consumer internet of things and associated mobile apps

c. What have the SA legislations done to address data privacy, security and trust issues when it comes to consumers of Internet of Things

5. **Delphi pilot study** – It was necessary for the researcher to conduct a pilot study with the aim of testing and adjusting the Delphi questionnaire to improve comprehension, and to work out any procedural problems. The researcher chose to pre-test each subsequent survey.

6. **Releasing and analysing round one questionnaire** – This was when the researcher distributed the polls to the participant. The participants completed and returned the answers to the researcher. The researcher analysed the results from the first round and consolidated them using qualitative coding.

7. **Developing round two questionnaire** – The researcher developed round two surveys based on the responses from round one. The opinions of the participants directed the focus of the research as the goal was to seek expert advice. The researcher earlier explained that there would be a second round, whereby he would summarize the participants' answers from the first round. In round two, the researcher formulated the answers into a series of more specific questions. Round two happened once the researcher had summarized answers from the first round and designed the new questionnaire.

8. **Releasing and analysing round two questionnaire** – The researcher released the survey for the second round to the participants. The participants completed and returned them for further analysis. The researcher allowed the participants to verify if the round one responses did indeed reflect their opinions. The researcher further allowed the participants to change or expand their first-round responses after seeing answers from other researchers. Adler and Ziglio (1996) posit that

continuous verification throughout the Delphi process is critical to improving the reliability of the results.

9. **Developing round three questionnaire** – The researcher used responses from the second round to develop the survey for the third round. He added more questions to verify the round two results. These new questions helped in understanding the boundaries of the research. In the third round, the researcher received second-round answers and worked on the average of the responses. The researcher shared averaged responses from round two, and the respondents could see reactions from other respondents. The researcher allowed the respondents to adjust their answers from the second round if they so wish. This adjustment depended on what the respondents saw from other respondents' answers. The identity of all participants remained confidential at all times. The researcher collected extra information as follow:
    a. Gender
    b. Age
    c. Number of years in the ICT industry
    d. Number of years working directly with the IoT technology

10. **Releasing and analysing round three questionnaire** – The researcher followed a similar process used to analyse the data in round one and round two to analyse the third and final round. The researcher stopped in the third round because he felt the participants reached consensus. If they had not reached a consensus, he would have continued until the respondents reach an agreement. The trick was to use the appropriate technique for the question type such as coding for open-ended, qualitative questions. In the final round, the researcher gave the participants another opportunity to change their answers. The respondents commented on the emerging and collective perspective of the research participants. The aim is to answer the research question. Once there is an answer to the research question, or the process has achieved a theoretical saturation, the

process stops. The process ending means experts have reached a consensus, and have exchanged sufficient information.

11. **Verifying, generalizing and documenting research results** – The researcher tested the Delphi results continuously throughout the Delphi process. It is at this stage that the researcher investigated the extent of generalizing the results.

3.4.2.3 Justification of using the Delphi technique

While consumers continue with the adoption of IoT, we cannot deny that it is a field that is still developing; thus, not everyone understands what it is and what it is not. The expert opinions seek to explain some of the issues and highlight what is practical approaches as opposed to wishful thinking.

Skulmoski et al. (2007) allege that researchers typically use the Delphi method as a quantitative technique. They are also quick to point out that the Delphi method is very much suited to capture rigorously qualitative data. One may use qualitative, quantitative or mixed research methods within a structured process. Rowe and Wright (1999) agree that researchers can also use the Delphi method for qualitative research purposes. The authors further say that the Delphi technique has become an extensive evaluation research tool and point out that some researcher uses it for measuring and aiding forecasting in a variety of disciplines. Hsu and Sandford (2007) contend that the Delphi technique is appropriate as a method for consensus-building utilizing a progression of surveys conveyed using multiple iterations. Delphi, as opposed to other data gathering and analysis techniques, uses multiple iterations intended to build a consensus about a particular topic. The IoT industry is a specialized field within the ICT industry. The expert opinion was critical as an input of the study as the researcher dealt with data privacy, security and trust from different angles such as legal approach, technological approach and consumers approach.

3.4.3 Population and sampling

This section addresses population and sampling for both the narrative inquiry and the Delphi method. There are many types of sampling, but researchers in qualitative research usually focus on relatively small samples. Bryman (2008) defines a population as a total number of subjects or participants that bear a common characteristic that would be of interest to the researcher and out of which the researcher can extract a small fraction to serve as participants.

According to Hsu and Sandford (2007), choosing the appropriate participants is the most crucial step in the entire process because it directly relates to the quality of the results to be generated. The choice of participants is from the judgment and discretion of the researcher. The authors state that the selection of participants, the periods for conducting and completing a study, the possibility of low response rates, and unintentionally guiding feedback from the respondent group are areas, which researchers should consider when designing and implementing a Delphi study.

Sillars and Hallowell (2009) state that when using the Delphi method, the selection of individuals is according to predefined guidelines. The researcher asks the participants to participate in two or more rounds of structured surveys. The guidance needs to be strict and direct the research towards a specific outcome. Hsu and Sandford (2007) state that the Delphi technique focuses on eliciting expert opinions over a short period. When selecting the participants, the degree of expertise of the sample may vary, and there is no definitive way of addressing this variation. One researcher may choose to begin with a predetermined list to rank and rate, while another may generate the initial list through brainstorming. Individuals are considered eligible to be invited to participate in a Delphi study if they have somewhat related backgrounds and experiences concerning the target issue, are capable of contributing helpful inputs and are willing to revise their initial or previous judgments to reach or attain a consensus. The participant should be highly trained and competent within the specialized area of knowledge related to the issue at

hand. The researcher needs to examine and seriously consider the qualifications of Delphi participants carefully.

For this study, the population consisted of users of mobile apps whom the researcher selected through the snowball technique. The researcher selected the research participants based on their supposed ability to provide detailed descriptions of their experiences and willingness to articulate those experiences. These attributes of the participants mean they were able to provide information that is rich and can challenge and enrich the researcher's understanding. Luborsky and Rubinstein (1995) compare different types of sampling that researchers can use in qualitative research, namely:

Convenience (or opportunistic) sampling - this technique uses an open period of recruitment that continues until the researcher achieves a set number of participants. The selection is based on a first-come, first-served basis and used in studies drawing on predefined populations

Purposeful sampling – this technique uses participants that are intentionally selected to represent some specific predefined traits or conditions. The objective here is to accommodate a relatively equal number of different elements or people to enable investigation and description of the conditions and implications happening inside each of the study conditions. The objective, however, is not to determine prevalence, incidence, or causes.

Quota sampling – this method is used for selecting several participants to represent the conditions to be studied rather than to serve the proportion of people in the universe. This is meant to assure the inclusion of people who may be underrepresented by convenience or purposeful sampling techniques.

Snowball sampling – this is sometimes referred to as or word-of-mouth techniques. The aim is to use participants as sources. In other words, participants recommend others they know who may be eligible to be used as participants. For this study, snowball sampling

was used in both the narrative inquiry methodology and the Delphi technique. The idea is that the participants need to be users of mobile apps for IoT purposes.

Snowball sampling technique is a non-probability sampling approach. In the beginning, the researcher approached participants that were known to him to be consumers of IoT, as well those that were known to be experts in the field. The sample got expanded utilizing referral whereby identified participants refer to another consumer of IoT and experts in the field of CIoT. Once one or two participants have been identified, referrals of people who are familiar with using mobile apps for IoT purposes was sort. As soon as the saturation point was reached, the data collection process stopped. It was not difficult for the research to identify experts as he works closely with such experts daily.

There are many existing views on the number of participants needed for a Delphi study. Many scholars (Murphy, Black, Lamping, McKee, Sanderson, Askham et al., 1998) support the notion that the more the participants, the better, suggesting that as the number of judges increases, the reliability of a composite judgement increases. They conclude that the diversity of expert participants is essential and leads to better performance. However, Powell (2003) refutes those claims and says that there is very little actual empirical evidence on the effect of the number of participants on the reliability or validity of consensus processes. He alludes that the qualities of the expert participants are more important than the number of participants. Jairath and Weinstein (1994) agree with Powell (2003) and further propose that participants should be experts who reflect current knowledge and perceptions. When dealing with CIoT, the participants need to be expert in that field, and thus it is hard to determine diversity beyond the area under study. Some scholars say that the number of participants will vary according to the scope of the problem and resources available.

Hsu and Sandford (2007) allude that that one of the primary characteristics and advantages of the Delphi process is subject anonymity which can reduce the effects of dominant individuals which often is a concern when using group-based methods used to

collect and synthesize information. Controlled feedback in the Delphi process minimises the impact of noise.

Since the researcher sought expert opinion in the case of the Delphi method, the sampling considered was a purposive sample. Purposeful sampling is necessary where the researcher selects people not to represent the general population, rather their expert ability to answer the research questions. While the researcher may identify the initial group using purposeful sampling, the researcher may use the snowball sampling technique later to generate subsequent participants.

In qualitative research, especially when using the snowball technique, the number of participants is informed by the extent to which the study addressed the research question. When the study answers the research question, we reach a saturation point. At saturation, it means themes have stopped emerging. The number of participants is, therefore, not pre-determined in this study. Figure 3.2 below portrays the relationship that exists between population and sampling.

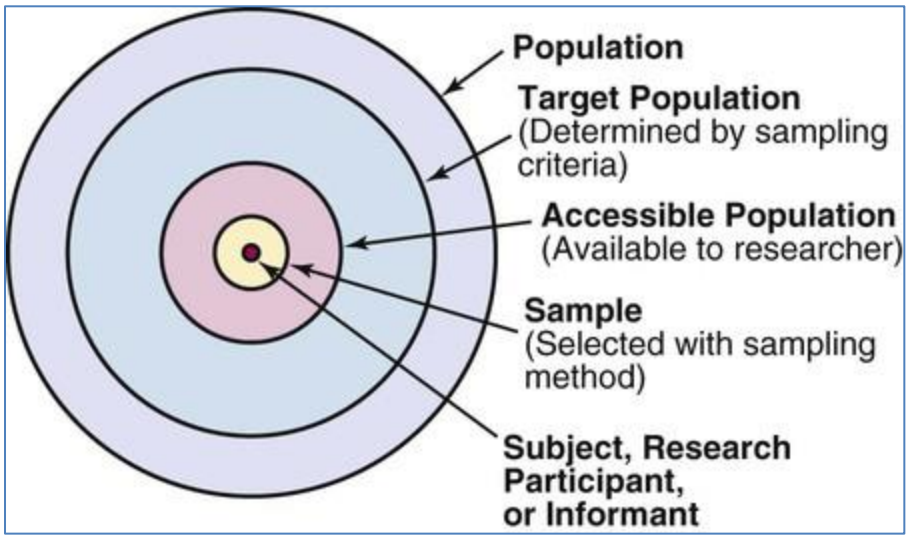


Figure 3.2: Relationship between population and sampling (Elite, 2019)

3.4.4 Thematic analysis

Using the Delphi Technique, the thematic analysis was iterative while collecting the data. There were three rounds of questionnaires sent to the experts via email. The researcher sought out permission before sending the surveys to the participants. He considered participant experts based on their field of work as it related to IoT and the number of years working in that field.

Before the researcher started with data analysis, he transcribed the data from the recorded interviews. Transcription is the process whereby we reduce the data by transcribing the recorded conversations. The researcher further transcribed paralinguistic features, such as voice tone or pauses, to study the rendering of stories not only by content but also by rhetorical form. Transcribing is useful for getting a good grasp of the material, and it opens up a flow of ideas for interpreting the text. The researcher in this study collected data using the narrative inquiry and the Delphi Technique. While the researcher used the two methods to collect data, different procedures can help the researcher in the analysis of data collected. The three standard procedures in qualitative data analysis are thematic analysis, Schütze's proposal and structuralist analysis. This study made use of thematic analysis. However, before using any of the three analysis, the researcher needs to reduce the data by transcribing the recorded interviews.

Some key questions are useful during qualitative data analysis and the researcher addressed these during the investigation. The first question relates to how the themes and common patterns related to the research objectives. In other words, the themes and patterns need to connect or link to the research questions. The second key question is about responses that are inconsistent with typical patterns and themes. Thirdly, the researcher looked at ways of explaining the inconsistencies or used those inconsistencies to expand or redirect the research. Finally, the researcher analysed if the patterns or themes indicated a need for additional data or suggestions for future research.

Thematic analysis is the process of identifying themes within qualitative data. The essential characteristic is the systematic process of coding, examining of meaning and provision of a description of the social reality through the creation of theme. In the thematic analysis, the researcher progressively reduced text units in two or three rounds of serial paraphrasing. After paraphrasing, the researcher developed a category system with which the researcher coded all texts. Firstly, the researcher sought to establish categories for each interview and then collated these categories into a coherent overall category system for all interviews. The researcher then stabilized a final category system through iterating revisions. Finally, he achieved the interpretation of the interviews, fusing relevance structures of the participants and himself, the interviewer.

Braun and Clarke (2006) suggest that researchers should learn this type of analysis as the first step in the qualitative method. They argue that this type of analysis provides core skills that will be useful for conducting many other kinds of analysis. This method involves the identification and reporting of patterns called themes. The researcher retrieved these themes from the primary qualitative data. The researcher utilised the technique to classify and organise data according to key themes, concepts and categories. Denzin and Lincoln (2011) state that qualitative research emphasizes the importance of context in analyzing data.

Jovchelovitch and Bauer (2000) mention that since the narrative interview is a technique for generating stories, it is open concerning the analytical procedures that follow data collection. Braun and Clarke (2006) state that thematic analysis is a method rather than a methodology. That means it is not tied to a particular epistemological or theoretical perspective and thus making it very flexible. The researcher continued to use thematic analysis in the data collected using the Delphi Technique. The Delphi method can employ a variety of different analytic techniques depending on the purpose of the research and type of data collected.

The researcher developed questions from the previous round of the Delphi technique using thematic analysis. Hsu and Sandford (2007) mention that for data analysis to happen, the researcher must have decision rules to assemble and organize the

judgments and insights provided by Delphi participants. The researcher chose the analytic techniques to use for the data collected using the Delphi technique based on the aim of the research, design employed, and type of data collected. Whenever a researcher uses the Delphi technique, he conducts the analysis iteratively throughout the study, as prior waves of data collection must be analysed to inform the questionnaires developed for subsequent waves of the survey. Specific, consistent criteria apply to all qualitative Delphi studies including purposive sampling, new design, anonymous and structured communication between participants, and thematic analysis. Within the methodological literature for the Delphi method, scholars have widely stated that qualitative Delphi studies should utilize thematic analysis. In using the Delphi technique, the primary rigour control is the ability of participants to extend and revise data during the survey, along with the use of consensus in determining what responses and data are valid. The researcher presented the analysis of the data collected using both the narrative inquiry and Delphi method in Chapter Four. The next section discusses the steps needed to analyse the data. Figure 3.3 summarizes the steps involved in the analysis of qualitative data.

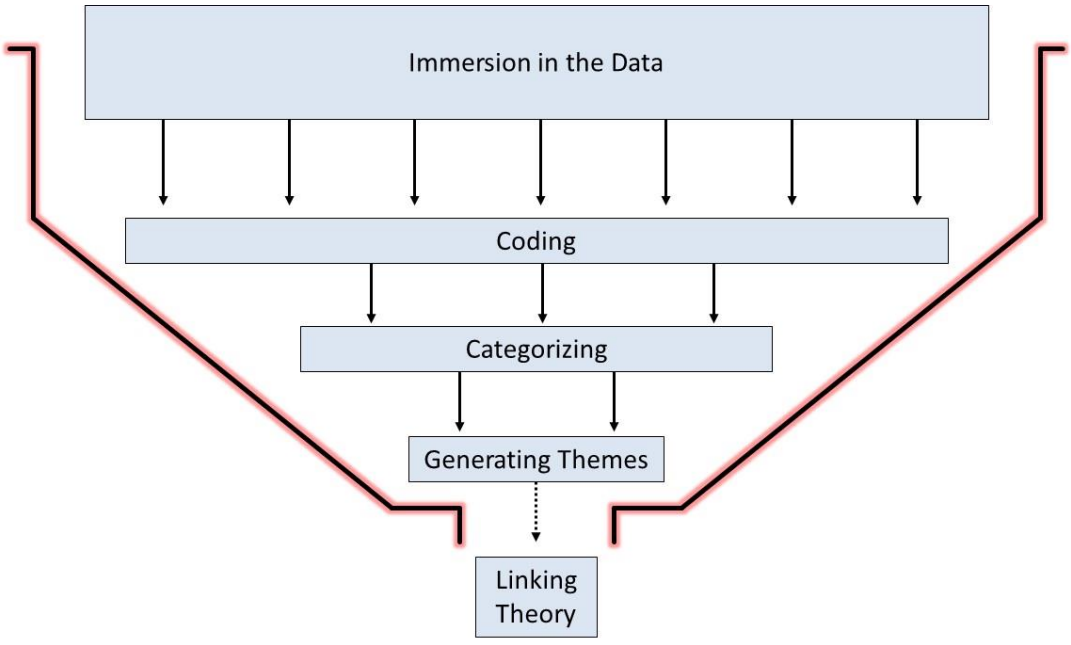


Figure 3.3: Steps in qualitative data analysis using thematic analysis (Braun and Clarke, 2006; Saldaña, 2015; Green, Willis, Hughes, Small, Welch, Gibbs et al., 2007)

3.4.4.1 Immersion in the data

After the researcher transcribed the data (from narrative inquiry), the analysis of the data commenced. Green et al. (2007) state that the first stage in the analysis process is the immersion in the data. Immersion in the information is a time consuming but a very vital process in the research. The researcher needs to understand the collected data in detail. The researcher was the interviewer as part of this study. The researcher recorded observations and experiences at the time of the interview and subsequently, these formed part of the raw data. Repeated reading and re-reading of interview transcripts and contextual data and listening to recordings of the interviews are, therefore, the first step in the analysis.

3.4.4.2 Coding

After the researcher immersed himself in the data, he then did a line-by-line coding whereby he looked at the data with a closer eye. Scholars agree on the definition of coding in general as a process of organizing and sorting your data (Saldaña, 2015; Carroll and Rothe, 2010; Gibbs, 2007; Green et al., 2007). The researcher generates codes from the coding process. According to Saldaña (2015), a code is most often a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and evocative attribute for a portion of language-based or visual data. Green et al. (2007) refer to codes as descriptive labels applied to segments of the transcript. However, they are quick to warn that the coding process is more than using a name. They argue that the coding process requires a clear sense of the context in which the interview data make definite statements.

Carroll and Rothe (2010) describe code as a label that captures the essence of a small portion of content. In reality, codes serve as a way of compiling and organizing the data. Codes allow the researcher to summarize and synthesize what is happening in the data. They are the basis for developing the analysis. Codes have more details, and the

researcher in this study gave a code to everything in the collected data. Some codes may not make it at the end, but they still needed coding at this stage. The data analysis of the data becomes more profound when the codes have more details. In the thematic analysis, the researcher examines participant responses and code them side by side for commonality and consensus.

Saldaña (2015) alludes that the researcher should focus on the purpose statement when coding. That means coding is not just labelling, but it is linking of data to the research questions. Gibbs (2007) state that the researcher is in charge of choosing the forms of codes and sticking with the choice for data consistency. Green et al. (2007) mention that coding forces the researcher to begin to make judgements and tag blocks of transcripts.

As the researcher discovered more information about the topic, he worked through the transcripts, added codes, and refined the meaning of each code. He revisited the previously coded transcripts to verify that the code is still applicable. In some cases, he had to re-code some of the older transcripts may need re-coding. This process involved moving forward and back through the transcripts, drawing on in-depth knowledge connected with the study, returning to the study question, and thinking in terms of systems and theoretical concepts.

The researcher selected texts from the collected data and gave each text a code name that captures the essence of the text. The coding was such that when the researcher encountered a text with the same meaning later on in the collected text, he gave it the same code name. The detail of codes entirely depended on the research question. That means the researcher needed to provide labels for codes related to the research question. There are two types of coding methods, namely deductive and inductive. The flexibility of thematic analysis allows its usage in both inductive and deductive methodologies. The flexibility further enables the researcher to deal with the observational data collected throughout the study.

Deductive coding refers to the coding method wherein the researcher has developed a codebook as a reference to guide him or her through the coding process. The codebook development happens before the researcher starts the data collection process. The codebook can still change as the researcher continues to code, and the new codes added and categories re-organized. In essence, Deductive coding refers to when the researcher is testing a hypothesis. In this case, the researcher develops codes and categories before the data is collected. Thomas (2006) defines deductive coding as an approach to data analyses that set out to test whether data are consistent with prior assumptions, theories, or hypotheses identified or constructed by an investigator.

Another coding method is the inductive coding method. Thomas (2006) refers to inductive coding as an approach that primarily use detailed readings of raw data to derive concepts, themes, or a model through interpretations made from the raw data by an evaluator or researcher. The author state that the inductive approach permits research findings to emerge from the many, dominant, or significant themes inherent in raw data, without the restraints imposed by structured methodologies. The researcher would typically use this method when conducting heuristic or exploratory research. There is no prior codebook in this type of research. The researcher builds codes based on the data collected. In the narrative technique, the researcher used the inductive method because he did not know the experiences of the consumers beforehand. In essence, inductive coding refers to when the researcher generates codes and categories after examining the collected data. The researcher used inductive procedure and included his experience in collecting and analysing the data. The research here is the product of the values of the researcher. When using the inductive approach, the researcher condensed raw textual data into a brief, summary format. He established links between research objectives and summary findings derived from raw data. Thomas (2006) states that the development of a framework of the underlying structure of experiences or processes happens from the evidence of the raw data. Figure 3.4 below highlights the difference between deductive and inductive approaches on how they both link theory and research.

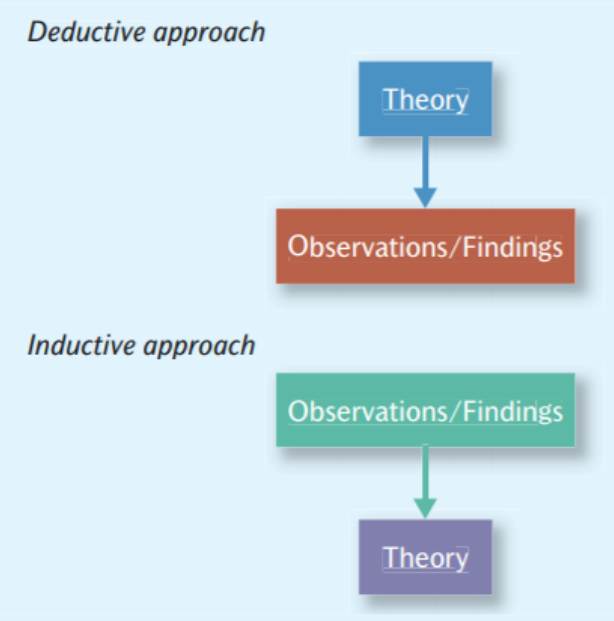


Figure 3.4: Deductive and inductive approaches to the relationship between theory and research (Bryman, 2016)

There are many types of coding, and below are some of the main ones:

- Structure coding
- Magnitude coding
- Evaluation coding
- Process coding
- Invivo coding
- Emotion coding
- Descriptive coding
- Narrative coding

The research uses mainly the descriptive coding for both data collected through narrative inquiry and Delphi Technique, with some narrative coding when dealing with data collected through narrative inquiry.

3.4.4.3 Categorizing

After the researcher did coding, he categorized the codes. At this stage, the collection of codes is most likely messy, and hence the categorization stage is used. The researcher put similar codes into the same categories and moved them around to find out a way that reflected analysis in the best way. When the researcher analyses and sorts the codes into categories, he or she can detect consistent and overarching themes from the data.

The researcher identified concepts from the responses of the participants based on the frequency that they talked about those concepts. Ideas or concepts are the nearest units of analysis of raw data, and categories are more abstract. Notwithstanding, categories give a more significant level of clarification than concepts or ideas alone. Categories require the researcher to use earlier information from the literature and expert consultation about the data to identify connections and different approaches to organizing concepts. The researcher may need to choose if there is a hierarchy in the categories.

The researcher carried out a detailed assessment of the data to categorise how participants talked about aspects of the issue under scrutiny. This linking of codes plans to make a rational classification and is the third step in the investigation of interview data. It is concerned with searching for a ‘solid match’ between codes that share a relationship. It is less likely for all participants to have the same experiences. Sometimes, data contain contradictions and exceptions that need sorting into different categories, generating an explanation for everything that the researcher observed or recorded in the data. The categories evolve and undergo refinement using an iterative process through the researcher's familiarization with the raw data. The consumers of IoT have different experiences, and thus the researcher noted these contradictions and exceptions in the interpretation and discussion chapter.

3.4.4.4 Generating themes and observations

After that, the researcher worked on generative themes or identification of themes. The generation of themes was the final step of the analysis of interview and survey data. Bradley, Curry and Devers (2007) define themes as recurrent unifying concepts or statements about the subject of inquiry. They explain that themes are a set of general propositions that help explain, predict, and interpret events or phenomena of interest. This last step involves shifting to an explanation and interpretation of the issue under investigation.

Furthermore, they characterize the experiences of individual participants by general insights from the whole of the data. Bradley et al. (2007) allude that themes are general propositions that emerge from diverse and detail-rich experiences of participants and provide recurrent and unifying ideas regarding the subject of inquiry. They state that themes evolve from the codes and from the relationship codes, which tag data that link concepts to each other. However, Braun and Clarke (2006) argue that themes do not just emerge, but the researcher generates them. They ascertain that “theme emergence” posits lack of involvement by the researcher. However, in constructivism, the researcher and participants are heavily involved as the instruments of the study.

Willis, Daly, Kealy, Small, Koutroulis, Green et al. (2007) state that the generation of themes requires testing the explanation both with the data and with the theory, explicitly referring to the theoretical concepts relevant to the study. When testing the explanation, the researcher links the results from interviews and surveys to what we already know about the people and other settings. The researcher generated themes from the participants’ comments. The themes came from the interview comments that were common during the interviewing or survey process. The litmus test of the study is in the identification of themes, rather than categories. The themes produced stronger evidence.

The common trends and observations became noticeable after analysing the data. Some themes were common across all participants. Green et al. (2007) ascertain that a “theme”

is the main product of data analysis that yields practical results. Bradley et al. (2007) point out that the researcher may also develop themes by conducting a comparative study of concepts coded in different participant groups or setting codes. For this situation, the researcher recovers information coded with both a conceptual or relationship code and with the participants' characteristics code. The examination can evaluate whether certain concepts, connections among ideas, or positive and negative viewpoints are progressively clear or are experienced contrastingly in one group than in another. Just like in categories, the researcher may need to decide if there is a hierarchy in the themes.

3.4.5 Approach to interpretation

In Chapter Five, the researcher interpreted the findings of the study after presenting and analysing the collected data. When we do research, we seek to produce new knowledge, and researchers articulate this knowledge using theories. After the researcher generated themes, he linked the themes to theories to find meaning and propose a holistic framework to deal with the concerns of consumer IoT. The interpretive paradigm guided the data analysis of the study. The idea was to view the narratives against the context in which it was set, and the subjective viewpoints of the participants. Participants of this research had experiences based on either use of the IoT technology from a consumer perspective or based on the work experiences in relation to the IoT technology.

The intuitive, subjective, particularistic nature of interpretation renders it difficult to model or present it linearly. Braun and Clarke (2006) state that theory and theoretical concepts guide qualitative data analysis. However, they acknowledge that it is “always shaped to some extent by the researcher’s standpoint, disciplinary knowledge and epistemology”. Hence, in the data interpretation part of the research, the researcher seeks to give meaning to the data whereby introspection, extrospection and tacit knowledge join forces. In this process, the researcher links collected data to existing theories in interpreting the data and develop a new approach with the help of the collected data.

Creswell and Creswell (2017) state that proper qualitative research needs to be able to draw interpretations and be consistent with the data that is collected. As alluded in the previous chapter, thematic analysis is capable of detecting and identifying factors that influence issues generated by the participants. The participants' interpretations are thus very significant in terms of giving the most appropriate explanations for their behaviours, actions and thoughts. Alhojailan (2012) makes a distinction between analytical procedures and interpretation. He alludes that analytical methods manipulate data, while interpretation makes sense of data through more abstract conceptualizations.

Denzin and Lincoln (2011) describe interpretation as the terminal phase of qualitative research. They argue that this is probably the most challenging, intricate part of the study. They state that interpretation is an art that is not amenable to formal rules. The processes to define interpretations are ongoing, unpredictable and unfinished. Flick (2002) mentions that data interpretation is the core of qualitative research. We can view interpretation and translation as the transfer of meanings across texts, objects, or domains. This perspective is useful in understanding interpretive processes in consumer research. Despite their different aims, designs, and analytical strategies, consumer researchers using alternative views attempt to understand and represent meanings by studying;

- the meanings that others attach to their experiences,
- how those meanings cohere and form patterns, and
- how symbolic forms, rituals, traditions, and cultural codes (especially those involving consumption) affirm and reproduce cultural themes and culture

Most qualitative studies use inductive reasoning, that is, interpreting the data to derive some theoretical framework or working hypothesis, proposition, or `essence' of the social processes under investigation. Induction happens from the data to reach new findings and generate a theory from the concepts inherent within the data. While it is possible to use a deductive approach with qualitative data, this research used the inductive approach. Some scholars argued that deductive approaches do not maximise the value available from qualitative data and that inductive methods are more likely to reveal new theories and progress understanding about the field.

Vaismoradi, Jones, Turunen and Snelgrove (2016) allude that the description and interpretation of participants' perspectives are features of all qualitative approaches. Some researchers believe that the application of thematic analysis is suitable for those who want to employ a lower level of inference interpretation, rather than a more abstract interpretation. That means those scholars focus on the explicit description of the content of communication with a limited reflection on its implicit meaning.

The theory seeks to emphasize the nature of correlative or causal relationships, often delving into the systematic reasons for the events, experiences, and phenomena of inquiry. In other words, theory seeks to predict and explain phenomena. The researcher tagged the data using relationship codes. These are essential to generating and reporting theory. Each code belonged to a category related to a research question (Bradley et al., 2007). The collected data is interpreted and conceptualized to generate theory.

Chenail (2012) warns that qualitative researchers should be able to refer to their original data and be able "to construct evidence of the code from the data". However, the researcher should still account for his or her perceptions, biases and personal beliefs. Creswell and Poth (2017) contend that the interpretation should include the voices of participants, the reflectivity of the researcher, and elaborate description.

3.5 Ethical consideration

By its very nature, narrative inquiry is about telling a story about oneself. Storytelling may involve telling a story about individual choices and actions, and thus raising moral and ethical dimensions to the research. This research involved human participants, and thus the researcher must observe the University of South Africa's (UNISA) policy on research ethics throughout the research stages. The policy aims to discourage unethical research practice, make ethics an integral part of the planning and methodology of research, and finally protect and promote the rights of research participants. The policy of the University stipulates, among other things, that the University is committed to (UNISA, 2013),

- maintaining an environment for researchers in which they may be autonomous and ethical in their work
- ensuring that researchers continue an ethical research practice
- enduring that the rights and interests of human participants are protected

As part of the research, participants needed to remain anonymous as part of respecting their privacy and confidentiality. After that, the publishing of research findings was such that it could not harm research participants in any way or form. Such results were reported accurately and truthfully, and historical records and study material was preserved and protected without revealing the names of the participants. The researcher respected and protected the dignity, privacy and confidentiality of the participants. The researcher informed the participants in detail about the purpose of the research so that they could make an informed decision on whether they wanted to participate in the study or not. In essence, the researcher sought informed consent from all the participants.

The participant provided verbal consent before the interviews were conducted. That means the participants willingly agreed to be interviewed for this research. It was also critical for the researcher to explain the research purpose and process. Some researchers may opt for written consent, but others advise against using highly formalized ways of securing approval (Miller and Bell, 2002; Corti, Day and Backhouse, 2000; Barnett, Wise, Johnson-Greene and Bucky, 2007). The idea is to foster relationships in which ongoing ethical regard for participants is sustained. Barnett et al. (2007) argue that the strength of qualitative research often lies in the informality of the communication as well as the interactive nature of the research process. Therefore, verbal consent was considered sufficient for this study. The obtained consent included permission to record the interview. The participants were informed of the anonymity of the research.

3.6 Research evaluation

The data collection process was very time consuming, especially in using the Delphi technique. In using the five experts, the researcher had to wait for input from everyone

before designing the next round of questions. The researcher had to remind some of the participants more than once. The researcher gave the participants an option to withdraw at any point during the research process. However, none of of the participants withdrew from the research.

The researcher could not triangulate the experiences of both the consumers and the smart things since the researcher could not interview smart things. As things become smarter and smarter, researchers should be able to interview smart things to get their experiences as they interact with humans. To overcome this challenge, the researcher sought expert opinion using the Delphi Technique.

The researcher interpreted the results from the study using the personal experiences (in the case of consumers) and industry expertise (experts opinion) of the participants. A different research philosophy may come up with mixed results. It may be useful for scholars to approach a similar study with a quantitative philosophy.

Qualitative research reporting has its challenges. These challenges differ somewhat from those faced by quantitative researchers, and this primarily relates to the different forms of data that are being analysed and the interpretative approach to analysis. The researcher is cognisance that when presenting qualitative data, it not as set-out as when giving quantitative data. The depth and richness of qualitative data is not a neat series of graphs as they would be in a quantitative report. The qualitative methods in themselves are useful because of their potential to investigate and explain complex and diverse social phenomena. The challenges thus required the researcher to address the following concerns in the final report:

- The researcher discussed the potential transferability of the qualitative findings to other settings.
- The researcher discussed the methods he used and the justifications thereof.
- The researcher demonstrated that the conclusions drawn within the study are consistent with the evidence using verbatim quotes.

- The researcher presented the interpretative analysis in a transparent way such that the reader could follow the processes leading to the conclusions.
- The researcher used diagrams and other schematics to illustrate the analytical process and findings. This proved to be a handy way of simplifying the complexity of the iterative process of the gradual refinement of analytical categories.

The researcher further discussed in detail any apparent contradictions or inconsistencies that emerged in Chapter Five on interpretation and discussion. Another challenge was that during the narrative interviews, female participants were very hard to find, and the researcher wanted diverse views in terms of gender. This diversity was not an objective of the research, but the researcher noticed that during the snowball sampling process, the participants were male-dominated. The researcher made a deliberate effort to ask if any females could be participants in the study. After the third referred participant in the snowballing process, the researcher actively asked for female participants to have female opinions. The initial females that other participants recommended were not willing participants as they felt they do not have enough experience to contribute invaluable information. Without gender diversity, it would be hard to determine if the concerns of CIoT apply regardless of gender.

3.7 Summary

This chapter highlighted the ontological, epistemological and axiological assumptions of the research. This is critical to prepare the readers on the approach that the researcher took. The researcher highlighted the researcher strategy and the justification of using that strategy. The plan was to use both the narrative inquiry and the Delphi Technique. Furthermore, the researcher described the research approach for this research as qualitative.

The researcher further expanded on the research design explaining in detail how he conducted the research using both the narrative inquiry and the Delphi Technique. The researcher explained the data collection tools and processes in detail for both methods.

The researcher explained that using two methods assisted in the triangulation of the research. The researcher explained the approach to analysing the data and the justification thereof. Thematic analysis was suited in the study and for both data collection tools. Finally, ethical consideration was crucial because the researcher need not cross ethical boundaries of participants. The next chapter analysis and presents the data.

CHAPTER FOUR

4 DATA PRESENTATION AND ANALYSIS

4.1 Introduction

The previous chapter discussed the methodology applied in this study. Qualitative presentations are mainly in narrative form. Qualitative analysis is about reducing data without losing meaning. Green et al. (2007) state that it is of vital importance to have a systematic approach and rigorous analysis of interview data. A systematic approach is critical to the generation of good evidence. In qualitative research, both the researcher and the participants are the instruments. This chapter presents the data and analysis thereof collected during the study. The data collection was in two parts. The first part used the narrative inquiry methodology, whereby the format was in the form of unstructured interviews. The second part used the Delphi technique, whereby experts' opinion was sort using structured and semi-structured interviews. In both cases, the researcher allowed the participants to express themselves beyond any pre-define question. He did this to gain further insights and relevant information that may be useful during data interpretation. Chapter Five of the research evaluated whether and how the data illuminated and answered the research questions. This chapter analyses the collected data into generative themes.

The researcher analysed the data collected from the interviews using thematic analysis, whereby he generated themes. Clandinin and Connelly (2000) state that stories, narratives, metaphors, and conversational interview notes are the units of study. The researcher analysed all these intending to understand and make meaning. The analysis also occurred at a social level because participants interacted with a social context in mind. It is essential to understand the participants within the context of their relationships. The participants have bonds with other stakeholders and with smart things. These bonds imply that the researcher needs to understand people as individuals as well as in relations with things. In the context of this research, the participants are part of the CIoT

assemblage. They interact with smartphones and other smart things in the assemblage. Other stakeholders are also part of the assemblage and influence what happens in the assemblage in one way or another.

It is now appropriate to remind the reader of the purpose of the study at this stage. The primary goal was to explore the data privacy**,** security, and trust for consumers of IoT in South Africa with a view of proposing an integrated framework that promotes safer adoption of CIoT as consumers of IoT continue to interact with smart things. The specific objectives were to:

- Analyse the legislative frameworks for data privacy, security and trust concerning CIoT in South Africa.
- Determine the technical approaches in dealing with data privacy, security and trust in CIoT in South Africa.
- Analyse the dynamics and experiences of consumers of IoT concerning data privacy, security and trust while using mobile apps as the primary interface to communicate with smart devices.
- Analyse the responsibilities of CIoT stakeholders that may influence the challenges that come with of CIoT.
- Develop a framework for data protection and security in CIoT when using mobile apps.

The presentation and analysis of collected data began by transcribing audio interviews, reading the interview transcripts and finally reading the answers from the questionnaires. The latter part happened iteratively throughout the process. After that, the researcher worked on the coding process and categorization of the collected data. The next stage of the analysis generated themes from codes and categories. The aim was to use the created themes to gain a conceptualization of underlying data privacy, security and trust patterns from a legal, technological and social paradigm. The researcher presented the different points of view of the participants. These different viewpoints helped in gauging the accuracy of the analysis. It was critical for the researcher to quote the participants and not dilute the narratives and opinions. According to Baxter and Eyles (1997), quoting

participants helps the researcher to reveal how the respondents expressed meanings in their own words rather than using the words of the researcher.

The researcher collected data from six participants using narrative interviewing and five participants using the Delphi technique. All eleven participants were unique individuals meaning; the researcher used a different set of participants in the narrative inquiry and another in the Delphi technique. When using the Delphi technique, the data collection process was in the form of emails sent to participants. Most scholars agree that the process of qualitative analysis is not linear but continuous and iterative. During narrative interviewing, each interview lasted for about 30 minutes. The overall recording in the narrative inquiry was 187 minutes across the six participants. The Delphi technique used email communication to a group of experts in the field of CIoT. That made the total number of participants between narrative interviewing and Delphi technique eleven. The participants' identities remained confidential throughout the research process and after that. To ensure confidentiality, the researcher referred the participants as "Participant followed by a letter and number" as follows:

- Naming of participants from narrative interviews; Participant A1 through to A6
- Naming of participants from Delphi approach interviews; Participants B1 through to B5

4.2 Background of participants

While the participants' identities remained confidential, this section gives a brief overview of their background without revealing their identities. The participants from groups, that is, narrative inquiry and Delphi method ranged from mid-twenties to the early fifties. Seven participants were male, and four were female.

4.2.1 Sample Group A – Narrative inquiry

This group consisted of users of the CIoT in their capacity, including wearables, home automation and security, fitness gears and connected cars. All participants were users of IoT devices in one way or the other. All of the participants owned multiple IoT devices. All the participants were familiar with the CIoT technology despite using different terminologies. They each explained how they make use of the devices and the technology, their concerns and their future intentions in using the technology. In presenting the data, the researcher quoted the participants from narrative interviewing. Bryman (2016) has a similar view to Baxter and Eyles (1997) on quoting the participants and further state that the inclusion of verbatim quotes from the participants is a beneficial way of illustrating the main themes that came out of the study and in demonstrating the reliability of the conclusions. The researcher was careful as not to overdo this as it could result in an overlong narrative, which could distract the main findings. The researcher described each of the participants below:

- Participant A1 – uses home automation, Hikvision cameras, an IDS alarm system and Roboguard beams. He can control all of these systems using his mobile phone connected to the internet regardless of his location in the world. This participant was once a victim of house robbery, and so the security of his home is of utmost importance. He is in his early 40s and married. The safety of his family was of utmost importance. The schematic diagram in (Figure 4.1) illustrates a basic setup of the cameras that are accessible via a mobile app/smartphone.

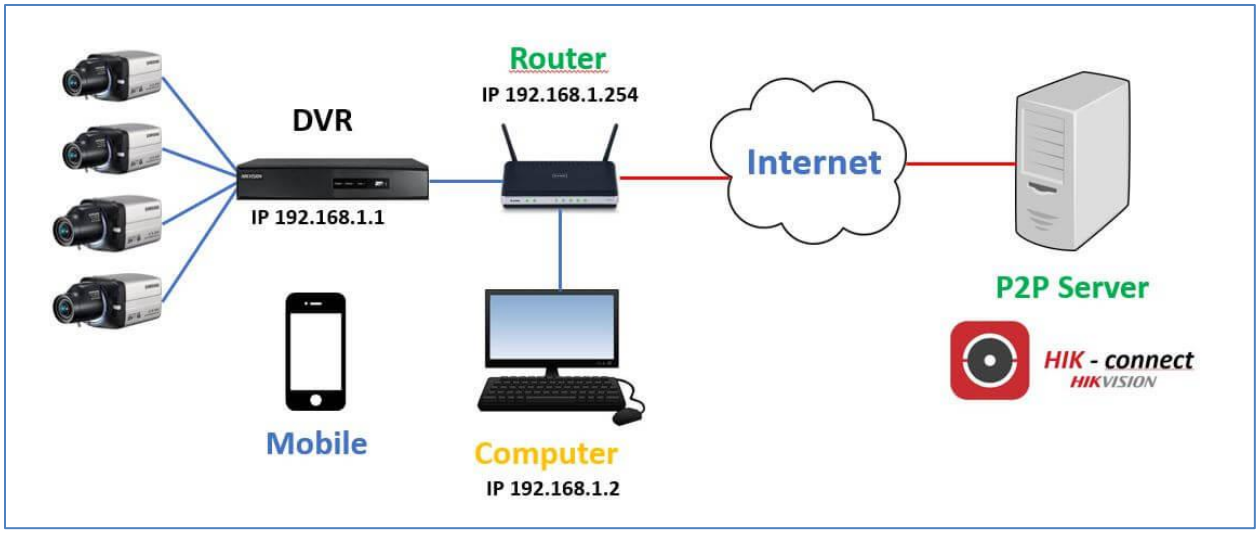


Figure 4.1: Security Setup for Participant A1 (Researcher)

- **Participant A2** – this participant uses wearables such as Fitbits wearables and connects to the Samsung Health app and Discovery app to monitor his training habits. He is male and in his early 30s. He has a history of being sick quite frequently. The doctors previously advised him to be more physically active. He takes his health very serious and thus very keen to monitor his health all the time. This participant defined IoT as very helpful and a way of simplifying his life with the use of devices that connect through the internet. He was very excited about the possibilities that IoT brings to humanity. He gave examples of using drones, smart cars, and home automation as life-changing technologies and making people's lives better. He had the view that connected devices have helped him monitor his fitness habits and provided instant feedback. He intends to make use of IoT more and more while taking cognisance of the possible dangers of using the technology. He sees himself as one of the early adopters of the technology.

- **Participant A3** - Participant A3 said he understands that IoT is about everything connecting to the internet. He is male and in his mid-40s. He said he is not a big user of IoT. However, on further narration, it became clear that he uses IoT a lot when it comes to his physical training. He mentioned that he likes convenience and thus uses IoT because it provides a lot of satisfaction. Also, he stated that he

likes using his phone to make payments as opposed to cash and bankcards. He uses Samsung pay and Vodapay with SnapScan, Zapper and MasterPass. These payments can be through bar code scanning or using virtual credit card loaded on the mobile app. He alluded that it is not very clear for him when a device qualifies as an IoT device.

- **Participant A4** – He uses a connected car using the Mercedes me application. He can monitor his car details such as fuel level, tyre pressure, open windows, vehicle location, among other things. He is also able to apply geofencing that allows him to know if his car is entering a zone that he has applied restrictions. He stated that this is helpful when his nephew is driving his car as it happens now and again. This participant also uses banking apps to do any banking transaction. He does not carry a regular banking card but the FNB mobile application that has both credit and cheque cards embedded in the mobile app. Besides, he uses Dahua (https://www.dahuasecurity.com/sa) cameras at home, Sonoff lights (https://sonoff.tech/), IDS alarms system, Roboguard beams, Alliance Air-conditioning. All these devices connect via Wi-Fi at his home, and he can monitor and control them. The enabling technology is through mobile apps in his smartphone regardless of his location in the world. The diagram (Figure 4.2) shows the Mercedes me connect app that makes it possible for this user to have a connected car.

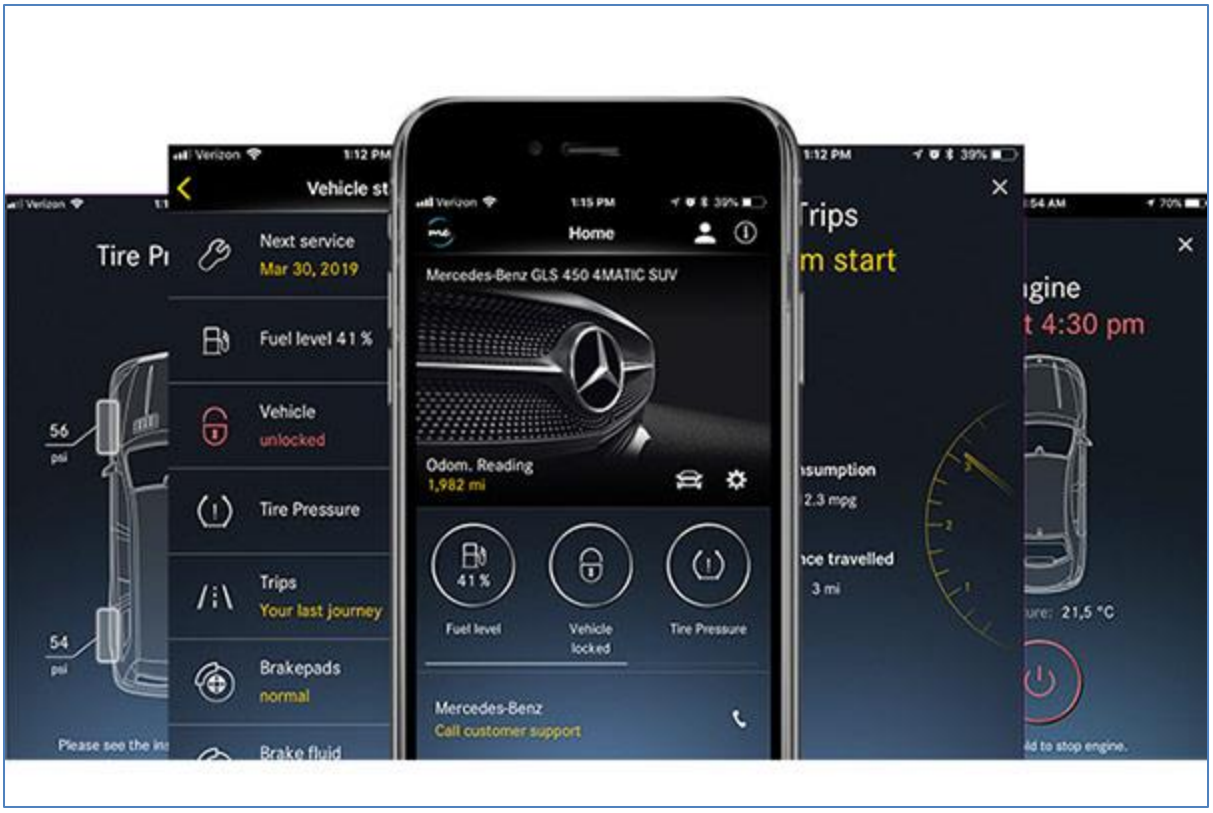


Figure 4.2: A view of the Mercedes me app used by Participant A4 (Researcher)

- **Participant A5** – This participant uses mobile devices to transact, monitor his dog, and kids. She uses V-Kids watch from Vodacom (largest cell phone company in South Africa), which lets parents track where their children. The parents can create virtual fences. Virtual fences assist parents by getting notifications when their children leave specific areas. The device also comprises an SOS button, which allows the child to tell their parents if something happens to them.

Figure 4.3: Vodacom V-Kids (Prior, 2019)

- **Participant A6** – This participant is a single mother in her mid-twenties. She has cameras from Ring (https://za-en.ring.com/) at her home that she uses to monitor her baby and few areas around the house. The primary purpose she is using cameras was to follow the child without having to leave her bedroom. She then bought more cameras to monitor her driveway, lounge and swimming pool. She said if she had enough money, she would install the Ring cameras everywhere. She said, “It gives me a sense of control”. Furthermore, she makes use of an app called Namola. Namola (https://www.namola.com/) is a South African emergency response solution. The Namola solution uses a mobile app as well as a standalone panic button in case the phone is not available or has no power.

4.2.2 Sample Group B – Delphi Approach

This sample consisted of participants that were all experts in IoT with between 10 and 25 years of work experience in the ICT industry. These participants are involved in IoT technology in their daily work environment.

- Participant B1 - is a Team Lead in Solutions Architecture in a large global company operating in South Africa. He has 15 years’ experience in the ICT industry. Part of

the solutions that the team design is IoT solutions. These solutions include controlling and automating HVAC (Heating, ventilation, and air conditioning) systems, SCADA (Supervisory Control and Data Acquisition) systems and PLCs (programmable logic controller) systems, among others.

- Participant B2 is Head of IoT Products Development in a large global company operating in South Africa. He has 25 years' work experience in the ICT industry. The team is responsible for developing IoT products and services.
- Participant B3 is a software engineer, mainly developing mobile apps. He has ten years' experience in software development. Some of the mobile apps he worked on in the past include those apps that control smart devices. He is very passionate about his job and has hope for the future. He stated that technology is changing the world for the better.
- Participant B4 is head of IT security in a global company operating in South Africa. His experience spans across industries in over 20 years. The securing of IT infrastructure includes the IoT ecosystems from platforms to sensors and from networks to applications.
- Participant B5 is an IoT Go-to-Market Manager for consumer IoT products. Her job is to develop a marketing strategy for CIoT products. She analyses CIoT markets, works on pricing strategies, segments the markets, and identifies distribution channels for the CIoT products and services.

4.3 From Coding to Theming

There are various steps involved in the analysis. The measures include the process of coding the data. This process is also known as indexing or labelling the data. The researcher used Narrative Inquiry and the Delphi Technique to collect data. The thematic analysis process was iterative when utilization of the Delphi technique as the researcher revisited and reconstructed the questionnaires from previous rounds. The researcher employed thematic analysis when analysing the data collected from either of the methods with the help of QDA Miner software.

The researcher used a frame called field texts in the data collection process. Clandinin and Connelly (2000) use the term field text to refer to data in the field of qualitative research. In the past, both quantitative and qualitative studies have used field texts research to gather data from the field with the intent of understanding the participants' point of view. From the perspective of narrative inquiry and from within the tradition of the social construction of reality, field texts are always interpretive insofar as participants are concerned. Researchers compose and construct the field texts at a particular moment in time. Clandinin and Connelly (2000) give examples of field texts as oral history, family stories, photographs or personal artefacts, research interviews, journals, autobiographical writing, letters, conversations or field notes.

Braun and Clarke (2006) allude that data analysis is central to credible qualitative research. Scholars describe a qualitative researcher as one of the research instruments because of the researcher's ability to understand, explain and interpret experiences and perceptions. The researcher is the key to uncovering meaning in particular circumstances and contexts.

The researcher captured recurring themes in terms of how research participants constructed their stories and made meaning of their experiences. The researcher broke each theme displayed them in a way that illustrated the interrelationship between each theme. The analysis proceeded from the standpoint of a three-dimensional narrative inquiry space. The first dimension is the temporal dimension. Clandinin and Connelly (2000) state that this dimension focuses "on temporal matters; they focus on the personal and the social in a balance appropriate to the inquiry; and they occur in specific places or sequences of places".

The second dimension refers to the personal and social experiences of individuals, as reflected in their stories. Within this second dimension, narrative researchers are encouraged to focus their analysis in four directions, namely; inward focus, outward focus, backward focus, and forward focus. The back and forward foci refer to the temporality of experiences, past, present, and future, and the intentionality of the person or persons

undergoing such experiences (Clandinin and Connelly, 2000). The third dimension focuses on what Clandinin and Connelly (2000) refer to as “situated within the place”. This third dimension “attends to the specific concrete physical and topological boundaries of inquiry landscapes”.

Coding is the essential first step in managing the analytical process. During the coding process, the researcher indexed and linked some elements of the data that shared some commonality. In research, codes simplify or reduce transcript data to manageable levels intending to achieve a simple conceptual schema (Saldaña, 2015). Coding usually involves the exclusive index coding of segments of data text (“line by line coding”) to be able to retrieve segments sharing common code. Alternatively, coding is a method to open up the data, thus enabling the researcher to think or conceptualise beyond the data itself (Braun and Clarke, 2006). The process allows for a more in-depth analysis, and the detailed analysis happens in several ways.

Raw data obtained from interviews and focus groups (transcripts of what was said), and observations (field notes on what was observed by the researcher) must first be analysed. No consensus exists amongst qualitative researchers concerning the process of data analysis. Instead, there are a variety of approaches to analysis and interpretation. These reflect the particular theoretical perspectives or field within which the researcher is working. In this study, the researcher clearly defined his approach in the analysis for the readers.

Despite that varied methods used in qualitative analysis, many of the qualitative techniques textbooks do attempt to identify some general features that are common to the analytical phase of qualitative research. These include the following:

- **Review of all the information to gain an initial sense of the data** - Based on what the preliminary data entails, the research may feedback the original ideas to the participants for verification purposes.
- **Organization of the data into a manageable form** - This organization happens is when the “data is reduced”, and usually involves developing codes or categories.

- **Interpretation of the data** – The researcher uses theories and personal experience to interpret the data.
- **Present the data in tables and diagrams** – This presentation seeks to summarize and clarify any ambiguity that may exist

Finally, the researcher generated themes. Most scholars refer to this process as theming. Sutton and Austin (2015) describe theming as drawing together of codes from one or more transcripts to present the findings of qualitative research in a coherent and meaningful way. Onwuegbuzie, Frels and Hwang (2016) mention that theming the data involves selecting/deselecting codes to generate a theme. It is essential to go through this process so that, at the conclusion, it will be possible to present the data from the interviews using quotations from the individual transcripts to illustrate the source of the researchers' interpretations. The researcher organized the findings such that each theme became the heading of a section in the report. Underneath each theme, the researcher showed the codes and categories, as well as examples from the transcripts. In the chapter on discussion and interpretation, the researcher used his understanding of what the themes mean.

4.4 Aggregated theming

This section combines the themes generated from both narrative inquiry data and Delphi technique data. The chapter presents each of the themes developed from the research. From the categories grouped according to the research objectives, the researcher generated the following central themes:

- Regulatory frameworks
- Privacy of PII
- Security concerns
- Trust issues
- Convenience and benefits

Table 4-1 summarizes each of the themes with associated sub-themes.

Table 4-1: Themes and Sub-themes

Themes	Regulatory Frameworks	Security Concerns	Personal data concerns	Trust issues	Convenience and benefits
Sub-Themes	Protection of Personal Information Act	Password Management	Identity Theft	Transparency by cloud providers, apps developers, device manufacturers	Perceived ease of use
	Consumer Protection Act	Security Protocol Exchange	Financial risk	Enforcement by regulators	Crime prevention
	Electronic Communications & Transactions Act	Encryption	Selling of personal information	Stakeholder using personal data for nefarious purposes	Simplification of tasks
		Security Updates	Location-based tracking		Perceived contribution to innovation
		Phishing	Medical privacy		
		Distributed Denial of Service	Unfair discrimination due to profiling		
		Physical Security			
		Operating system and storage			
		IoT Malware			

4.4.1 Regulatory frameworks

The experts identified the POPI Act, the CPA, the ECA and the ECT Act as the regulatory frameworks related to data privacy and security. Their view was that these were the closest legal instruments that may deal with CIoT. However, there are severe shortcomings with these instruments in dealing with issues arising from CIoT. One of the questions asked to the experts was in the second round of the Delphi technique;

- What legal instruments exist in South Africa to address the issues of data privacy, security and trust as far as consumer internet of things is concerned?

The response was unanimous in that they identified; *"POPI Act, the CPA, the ECA and the ECT Act",* in the emailed survey.

The third round ask the experts to whether South African regulators were doing enough to regulate the use of consumer IoT. The researcher asked them to rank the statements according to their level of agreement with the statement on a likert scale where 1 was strongly disagree, and 7 was strongly agree. The experts gave this a rating of 2. The comment was that *"the existing legal instruments are not addressing the newer technologies like the CIoT"*.

For example, the POPI Act does not focus on IoT but focuses on anything that threatens personal information. All experts' opinions pointed out that there is currently no security laws and regulations in South Africa to deal with IoT specifically. They agree that while law enforcement agencies may use laws such as the POPI Act, CPA, ECA and ECT Act, these laws are too generic and do not specifically address IoT assemblages, devices, mobile apps or any layer of the IoT assemblage. The view of experts was that lawmakers are always behind when it comes to technological advancements. They agree that in South Africa there has not been a focus on regulating the IoT technology. Participant B2 stated that *"technology is evolving too fast for lawmakers to understand what is happening"*.

They further agreed that if South Africa does not address issues of privacy and security, the national security information, business secrets and personal privacy may be compromised and thus be detrimental to the development of the country. Therefore, South Africa needs a legal point of view to promote the development of the IoT. Participant B5 stated that,

> *"there is a dire need for policies and regulations, and there is still a lot of work to do in that area".*

The experts identified the POPI Act as the closest in regulating personal information in CIoT, followed by the CPA and finally the ECA. The second round asked if South African consumers have any legal recourse when their information become subject of abuse outside the borders of South Africa? The response from participant B1 was that,

> *"while the POPI Act is aligned to the EU GDPR, it does not explicitly address cases of smart things collecting data. It is still a good and closest law to deal with privacy issues but it is still to be implemented after being enacted more than 7 years ago".*

Participant B3 stated that

> *"the POPI Act is toothless and has taken forever to be implanted. Consumers can leave their hope with the CPA for now".*

Surprisingly, none of the experts mentioned the ICASA Act. This study further analysed these pieces of legislation. The study of the POPI Act revealed the eight principles addressed by the Act as follows:

Accountability – The principle of accountability state that the responsible party or the entity processing the information must ensure that they adhere to all eight principles. Since things in CIoT can be autonomous because of machine learning and artificial intelligence, the processing of data can be independent of any person or entity. How do we hold smart things accountable? According to experts, everything has an owner, but they agree that the POPI Act does not address accountability in CIoT. How do we decide on the responsible entity in CIoT? Is it the cloud provider, or the device manufacturer, or

the mobile app developer? The CIoT assemblage may be comprised of multiple device manufacturers. A smart home may have an alarm system from IDS operated by Fidelity ADT, connected with Hikvision cameras and integrated with Amazon Alexa. All entities are collecting personal data in one way or the other. The question arises as to who is the responsible entity. These are challenges that the POPI Act does not address. Future legal instruments that deal with CIoT need to define clearly the responsible entities. The issue of accountability is easy when dealing with one entity, but CIoT is not a single entity.

Processing limitation – In data or information processing, the principle insists that there should be limits. That means a responsible entity should lawfully process information and not excessively. Excessiveness is subject to further interpretation.

Further processing limitation – To further process the information, the principle state that this must be compatible with the original purpose. Further processing is critical as systems update, and new market needs may influence how the data is processed. Due to further interactions with other things and people, the CIoT elements learn new things and can process additional information that was never part of the original purpose. Which entity is responsible for monitoring whether the actions of a CIoT assemblage is still in line with its original purpose and implement a measure that brings it back to its original use? A future CIoT legal instrument need not leave the interpretation of "accountability" to the legal practitioners to interpret but should be as transparent as possible.

Purpose specification – This principle state that there should be a specific lawful purpose of why personal information is collected. In other words, the responsible party should be precise according to the law as to why such information is collected. The principle state that the consumer should be aware of the purpose of this data collection. The consumer may give consent before any entity collects the PII. However, does the consumer know the purpose? However, autonomous smart things may send information to other entities without the involvement of the consumer. In CIoT, the responsible entity may further collect more information during the lifecycle of the assemblage. At that point, there is no consent from the consumer. The legal instrument that addresses CIoT needs

to be specific when it comes to any future updates and data collection. It also needs to be accurate on how the law should address autonomous smart things.

Information quality – The responsible entity must ensure that the information is complete and accurate. The responsible entity may wish to update the information. If that is the case, they need to take into account the purpose of collecting that data. How do we monitor the quality of the data collected from faulty devices? Who is responsible for ensuring that devices are sending quality information?

Openness – This principle state that there should always be openness. This means that the entity processing the information must notify the Information Regulator before any information processing occurs. The entity processing the information should note the processing in a register and inform the data subject that data they collected data about them. This principle seems to imply that is if fine to obtain the subject's personal information without their consent as long as they receive notification about the changes. The researcher's view is that consent need to be sought out before any collection or processing of information.

Security safeguards – This is in lines with the Information Quality principle. The entity is responsible for ensuring the integrity of collected personal information. All security measure should be in place so that no one interferes with the collected data. However, in CIoT, there are multiple entities, which makes it harder to deal with responsible entities. The CIoT legal instrument needs to hold these entities accountable for any compromises in the integrity of personal information. There should be clear segregation of functions amongst all entities involved.

Data subject participation – This principle gives powers to consumers. It states that the data subject has the right to ask and to be provided free of charge any information that the responsible party might have. This is easier when we refer to unprocessed information. Can users request information such as their buying patterns and other predictive analytics data? Since this is processed data, the entities may wish to charge

for such data even though it is a result of one's personal information. The CIoT legal instrument needs to state what can be charged or not charged.

4.4.2 Security concerns

The security of the CIoT assemblage was one of the themes that the researcher generated from the collected data. The participants and the researcher generated the following sub-themes: password management, encryption, security updates and phishing. The next section describes these sub-themes:

Password management – The experts, agreed that password management is a critical part in securing any environment, including the CIoT assemblage. Participant B4 state that,

> *"your system is as week as your weekest point of entry. It is critical for individuals and organizations to have robust passwords to avoid surprises"*.

They alluded that there is a need to increase password length and complexity. Participant B1, B2, B4 and B5 raised concerns regarding consumers to keep a default password after buying a device. Participant B1 stated that,

> *"it is too easy to predict default passwords. Most router for home use come with admin as username, and admin as password. It is critical to change these before you connect the router to the network".*

Participant B2 mentioned that,

> *"I advice consumers to a combination of letters, numbers, and special characters, and make it not less than eight characters".*

Participant B4 stated that,

> *"using defaults passwords is like giving everyone in the community (including criminals) the keys to your house".*

Participant B5 state that *"people need to be educated on the importance of using password that are hard to predict. Most people do not understand the dangers they put themselves in by using their kids names, birthdays, etc".*

In essence, they worried that the default passwords that come with IoT devices are too predictable and hackers easily target those devices. In addition to the long and complex password, they ascertain that the authentication methods should be more robust. There was a consensus among the experts concerning what safe password management means. The suggestions were that the passwords should,

- have at least eight characters
- have a combination of lower cases and upper cases
- include numbers and symbols
- not use words, dates, people or places names
- not use a sequence of letter or numbers
- not use the same password for multiple devices
- be changed more frequently

However, the experts did not see the password as the only security mechanism for CIoT assemblages. They discouraged the use of passwords as the single security protection mechanism in IoT devices due to their low entropy. They stated that IoT providers need something more than strong, unpredictable and frequently changed passwords. They suggested using that those responsible stakeholders need to use a robust password-based authenticated key exchange protocol such as Secure Remote Password (SRP) protocol or with the use of PSK augmented Diffie-Hellman exchanges.

The consumers of CIoT also raised their views when it comes to passwords. For example, Participant A1 stated that,

> *"I make sure I use different passwords for different devices. Many times I even use fake accounts just in case".*

Encryption – The experts agreed on the need to encrypt the devices. Participant B1 mentioned that,

> *"Despite having lost popularity over the years, Blackberry devices are the most secure in terms of encryption. Apple encrypts their devices by default*".

Participant B3 agreed on the criticality of encryption and mentioned that,

> *"I do my encryption including encrypting a smartwatch".*

Participant B4 mentioned that,

> *I look for the possibility of encrypting a device before buying it. While some IoT devices have encryption by default, those that do not have encryption by default need the installer or the consumer to encrypt them before using them".*

Participant B2 was concerned and stated that,

> *"Encryption is not by default, and it is not possible to apply encryption in some devices".*

Security updates - The experts reached an early consensus when it comes to security updates of the IoT devices and associated mobile applications. They agreed that this is a critical part of mitigating security threats. Participant B1 added that,

> *"Updates need to be installed as soon as they become available. However, one needs to check what the update is about and how they affect current settings of the apps or devices.*

Participant B2, B4 and B5 said they update devices and apps when they hear of a need for a new security patch. As much as they do the updates, it is not necessarily immediate. Participant B3's concern was in disturbing current operations of the devices and apps because of the updates. He is more of a follower because he stated that,

> *"I wait for a week to a month before applying the security updates. I wait to avoid breaking things. I understand that updates should make things more secure. However, sometimes things break while we try to fix other things".*

All participants agree that software updates may come with new features as well as security updates. The new features may be a way of upselling more and more services. They stated that it is essential to review those updates to see if they are necessary for one's needs. However, some had a view that such reviews are for people who have a practical technical understanding of why the updates are required if need be.

Phishing and hacking – The experts were worried that inexperienced consumers of IoT might easily be victims of phishing. All participants were concerned about the financial implications that may happen to the naive IoT consumers. For example, criminals may gain access to personal information that that may use to gain access to banking information, among other things. Participant B5 mentioned that,

> *"Phishing can destroy a person's life. Identity theft is real, and personal information needs safeguarding from criminals".*

The participants agree that personal information is essential, and consumers of IoT need to be careful when connecting online or using smart devices. Participant B3 noted that,

> *"Hackers can get personal information either through mobiles apps or through the internet. It is easy these days for people to steal information that reside online".*

The expert participants agree that all apps should give options to the consumers to accept all permissions. For examples, the applications should prompt the consumer on whether they want to allow it to access the camera functions or not. In this way, the consumer has some level of choice on what they allow and not allow on their smart devices or phones. They agree that there is a problem when the apps give consumers only one option; that is, you either agree on everything or not. If the consumer does not agree, they cannot use any function of the app in question. The more options the service provider gives the consumer, the better. In other words, consumers may use different parts of the app other than the camera.

The experts warned that consumers should uninstall mobile apps that they do not use. Besides, to avoid phishing, consumers need to read the reviews of the apps and look at the reputation of the app developer. Participant B3 mentioned that,

> *"The consumer needs to make sure that the developer of the apps is trustworthy, especially in the google app store. The Apple store is more stringer on the apps that developers can publish on the store".*

Participant B3 warned consumers that,

> *"They need to turn off all their devices that are not in use. This includes smart TVs, personal computers and tablets. It may not be possible to turn off all smart devices, but some may be connected through Wi-Fi at homes but are hardly used".*

Participant A6 agreed with Participant B3 and stated that,

> *"When I'm not in the house, I leave the cameras on so that I can view my house for security reasons. However, I turn off anything that I do not require remote access to. In that way, I avoid criminals from hacking into my home by limiting the number of connected devices".*

Participant A4 raised a concern on what hackers are capable of doing. While he acknowledged that a connected car helps curb criminal activities like stealing of vehicles, he also raised the matter of criminals hacking into the connected car by stating the following,

> *"In South Africa, thieves steal cars daily. Based on that reality, I feel a little bit in control, knowing that I can switch off my car remotely. I hope no one gets hurt during the robbery. However, I am also aware that there is a possibility of people hacking into the car and stopping me as the owner. I hope that security experts can stay ahead of criminals when it comes to technology. In the past, I had the feeling that criminals were always ahead".*

4.4.3 Trust issues

Participants A1, A2, A3 and A5 mentioned that they trust the internal policies already implemented by OEMs of either IoT devices or the apps used to control those devices. Participant A4 and A6 were of the view that trusting the global brands that provide CIoT in one way of the other is equivalent to being naïve, and the onus should always be with the consumers to protect themselves.

Participant A3 felt that he is co-creating the future technology by allowing OEMs to use his data and personal information. He stated that:

> *"I feel like I am part of the creation of new technologies and innovations. I do not believe I should be paying for the devices. The providers should incentivise us for allowing them to use our data. These companies use our data to innovate and provide better services in future, and hence I feel I have a responsibility to contribute in my way to innovation. I am happy to pay for the extra value-added services but not the hardware".*

Participant A2 voiced that,

> *"Consumers, as part of the stakeholders, may use the devices in an untrustworthy way. An example I have in mind is the use of Discovery Health app that rewards physically active consumers. Some people put the wearables on dogs and accumulate many steps in a day and thus gaining points that help reduce the premium or get other rewards. Putting the wearables on the dogs defeats the purpose of rewarding active members. This has greatly compromised trust between the service provider (Discovery Health) and the member or consumer".*

The underlying contract is that the consumer gives up a little privacy and gets valuable information. Participant A2 further ascertained that,

> *"Like most people, I value my data. When I use an IoT provider's site or device, there exists a psychological contract that the provider can use my information. The*

terms and condition of most if not all providers state that they can use my data for various purposes, including research purposes, marketing, and sharing with their partners. I trust that the service providers will safeguard my information and are not going to use my information to damage my reputation.

Almost all health apps are free. However, Participant A2 mentioned that,

"Free is not necessarily free. Companies will always find a way of monetizing your data. For example, Discovery Insure track drivers' behaviour with the promise of lowering the premiums if they prove to be good drivers. However, the company might use your information to build a case for future claims so that they can reject those future claims".

Participant A4 uses the Mercedes me connect apps to interact with his car. He alluded that,

"As far as I'm concerned, the technology of connected cars can go a long way in curbing crimes in South Africa. Historically, people depended a lot from companies such as Tracker to locate stolen vehicles or investigate crimes committed. Over the years, Tracker has been working very closely with insurance companies, and those insurance companies have increasingly declined claims based on the data they get from Tracker".

However, most participants agreed that there is a need to service providers to be clear in detailing how they will use the consumers' data. The stakeholder trust looks at how different stakeholders use PII and how that information benefits the consumer. At what cost is personal information used and can the end consumer trust that service providers or any stakeholders positively use their data? Participant A2 was more vocal on the issue of costs as he felt he need to benefit financially after sharing his information with IoT service providers. He voiced out his perceived costs in the following manner,

"If companies are to use my data, I have to benefit somehow. I am somehow helping them to make better products and provide better services. I feel I am co-creating with them. The prices I pay for hardware is just too much for a person

who is indirectly contributing to making better products and providing better services in future. I trust global brands such as Apples or Samsung and believe they cannot use or share my information for malicious use".

Participant A2 trusts global brands. This is, in essence, shows that Participant A2 sees stakeholder trust as related to the branding of those stakeholders. However, the perceived costs can be a deterrent in the adaptation of CIoT. Consumers of IoT are critical stakeholders in the CIoT assemblage, and thus their buy-in is of utmost importance.

The participants addressed stakeholder trust as a way of trusting private companies in the form of OEMs, apps developers, or cloud providers to keep their data secure. Companies would typically use the collected data to understand better and service their customers and upsell new services in future. Most participants did not welcome the idea of companies tracking them. Participant A1, A3, A4, A5 felt that companies collect too much personal data. Participant A2 was of the views that data collection, especially by trusted brands, is a good thing as they can use that data to advance new technological innovation and service their customers better. He had a view that he was part of co-creation.

Participant A4 felt comfortable having the location-based information shared with Mercedes. He mentioned that this could be for his protection when something wrong happens. However, he warned against using similar technology with insurance companies. He felt insurance companies, especially in South Africa, are untrustworthy.

Some participants were not aware of where their personal information resided. Some participants stated that their data lived in the cloud. Others had a view that their data lived in their phones or any of the devices they were controlling. None of the participants was confident enough to state with certainty where their data resided. Furthermore, the participants struggle to say confidently how CIoT services providers were using their data. However, Participant A2's trust in big corporates was visible and stated that,

"The benefits are much higher than the risks, and these are global companies with advanced internal policies that respect people's privacy. Maybe I'm naïve, but I feel I'm helping them to create better services in the future".

4.4.4 Privacy of personally identifiable information

Dinev and Hart (2006) allude to the trade-off between giving away one's private information for associated benefits. They describe two views, namely, privacy benefit and privacy risks. The authors argue with the notion that absolute privacy is unattainable. Individuals make choices in which they surrender a certain degree of privacy in exchange for outcomes that they perceive to be worth the risk of information disclosure. Some of the participants felt that it is up to the consumers to protect their information. They felt too much protection of information might stifle innovation. Participant A3 noted that,

"Most IoT devices he has come across display privacy policy that the consumer must agree to whenever he switches them on. He made an example of a "Mercedes me connect" app".

During the narration, most of the participants stated that the terms and conditions or privacy policies that come with software and devices are too long and it is impractical to go through them before using the CIoT system. The general feeling was that these privacy policies are time consuming and pointless. The participants generally all felt that they would like to keep their data private, and the critical point was that they thought their personal information was a valuable asset. Participant A5 pointed out that,

"I am not aware whether my personal information resides on the smart device or somewhere else".

All consumers felt that service providers track them when they use IoT devices. They trace their behavioural patterns, locations, spending habits, health, to name but a few. In most cases, they do these without consumers understanding.

Participant A2 acknowledged that his FitBit wearables track his heart rate, track how he sleeps and measure his physical activity. He stated that:

> *I am well aware that they follow my actions and my health status. I am okay with it because they noted these in the terms and conditions that apply before using the device.*

Participant A1 and A6 were concerned about criminal stealing their information. They ascertained that because of the concerns, they started using fake email accounts and other accounts. For them to register so that they could use websites or mobile apps to access the CIoT system, they would use accounts that do not relate to anything close to their personal information. Some of the participants resorted to creating false email accounts and disabling usage tracking where possible. For example, Participant A4 was concerned with location-related data and stated the main reason for his concerns by saying that,

> *"Location-related data such as when using the Navigation system in a car, or using wearables that track me when doing road running worries me a bit. This worry is mainly because these reveal things like my place of work, the places I frequently visit, my home and any other and daily routines. I do not know what would happen if criminals hack me and trace me. Additionally, hackers could easily impersonate me after hacking the IoT system and gaining access to all my data. They could commit crimes using my information by pretending to be me".*

Sharing of personal information was less of a concern for Participant A3. He had the view that,

> *"The global brands take all the necessary steps to make sure the information shared with their partners is not used for nefarious purposes. I feel like I am making a positive contribution to innovation when I share my information with a service provider such as the IoT service providers. In future, they can improve the services using the provided data. I am also aware that these companies can resell my information. However, I believe it's for the greater good".*

Participant A2 justified the adoption of CIoT by looking at the benefits and comparing them to the risk. He voiced the following justification,

> *"I am worried as to how these companies use my personal information, but the convenience of using the services outshine the risks. For example, we still buy and drive cars even though car accidents happen all the time. We still board aeroplanes despite some reported air crashes."*

Participant A1 felt that the use of home automation systems and connecting them to the internet poses security risks and were a danger to the homeowners. However, he was quick to say that the benefits of securing his home from burglars outweighed the risks of data privacy threats.

Participant A5 felt that companies are not transparent in their use of personal data. She stated that:

> *"They should always declare what they are going to do with our data. The data belongs to me, and thus I feel I have a right to know what is happening to any data related to me. I think most if not all companies are suspect when it comes to declaring their intentions concerning our data. My other problem is that if they happen to declare they use jargon which makes it hard to decipher what they are trying to convey".*

None of the participants could mention what the IoT providers do with the data that they collect. Participant A3 raised his worries and state that,

> *"I worry about the things that can be done using my personal information. The damage can be very dire, and I have heard of stories whereby people's identities landed in the wrong hands resulting in stolen identities. My brother was once a victim, but luckily for him, he took action before the damage was too much".*

Participant A5, who was once a victim of stolen identity and a victim of house robbery had an intense concern when it comes to security and privacy. His experiences from the past influences the level of intensity of his worries. He agrees that there is a concern about the

physical safety of his house. The challenge or dilemma is in balancing the online security and data privacy concerns with the physical break-in at his home. He uses camera systems that he can access using his mobile phone. The connection to his house from the phone is via the internet. His worry is on the possibility of someone stealing his online profile. However, he sees even a more significant danger when people can break into his home and rob his family at gunpoint. He mentions the following,

> *"I was once a victim of both stolen identity and a victim of house robbery. The question for me is to balance the level of trust in the systems I use to protect my home. I tried to use fake profiles as much as I can to avoid criminals interfering with my real profile or identity".*

Information can be stored either in the cloud or locally on the devices. However, devices have limited information, as they do not have enough capacity to store data that they generate. The necessary information stored in the devices may be essential, but hackers use any information to gain access to the bigger system and hence the whole CIoT assemblage. The participant was concerned with the necessary information stored in the IoT devices. Many participants felt that CIoT services providers have access and control to too much personal information. This study has found that individuals who have previously been victims of personal information breaches have concerns regarding the privacy of their data on IoT devices. CIoT service providers need to be more transparent to their users and return more privacy controls to the end-user. Most participants felt that big global brand give them a level of comfort when it comes to security threats. Any perceived security threat this is constraining and limiting as opposed to positive and enabling.

4.4.5 Convenience and benefits

Participant A5 was more concerned with data privacy and security online. The perceived risks as alluded by Participant A5 is significant due to the experiences from the past. He state that,

“My pass experience make me feel uneasy. However, I try to balance the fraud related concerns with the everyday concerns of other criminal activities like house breakins. My security system need to protect me from violent crime while I also worry about cyber criminals breaking through my security system”.

Participant A2 and A3 felt the perceived severity is not critical. The benefits are much more significant than the risks. This balancing act is about consequences, implying that some consumers may weigh the risks against the benefits. Participant A2 mentioned that,

“everything in life comes with some level of risks. I do not want to be paranoid about security issues such that I do not enjoy the convenience that technology brings. I like the convienience of controlling things via my phone. Just because there is car accidents daily does not mean we’ll stop using cars”.

Participant A3 stated that,

“mobile apps and smart things are here to stay. If you do not adapt you’ll be left out, and you’ll not enjoy the convience that they bring. Imagine being able to control my gyser, lights, refrigerator remotely. What we are currently using is just the beginning. In the next few years, we’ll be doing more amazing things with this technology”.

4.5 Summary

Chapter Four described the presentation and analysis of the collected data. The chapter started by summarizing the nature of the participants chosen for the research. The participants for collecting data using narrative inquiry were selected based on their usage of connected things with their mobile apps. The participants were very diverse from those who use connected cars, home automation systems, health or mobile apps used for physical fitness purposes. The researcher chose the participants that he used in the Delphi technique based on their expertise in the field of IoT. The researcher chose the participants from the industry.

In the data analysis, the researcher transcribed the narrative interviews and then immersed himself in the collected data. After that, he started the coding process. He categorized the codes according to the research questions. Some codes were group together to fit them into appropriate categories. Finally, the researcher generated the themes from the categories, and he discussed each theme in this chapter. The researcher found five themes, namely personal security concerns, data privacy concerns, trust issues, convenience and benefits, regulatory matters. The themes showed that as much as consumers worry about personal privacy, security and trust, the benefits outweigh the worries. Most participants have not had negative experiences when using CIoT. The experts' opinion revealed that South Africa as a country is not doing enough to deal with the challenges of CIoT. The next chapter interprets and discusses the findings of the study.

CHAPTER FIVE
5 INTERPRETATION AND DISCUSSION

5.1 Introduction

The previous chapter analysed and presented data collected through Delphi and narrative inquiry. The aim of this chapter is for interpretation and discussion of the data collected to gain more insight and understanding into the responses of the participants. Clandinin and Connelly (2000) allude that the narrative inquiry approach to qualitative research view all these field texts as socially constructed and guided by the particular interpretations of those who put these texts together. The understanding in narrative inquiry is that whenever we try to understand the world, we deal with interpretations. The researcher used thematic analysis to analyse data collected via narrative enquiry and the Delphi method to generate themes. The researcher discusses these themes and sub-themes and identifies any relevant inter-relationships.

5.2 Interpreting participants' experiences

Novak and Hoffman (2019) state that according to the assemblage theory, we can have either positive and enabling experiences or negative and constraining experiences. When we use CIoT for the benefit of consumers and society, we get a positive experience that enables people to have better lives in one way or the other. The authors also acknowledge that when criminals take advantage of personal information and use such information to commit crimes, the experiences are negative and constraining. The participants who were consumers of IoT pointed on experiences that were mostly positive and enabling. For example, Participant A4 voiced out a positive and enabling experience by stating that,

> *"I feel a little bit in control knowing that I can switch off my car remotely…. I hope that by the security experts can stay ahead of criminals when it comes to the technology. In the past, I have a feeling that criminals were always ahead".*

Participant A3 stated another example of a positive and enabling experience like this,

> *"Since I installed cameras and connected my alarm system to the security house, there have been no break-ins. I can use my phone to arm and disarm the alarm system, view what is happening through cameras and communicate with possible threats to security. This capability has helped in avoiding break-ins before they happen. I have a better sense or feeling of security" - Participant A3*

Most participants had positive and enabling experiences. However, Participant A5 had a negative and constraining experience and stated that,

> *"I was once a victim of stolen identity….. The question for me is to balance the level of trust in the systems I use to protect my home. I tried to use fake profiles as much as I can to avoid criminals interfering with my real profile or identity".*

These experiences, whether positive or negative, influence the future behavioural intentions of consumers. They determine whether the consumers will be willing to adopt other CIoT systems or not. The research focuses on those experiences that are negative and constraining. Those experiences pose a threat to the following:

- the personal privacy of the consumers of IoT
- security of the assemblages and finally to
- trust issues among the stakeholders of the assemblage

5.3 Interpreting the themes

This section interprets the themes that the researcher identified during data analysis. The five main themes were personal security concerns, data privacy concerns, trust issues, convenience and benefits, regulatory matters, and general attitudes towards IoT technologies that inform future behavioural intentions. The researcher acknowledges that the interpretation of the consumers' experiences in this study is by nature subjective.

5.3.1 Regulatory frameworks

This study established that in South Africa, there are various laws that law enforcers may use in CIoT, and these include the POPI Act, the CPA, ECA and the ECT Act. These laws do not necessarily address IoT specifically. They are, in fact, outdated and fragmented. It is no surprise as these legal instruments came to existence before CIoT maturity being at the present levels. They do not necessarily directly cater to CIoT, and thus the room for interpretation of the law is too broad. It is in contrast to the European Union, the United Kingdom and the United States (especially the State of California), which have been working hard to come up with legal instruments that address IoT specifically.

In South Africa, the Authority (ICASA) needs to work on legal instruments to deal with the concerns of CIoT. The Memorandum of Understating that ICASA and SABS signed need to be clear on the responsibility of stakeholders to remove any doubt in the interpretation of the law. For example, when a consumer of IoT suffer financial losses, identity theft because of improper business practices, the laws of the country need to be clear on who is liable for such loses and protect the consumer from the negligence of big businesses. The Authority and other legal bodies need to provide a framework of legislation, policies and government authorities to regulate consumer-supplier interaction. Legal instruments should be such that they discourage businesses entirely from engaging in improper business practices. Such practices may include enterprises providing misleading information, advertising, direct marketing, use of inferior products and unclear instructions on the use of the services. The experts stated that none of the legal instruments in their current state could protect consumers of IoT. These instruments are just the closest available in the absence of proper legal tools.

The literature review revealed that some developed countries such as the UK, the USA and the EU have recently developed legal instruments that are specific to IoT. These instruments are in addition to all other tools that seek to protect the consumers. The

threats of that come with the adoption of CIoT prompted these countries to do more than depend on existing laws by introducing new regulations.

5.3.2 Security concerns

The researcher's view after each interview was that each of the participants had concerns regarding the issues that come from CIoT. The security concerns of CIoT assemblages came up from all participants. However, these security concerns were not enough to discourage consumers from adopting IoT technology. The participants acted differently on how they need to protect themselves and their CIoT assemblage from achieving the level of security satisfaction. The concerns for security was across all participants. It would be irresponsible for authorities in South Africa to leave the responsibility of data privacy, security and trust to the consumers. The consumers are powerless against big businesses. If big companies do not take the proper steps to secure IoT networks, then the consumers are at risk when using the CIoT assemblage.

The experts provided more details around the CIoT subject from both the technical and legal point of view. The researcher expected the experts to have such information because of the expertise and industry experience. Their profession is such that they deal with IoT in one way or another daily.

5.3.3 Concerns over privacy of personally identifiable information

The consumers' experiences affect future behavioural intentions. That means the way consumers view privacy concerns determines how they treat information privacy issues. Some of the consumers of IoT interviewed had no technical understating or concerns. The general consumer that does not have technical understanding need terms and conditions or policies that displayed clearly on the CIoT devices. The service providers need to make their information practices clear. The legal instrument needs to enforce this such that it becomes a common thing for all CIoT service providers. The information

should very clear and provide explicit warnings of the potential dangers to the consumers because of using the device or system. CIoT service providers should be transparent when it comes to the information they collect, process, store and use. Consumers need to be educated on the dangers of using IoT devices. The consumers need to understand that the risks of CIoT are the same, if not more, like any other online dangers when it comes to personal information.

Data privacy is about personal information. While businesses see consumers accepting their terms and conditions, laws such as the POPI Act seek to give back control of personal data to the consumer. Some experts had the view that as soon the consumer accepts the terms and conditions of the provider of CIoT, they have relinquished their rights to their personal information. This inconsistent with human rights in general. In South Africa, it is incompatible with both the POPI Act, the CPA, and the ECT Act.

The findings implied that the interactions with CIoT assemblages bring in positive experiences. These positive experiences promote adoption and usage. PII extend beyond the consumers' known data such as age, gender, race and other attributes. Smart things can continue the identity of consumers. Their ability to identify consumers is because smart things generate data related to the consumers' location, preferences, shopping habits, among other things. This integration of one's identity with things is possible through routine and frequent use. The consumers' experiences as per data collected emphasize that smart devices are part of consumers' lives.

The revelation by consumers that the terms and conditions or policies that come CIoT systems imply that they do not read those policies at all. Consumers need to take responsibility for their actions. If they do not read and understand the "small prints", then they should not be surprised to discover that third parties use their information for purposes unknown to them. The idea is that if you cannot read the terms and conditions before using a service, then you cannot blame anyone for the perceived misuse. The expert had a different opinion, as they believed that the responsibility of data privacy could not be at the hands of the consumers entirely. As far as the researcher is concerned, data

privacy is a collaborative effort amongst all stakeholders. None of the stakeholders should relinquish their responsivity to others. However, the legal instruments should be precise when it comes to the lines of responsibility to avoid ambiguity.

5.3.4 Trust issues

The level of trust is of utmost importance through the CIoT assemblage and between all stakeholders. For example, consumers interact with their smart things such as the smart home until they trust it to operate as it should. The constant interactions create a true dependency. Communications among all of the components matter in assemblage theory. The interactions among the components that do not involve the consumer also contribute to indispensability and other outcomes.

The relationships between consumers and smart devices are personal. The interactions with the machines are personal and diverse from one consumer to another. For example, the findings in the study show that the choice of system to use for either home security purposes or personal fitness purpose was different from one consumer to another. The consumer's original decision may be influenced by many factors such as devices sponsored by one's health insurance (as in the case with the participant that uses Discovery Medical Aid). However, the constant use of a specific system makes it personal and more comfortable for the consumer. The level of trust in the provider and the CIoT system they provide increases with the constant interactions.

The researcher's wishes are that insurance companies do not use personal information as a tool to decline claims in the future. In the case of car insurances, they may use driving behaviour to reject claims. While we agree that people should be responsible drivers, car insurance drivers should issues warnings to their clients about their driving habits. They further need to state the consequences of continued bad driving habits., and that such behaviour could result in cancelling the consumer's membership if need be. The problem

is when the insurance company continues taking the clients' premium while being aware of the risky behaviour by the consumer.

The consumers saw the benefits of automating some of the routine tasks using CIoT. The CIoT does everyday tasks as if the consumer has himself or herself is doing it. The assemblage theory makes us understand the importance of all the component interactions and stakeholders. The question arises as to whether automating mundane tasks will make South African society more productive in the long term or not.

5.3.5 Convenience and benefits trump over concerns

The data collected show that CIoT has many benefits for both consumers and businesses. The researcher agrees with the participants that CIoT has many advantages, including remote control, monitoring, fault diagnosis and the ability to collect data for analysis. The consumers pointed out that CIoT gives convenience and a whole lot of other benefits. The research data imply that consumers will continue using CIoT because of the convenience they provide. Most consumers see smart things as servants that respond to commands. These things simplify consumers' lives through direct interactions. However, the consumer does not have to interact with things all the time, but things can be autonomous. All participants acknowledged that they were aware that service providers collect their data. Still, some revealed that this was an acceptable practice as long as they received the benefits of using the system. This revelation implies that consumers slightly ignore some of the risks to gain the benefits of using CIoT.

The researcher identified convenience or perceived usefulness and need for sociality as motivators for the consumer to interact with things. For example, the connected car may have its air conditioning switched on before the driver arrives. Alternatively, the smart home may prepare a warmly lit environment for dinner. Smart things are extending their resources to the consumers, and thus the consumers may interpret a specific smart object as a partner rather than just a device that is trying to satisfy her needs. The results gave

insight into these driving factors of individuals' willingness to use IoT technology. The participant showed particularly strong support for the effects of the convenience of using the technology. Security, data privacy and trust issues do not deter the participants from adopting the technologies. That does not negate the worries raised, and those worries still warrant further research in both academia and industry. The concerns played an insignificant role in predicting the participants' future behavioural intentions. They all made it clear that they would like to see more and more use of CIoT to simplify people's lives. Evidence from the consumers of IoT suggests that consumers want their smart devices to learn what they are doing so they can benefit from it.

The researcher used Dewey's theory of experience in interpreting what consumers' experience meant. The experience theory coined by Dewey (1958) and expanded by Clandinin and Connelly (2000). Dewey (1958) combined two principles, stating that one's present experiences are a direct result of how their previous experiences interact with and influence their current situation. The revised experience theory by Clandinin and Connelly (2000) look at personal and social (interaction); past, present, and future (continuity); and place (situation). The consumers are the only ones who can relate their experiences as they interact with mobile apps and devices. Storytelling is part of our lives, and thus interpreting stories of consumers of IoT gave insight into their experiences as part of the research. The consumers narrated their past and present experiences, as well as how they intended to do things differently in the future. Finally, the consumers provided context or situations as to where they felt it is worth using IoT and mobile apps. The idea was to explore and analyse the experiences of IoT consumers as they use mobile apps to interact with things. For example, Participant A3 related some his experiences from the past, highlighted how they affect present decision, and how they finally influence the future.

Past Experience:

> *"We've had previous burglar break-ins in our house. This incident was a traumatic experience. It put my family at risk. Luckily, no one was hurt in the process. I had to beef up my security systems because of that incident". – Participant A3*

Present:

> *"Since I installed cameras and connected my alarm system to the security house, there have been no break-ins. I can use my phone to arm and disarm the alarm system, view what is happening through cameras and communicate with possible threats to security. The security system has helped in avoiding break-ins before they happen. I have a much better sense of security" - Participant A3*

Future:

> *"I am happy to invest more in newer technologies that will bring convenience and safety to my home. However, I am also careful as to which company I use so that I do not compromise my personal information. I believe the regulators need to regulate all stakeholders for those stakeholders to safeguard personal information in one way or the other. The only challenge is that most of these companies operate outside the jurisdiction of South Africa. In future, I am hoping to automate the mundane tasks in the house". - Participant A3*

Participant A3 alluded to a sense of security in his home due to the installed camera that he able to control via a mobile app. In this case, the experience that emerged from this is a sense of security. The consumer developed a capacity to feel more secure in his home. The data privacy, security and trust concerns in CIoT are lower when the consumer perceives the assemblage as useful, meaning that the adoption rate increases with the incremental value that consumers experience from the assemblage.

The theme on convenience and benefits of CIoT show that consumers will use the technology despite some of the challenges related to privacy, security and trust. However, the researcher's view is that these issues should not be left at the hands of the consumers. The regulators, manufacturers, cloud providers, mobile apps developers and other stakeholders are more informed than the consumers, and thus they are duty-bound to protect the consumers' information.

The technology needs to benefit both the businesses and the consumers. We do not expect firms to make a profit at the expense of consumers or in such a way that it is detrimental to the consumers. While we acknowledge that businesses have access to an enormous amount of consumers data, consumers need to use technology with care and have the ability to choose practices that will not compromise their privacy. In essence, CIoT needs to create actual value for both businesses and consumers.

The convenience of use is not enough if the incremental value provided by the CIoT assemblage does not benefit the consumers. It is ideal that such additional benefit both the consumers and the businesses too. The data from IoT devices can be used by enterprises to incentivize consumers. These incentives can be in the form of money, promotions, points, among other things. The idea is to promote consumers to interact more with smart objects and thus enhance innovation. Some of the participants mentioned that they see themselves as co-creators, and therefore it is essential that providers of CIoT recognize them as such. The businesses benefit from using consumers data. The consumers need rewards for their interactions in terms of time, loyalty, purchases, location, use of service, among other things. Consumers like rewards for their time purchases and other efforts — businesses like traffic, either online or physically.

Connected devices have the potential to play a more significant role in a person's life. For example, smart fridges can act as assistants for all aspects of food management, allowing the owners to remotely see what is inside their refrigerators, access recipes and other contextual information, and even to order food based on personal preferences. CIoT makes it possible to turn what was once just a product into a fully-fledged service. Businesses can forge a much more meaningful connection with consumers and reach them continuously.

Participant A1 mentioned, *"IoT is here to stay"*. This comment, in essence, implies that the identities of CIoT assemblages have the potential to emerge that are likely to outweigh privacy and security concerns. The evolution of CIoT will give insight into the preferences and features that consumers value enough to trade off some aspects of their privacy.

From the findings, we can predict that because of frequent repetition, service providers and all other stakeholders will come to know more about the consumers, surroundings and potential benefits. The benefits are likely to trump over privacy concerns. Pelaez, Chen and Chen (2019) state that the consumer's intention to transact represents a personal subjective construct. However, defining the construct is a bit simpler. The intention to create a construct represents a consumer's intent to have a relationship with the service provider. All participants were planning to continue buying IoT products and consuming IoT services in the future.

5.4 Summary

In this chapter, the researcher linked the themes to theory. Some of the theories he used were Dewey's experience Theory, Assemblage Theory, The South African POPI Act, and The South African Consumer Protection Act and the Electronic Communications Act. The next chapter summarizes the findings of the study and recommends the framework necessary to address the concerns of CIoT adequately.

CHAPTER SIX

6 SUMMARY, CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

The previous chapter interpreted and discussed the results of this study. In this final chapter, the researcher made recommendations for future research, whereby other researchers may collect and use additional data or use existing data. The field of CIoT and mobile apps developments attracted significant interest in the last twenty years since Kevin Ashton of Procter & Gamble coined the term “Internet of Things”. The challenges in as far as data privacy, security and stakeholder trust is concerned increased with the increased adoption of CIoT. The study developed a holistic framework to address the CIoT concerns.

6.2 Summary of findings

The researcher was able to generate themes from the collected data through thematic analysis. The interpretation of the collected data included the researcher’s experience and knowledge of the IoT field. These findings expanded on the conceptual framework and considered the legal, technical and social context in dealing with data privacy, security and trust.

From a legal point of view, the main concerns from the study were non-existence of legal instruments to deal directly with CIoT. In the literature review, the researcher first looked at international laws and discussed how they align with South African requirements to address CIoT challenges. The literature review revealed that the United States and the United Kingdom are working on regulations that seek to address the IoT space specifically. The South African government can adopt some of these legal instruments and customize them to deal with the South African conditions. It would not be the first time South Africa uses an international legal tool to address its challenges. The study showed that South Africa previously adopted the POPI Act from the European GDPR. In

the past, South Africa took the civil law systems of Europe, the common law of England and the Roman-Dutch law (Frolova, Belikova, Badaeva, Belozerova and Ulianischev, 2017). This mean South Africa is already used to taking some the international laws and customizing them for its benefit.

All the experts who participated in the research agreed that the South African POPI Act, the CPA and the ECT Act are the closest legal instruments that may be used to address the CIoT concerns from a legal point of view. However, the consensus was that these laws are not sufficient and are far from being able to address these challenges, as they are very generic to consumers and not specific to CIoT. The consumers of IoT worry when the laws, regulations and technological means to curb the challenges are lagging. Expert opinion about these laws revealed that they lack clarity when it comes to CIoT and their broadness in scope means that legal practitioners can interpret them in too many ways. Hence, the researcher recommends a need for a more direct legal instrument that deals with CIoT. The proposed holistic framework will incorporate such a legal tool, among others, when it becomes available.

The consumers of IoT mentioned that they are concerned with the possibility of companies and criminals using their data for evil purposes. However, the results further showed that consumers enjoy the convenience that IoT technology brings. The results also show that the perceived privacy risks and personal interest influences consumers' future behavioural intentions in as far as adoption of CIoT is concerned. The tracking of location-based information is evident to the consumer as she or he is aware of it and intentionally use it. For example, services may be running in the background, or the consumer may forget to logout from the smart device or system they are using. The challenges are especially true when CIoT service providers track personal information, and the consumer is not aware that the service provider is following them. Sometimes these location-based services may link to social media, and thus exposing the consumers' data to the rest of the world. When this happens, criminals may use such information to conduct their criminal activities. Crimes may include kidnapping, breaking into empty homes and stealing of cars, among other things.

When location-based information links to social media, criminals can use the information to commit crimes such as breaking into an empty home. In some cases, the intentional recording of personal data happens in the background. A good case in point is a health monitoring service that tracks consistently critical health parameters of an individual without notifying them about it all the time. It is thus crucial to understand usage patterns and perceptions from the consumer's point of view. This understanding will assist in the development of IoT services by keeping appropriate privacy and security standards in mind.

The research findings provided vital information that academia and industry may use, and they brought insight into the security and privacy concerns of CIoT. The findings provide a baseline for future research as well as for the industry to develop a more secure CIoT environment. The results will help CIoT services providers understand that their customers require more controls of their personal information when using the CIoT services. As CIoT develops, it will continue to create more powerful and more intimate ways to augment our control over the environments in which we live, work and play. The CIoT means that consumers are going to be interacting with machines that autonomously communicate with each other.

IoT content primarily involves the quantification of interactions involving physical events that can and do happen in the real world. While individually these events represent the minutia of everyday living that is trivial by itself, they together generate coherent emergent assemblages that have meaning and specific identity, with the potential to make significant impacts on people's lives. The participants were all hopeful that CIoT in the South African context could stimulate innovation, create new entrepreneurs, create jobs, fight crime and improve the health of citizens, among other benefits. The findings of the research are such that there should be a legal framework to drive the adoption of CIoT directed at providers of CIoT and the consumers of IoT. Consumers should take responsibility for their safety when consuming IoT. Still, the legal framework should help

in enforcing practices that may be dangerous to the consumers and those close to the consumers.

In CIoT assemblages, the interactions take place in complex nested, overlapping and constantly evolving networks that connect heterogeneous entities in the digital world with equally varied objects in the physical world. All stakeholders should keep in mind that the CIoT assemblage is by nature dynamic, nonlinear and often non-social experiences emerge from these interactions with devices that also interact with each other, all regularly. The research shows that as much as we can tell our stories about our experiences with smart things through IoT technologies, things can equally tell stories about us, our environment, other people and other things. Sundmaeker, Guillemin, Friess and Woelfflé (2010) state that users may benefit from IoT technologies used in smart fridges that autonomously monitor the consumption of food and beverages and re-order goods.

6.3 Conclusions

The CIoT is a thrilling phase in the Internet revolution because it brings the intelligence of the Internet to physical products with the potential for something new to emerge. CIoT is an assemblage of interconnected sensors and actuators, which enable decision-making and simplify the consumers' lives. At the heart of CIoT is information that feeds into a continuous cycle of sensing, decision-making, and actions. Consumers interact with things continuously, leading to new capacities and properties.

This study reviewed the background of IoT, analysed security characteristics and requirements from four layers, compared and contrasted CIoT and IIoT. It further highlighted the benefits and the challenges in the adaptation of this technology by consumers in South Africa and finally proposed the means of addressing these challenges. The researcher answered the questions about the challenges that consumers of IoT face in South Africa through a detailed review of literature, narrative interviewing the consumers of IoT and finally getting experts opinions through Delphi technique from

the industry expert. The study revealed that the development of the CIoT brings with it more strict security, data privacy and stakeholders' trust issues, which became the focus and the primary task of the research.

While the legislators may not react at first, there is a greater need for them to respond to protect the consumers. Technological advancement seems to evolve faster than lawmakers can regulate it. The POPI Act's place in the international privacy paradigm is promising. Its provisions match the EU DPD's standards of data protection with the effect that South African businesses could engage in transactions with European companies that are heavily reliant on data. A similar provision does not exist when dealing with other parts of the world, such as the Americas and Asian counterparts.

6.4 Recommendations

We need a framework to address all fundamental issues of consumer concerns at the international and national level. This study has proposed such a framework (See Figure 6.1). A globally focused regulator needs to adopt the framework and used it for every object on earth from when its creation to its destruction. Data protection and privacy need communication strategies establishing an effective platform for dialogue between state legislators, non-governmental organizations, public interest groups and the international private sector. Otherwise, the IoT becomes impractical, and it becomes hard to use it efficiently. All stakeholders of CIoT in South Africans need to embrace CIoT to stimulate economic growth. While the country adopts IoT, care needs to be taken to safeguard the consumers' privacy.

Both newly proposed American and British laws of these IoT security laws could become templates for other nations such as South Africa looking to improve the security of so-called "smart" devices hooked up to the Internet. Consumers and governments gave little or no thought to the cybersecurity protections built into Internet-connected devices, or to how simple security vulnerabilities of those devices could lead to real-world problems.

The South African government need to have new regulations, in additions to the POPI Act and the Consumer Protection Act. The aim of the new rules should aim at ensuring IoT devices are more secure both in the public and private sectors. The laws need to be more consumer-orientated and should let the consumers know how secure an IoT device is before they buy it, setting some baseline standards for the devices to ensure security. It should be mandatory that if companies want to sell their products, they should put a label on IoT devices indicating the degree to which they meet the security requirements. This requirement is just an effort to help inform consumers when purchasing. South African companies must come up with unique default passwords, state the length of time security updates will be made available, and offer contact at the vendor for disclosure of the product's cybersecurity vulnerabilities**.** Application developers need to present the consumers with a list of features that the application provides. Furthermore, the application developers need to deliver the authorization that the consumer needs to give to activate each of those features. The application developer must give control to the consumer to decide which features they want to activate.

The study recommends practical approaches to deal with data privacy, security and trust issues. Stakeholders of IoT need to use the holistic framework in Figure 6.1 to ascertain if a specific assemblage poses any threats to the consumers. Each stakeholder may develop a list of questionnaires using the proposed framework to ensure that they have covered all aspects of the CIoT concerns.

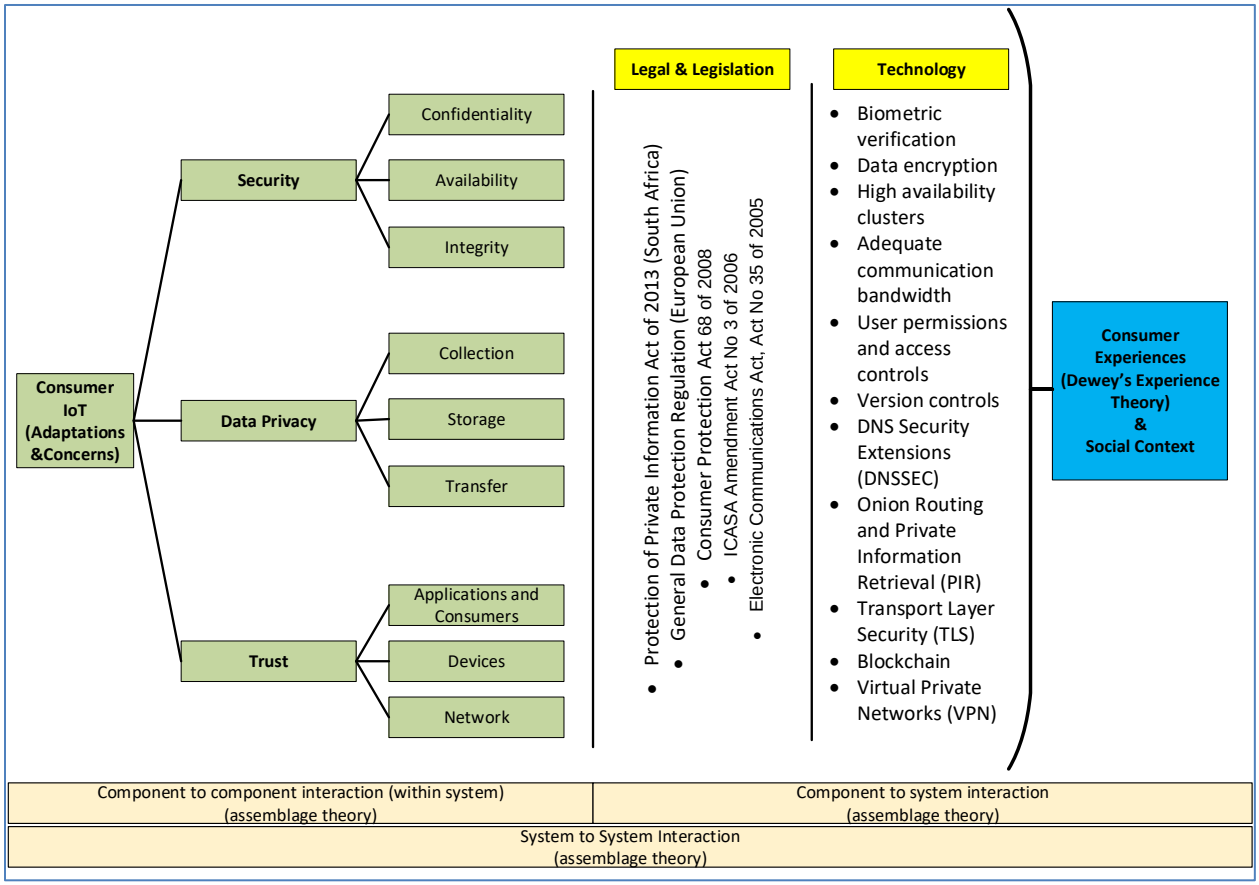


Figure 6.1: A framework for security, privacy and trust in CIoT (Researcher)

6.4.1 Security

The literature review discussed the CIA Triad as a framework that all stakeholders need to take into consideration when dealing with CIoT. The three services in the CIA Triad (confidentiality, integrity, and authentication) counter common security vulnerabilities available in IoT devices. The literature review revealed the importance of security for the efficient functioning of CIoT. The researcher recommends that the CIA Triad form part of the guiding principle in the implementation of CIoT. In addition to the implementers of CIoT, country-level lawmakers, company level policymakers should all consider the CIA triad.

However, the CIA Triad is not enough to address the security issues in CIoT and thus serve as one of the pillars. The study noted in the literature review that the CIA Triad has a limited view of the security and ignores other important factors that include the respect for one's privacy and the trust level that need to exist among all stakeholders. The consumers of IoT agreed in general that they have to be responsible for their safety. Some were more careful in how they manage the passwords of their IoT devices, while others did not take it that seriously before the interview.

The experts suggested different technical approaches to use in dealing with the security of CIoT. The service providers need to ensure that they transfer personal information from devices to storage areas is via secure channels. The experts suggested the use of robust passwords as well as security exchange protocols. When consumers and smart things interact or when smart things interact with each other, the communication protocol between the device and any other communication partners needs integrity and confidentiality protection, or else criminals can modify messages in transit or eavesdrop. CIoT service providers should provide authentication between the communication endpoints to prevent man-in-the-middle from interfering with the CIoT assemblages

When the participants raised their strategies in password management, they, in essence, talk about credentials management. Pure data transport (without security) is frequently the goal of hackathons and other hands-on IoT workshops. The literature review discussed Biswas and Muthukkumarasamy (2016)'s study on the blockchain technology and how designers of CIoT can use it to curb security-related issues. The research agrees with these researchers that the resilience of the blockchain technology calls for providers of CIoT services to use it to enhance security. This technology is a decentralized and distributed digital ledger technology that records transactions across many computers so that hackers cannot alter retroactively any record, without the alteration of all subsequent blocks. The main problem with a centralized database is that it presents a single point of failure to the whole assemblage. When hackers gain access to the centralized database and analytical systems, then they can take control and infect the assemblage with malware.

6.4.2 Data privacy

The study looked at data privacy from various angles. A CIoT assemblage can compromise data from the collection, storage and transfer points. The researcher recommends that consumers use trusted devices that ICASA (the Authority) and SABS have given the green light in South Africa. If the Authority has not tested the sensors or devices that collect consumer information, those devices may infect other devices and systems that connect to the internet. In addition, this will be a violation of statutory bodies and legal instruments.

As much consumers need to take responsibility for their conduct when dealing with CIoT personal data, all other stakeholders should be responsible when dealing with consumer data. The researcher recommends legal instruments that are specific and provide clear boundaries on the responsible parties when it comes to data privacy. No privacy policies should contradict the national laws, and the national laws should not contradict the international regulator. In South Africa, the constitution is the guiding law. That means the underlying legal instruments in South Africa should not in any way contradict the constitution and should find a balance to be in line with the international regulator. The right to privacy is enshrined in the constitution of South Africa Company policies should not infringe on fundamental human rights such as the right to privacy, right to safety, freedom to choose, among other rights.

Once the devices have collected the information, that information is usually stored in a centralized location. As discussed under security, the researcher recommends against the use of a centralized system but supports a distributed ledger technology such as blockchain technology. Stealing personal data and hence identity theft, among other risks, is more challenging in distributed systems.

The Authority needs to work on a legal instrument that addresses IoT explicitly in South Africa. The researcher recommends that the Authority sought a blueprint from the

European Union, United Kingdom and the United States. The literature review discussed the advancement of legal instruments that deal with IoT in these jurisdictions. The legal tools should cover how we need to treat data privacy from data collection to data transfer and finally to data storage.

The risks of hackers stealing personal information from storage are high, and the problem stamen highlighted these risks. The legal instrument needs to be clear as to where CIoT service providers can store the data. For example, if the service rendered is in South Africa, but the information is stored in the United States, how can consumers or any stakeholder institute legal claims? Some countries do not even have laws to protect consumers, and thus South Africans using some of these overseas storage services may be at risk with no legal protection on their side. Therefore, the researcher recommends that the Authority demands that service providers store consumers' information in South Africa.

In many cases, service providers may use personal information without the consent of consumers. The legal instrument needs to be strict on how service providers may use personal information and show respect to the consumers' data. The statutory instrument should forbid marketers from doing what they want to do with consumers' data.

6.4.3 Trust

For consumers to adopt CIoT faster in South African, the level of trust between all stakeholders needs to be high. The trust needs to exist between all the providers of CIoT, regulators and consumers. In addition, the heterogeneous devices that form part of the CIoT assembly should trust each other using standardized protocols.

The Authority such as ICASA and SABS should make sure that IoT devices in the South African market are trustworthy. The providers of CIoT should also be companies registered in South African so that the authorities can hold them accountable if they violate

the laws in one way of the other. The police should further prosecute consumers and service providers who use personal information for nefarious means. The idea is to discourage bad behaviour, build trust amongst all stakeholders and stimulate innovation and economic development in the country. The Authority needs to be clear on the responsibility of the service provider to avoid hackers from stealing personal information.

6.4.4 Consumers

The researcher recommends that consumers should take some level of responsibility for their safety and privacy. He suggests that consumers should act responsibly to help fulfil their rights to protection. A responsible consumer may need to consider the following actions:

- Read consumer reviews before buying smart devices or IoT services
- Review and change the privacy and security settings on the devices and their applications before using them for the first time. Would a specific device be able to spy on the consumer somehow? Does the device require personal details?
- If the consumer is not using the devices, he or she should switch off the devices.
- If the consumer does not require the services at all, he or she needs to disconnect them from the internet.
- The consumer needs to check if there is a requirement for firmware updates, patches and revisions. If need be, he or she needs to update all devices and with the current software.
- The consumer needs to make use of multi-factor authentication.
- The consumer needs to use complex passwords, reset them frequently, change from default passwords and easily reset passwords if need be.
- The consumer needs to read the user agreement thoroughly, especially concerning privacy and data sharing.
- The consumer needs to keep himself or herself updated by subscribing to newsletters from service providers whereby the service provider informs consumers of possible data breaches.

6.5 Final Conclusion

The Internet of Things is here to stay, and so is its application by consumers. The advances in IoT technology has an increasing impact on our daily lives. The research aimed at exploring data privacy, security and stakeholder trust issues in CIoT assemblages. The exploration resulted in the development of an integrated framework that will assist all stakeholders in understating and dealing with CIoT issues.

The study helped us to understand consumers' reactions to CIoT assemblages. It further brought awareness to the threats of CIoT and highlighted how various stakeholders could assess and manage these threats. The research also determined the factors that influence the acceptance of IoT technology by consumers. The researcher proposed a framework that considers legal approaches and technological approaches in addressing concerns of data privacy, security and stakeholder trust issues. The framework further looked at the social context or social influence. CIoT assemblage as a complex system, where having smart things is an emergent property of many interacting components, and we understand it only by analysing the parts in isolation. The consumer experience is of vital importance in CIoT. Devices that were dump in the past are now smart computing devices. The researcher recommends further study that will cover the regulators such as ICASA in detail and the enforcement of the POPI Act as it comes into effect in 2020. Such a study can look at the policy and legislative framework.

REFERENCES

ABBASI, A., MEMON, Z. A., MEMON, J., SYED, T. Q. & ALSHBOUL, R. 2017. Addressing the Future Data Management Challenges in IoT: A Proposed Framework. *International Journal of Advanced Computer Science and Applications,* 8**,** 197-207.

ADLER, M. & ZIGLIO, E. 1996. *Gazing into the oracle: The Delphi method and its application to social policy and public health,* London, Jessica Kingsley Publishers.

AKTURAN, U. & TEZCAN, N. 2012. Mobile banking adoption of the youth market: Perceptions and intentions. *Marketing Intelligence & Planning,* 30**,** 444-459.

AL-FUQAHA, A., GUIZANI, M., MOHAMMADI, M., ALEDHARI, M. & AYYASH, M. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials,* 17**,** 2347-2376.

AL-MOMANI, A. M., MAHMOUD, M. A. & SHARIFUDDIN, M. 2016. Modeling the adoption of internet of things services: A conceptual framework. *International Journal of Applied Research,* 2**,** 361-367.

ALDOSSARY, S. & ALLEN, W. 2016. Data security, privacy, availability and integrity in cloud computing: issues and current solutions. *International Journal of Advanced Computer Science and Applications,* 7**,** 485-498.

ALGHAMDI, S. & BELOFF, N. Towards a comprehensive model for e-Government adoption and utilisation analysis: The case of Saudi Arabia. 2014 Federated Conference on Computer Science and Information Systems, 7-10 September 2014 Warsaw, Poland. IEEE, 1217-1225.

ALHOJAILAN, M. I. 2012. Thematic analysis: A critical review of its process and evaluation. *West East Journal of Social Sciences,* 1**,** 39-47.

ALI, M. S., VECCHIO, M., PINCHEIRA, M., DOLUI, K., ANTONELLI, F. & REHMANI, M. H. 2018. Applications of Blockchains in the Internet of Things: A Comprehensive Survey & Tutorials. *IEEE Communications Surveys***,** 1676-17117.

ALVESSON, M. & SKÖLDBERG, K. 2017. *Reflexive methodology: New vistas for qualitative research*, Sage.

ATZORI, L., IERA, A. & MORABITO, G. 2010. The internet of things: A survey. *Computer networks,* 54**,** 2787-2805.

AVELLA, J. R. 2016. Delphi panels: Research design, procedures, advantages, and challenges. *International Journal of Doctoral Studies,* 11**,** 305-321.

BABAR, S., MAHALLE, P., STANGO, A., PRASAD, N. & PRASAD, R. Proposed security model and threat taxonomy for the Internet of Things (IoT). International Conference on Network Security and Applications, 23-25 July 2010 Chennai, India. Springer, 420-429.

BABAR, S., STANGO, A., PRASAD, N., SEN, J. & PRASAD, R. Proposed embedded security framework for internet of things (IoT). 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 28 February - 3 March 2011 Chennai, India. IEEE, 1-5.

BARNETT, J. E., WISE, E. H., JOHNSON-GREENE, D. & BUCKY, S. F. 2007. Informed consent: Too much of a good thing or not enough? *Professional Psychology: Research and Practice,* 38**,** 179a.

BASSI, A., BAUER, M., FIEDLER, M., KRAMP, T., VAN KRANENBURG, R., LANGE, S. & MEISSNER, S. 2016. *Enabling things to talk*, Springer.
BAXTER, J. & EYLES, J. 1997. Evaluating qualitative research in social geography: establishing 'rigour'in interview analysis. *Transactions of the Institute of British geographers,* 22**,** 505-525.
BELK, R. W. 1988. Possessions and the extended self. *Journal of consumer research,* 15**,** 139-168.
BELL, E. & BRYMAN, A. 2007. The ethics of management research: an exploratory content analysis. *British Journal of Management,* 18**,** 63-77.
BERDYKHANOVA, D., DEHGHANTANHA, A. & HARIRAJ, K. Trust challenges and issues of e-government: E-tax prospective. 2010 International Symposium on Information Technology, 5-17 June 2010 2010 Kuala Lumpur, Malaysia. IEEE, 1015-1019.
BIRNHACK, M. 2008. The EU Data Protection Directive: An engine of a global regime. *Computer Law and Security Review,* 24**,** 508-520.
BISWAS, K. & MUTHUKKUMARASAMY, V. Securing smart cities using blockchain technology. 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 12-14 December 2016 Sydney, NSW, Australia. IEEE, 1392-1393.
BLOWERS, M., IRIBARNE, J., COLBERT, E. & KOTT, A. 2016. *The Future Internet of Things and Security of its Control Systems* [Online]. Cornell University Library: ArXiV. Available: https://arxiv.org/ftp/arxiv/papers/1610/1610.01953.pdf [Accessed 30 August 2018].
BOJANOVA, I. & VOAS, J. 2017. Trusting the internet of things. *IT Professional,* 19**,** 16-19.
BOTHA, J., ELOFF, M. M. & SWART, I. The effects of the POPI Act on small and medium enterprises in South Africa. 2015 Information Security for South Africa (ISSA), 2015. IEEE, 1-8.
BOTHA, J., GROBLER, M., HAHN, J. & ELOFF, M. A High-Level Comparison Between the South African Protection of Personal Information Act and International Data Protection Laws. International Conference on Cyber Warfare and Security Conference Proceedings, 2-3 March 2017 Dayton, Ohio, USA. Academic Conferences and Publishing International Ltd, 57.
BOTHA, J., GROBLER, M., HAHN, J. & ELOFF, M. A high-level comparison between the South African protection of personal information act and international data protection laws. International Conference on Cyber Warfare and Security Conference Proceedings, 2017. 57.
BRADLEY, E. H., CURRY, L. A. & DEVERS, K. J. 2007. Qualitative data analysis for health services research: developing taxonomy, themes, and theory. *Health services research,* 42**,** 1758-1772.
BRAUN, V. & CLARKE, V. 2006. Using thematic analysis in psychology. *Qualitative research in psychology,* 3**,** 77-101.
BROWN, D. R., DAWSON, T. M. & SEESSEL, B. V. 2019. The Internet of Things: Proposed Federal Legislation and Potential Federal vs. State Conflict? *The*

National Law Review [Online]. Available: https://www.natlawreview.com/article/internet-things-proposed-federal-legislation-and-potential-federal-vs-state-conflict [Accessed 20 December 2019].
BRYMAN, A. 2008. *Why do researchers integrate/combine/mesh/blend/mix/merge/fuse quantitative and qualitative research*, Sage.
BRYMAN, A. 2016. *Social research methods*, Oxford university press.
BRYMAN, A., BECKER, S. & SEMPIK, J. 2008. Quality criteria for quantitative, qualitative and mixed methods research: A view from social policy. *International Journal of Social Research Methodology,* 11**,** 261-276.
BRYMAN, A., BELL, E., MILLS, A. J. & YUE, A. R. 2011. Business Research Methods. First Canadian Edition.
BUCHANAN, I. 2015. Assemblage theory and its discontents. *Deleuze and Guattari Studies,* 9**,** 382-392.
CARLIN, B. I., GERVAIS, S. & MANSO, G. 2010. Libertarian paternalism, information sharing, and financial decision-making. *Information Sharing, and Financial Decision-Making (March 7, 2010)*.
CARROLL, L. J. & ROTHE, J. P. 2010. Levels of reconstruction as complementarity in mixed methods research: A social theory-based conceptual framework for integrating qualitative and quantitative research. *International journal of environmental research and public health,* 7**,** 3478-3488.
CASE, D. O. & GIVEN, L. M. 2016. *Looking for information: A survey of research on information seeking, needs, and behavior,* London, Emerald Group Publishing.
CHEN, D., CHANG, G., JIN, L., REN, X., LI, J. & LI, F. A novel secure architecture for the Internet of Things. 2011 Fifth International Conference on Genetic and Evolutionary Computing, 29 August - 1 September 2011 Xiamen, China. IEEE, 311-314.
CHEN, R., BAO, F. & GUO, J. 2015. Trust-based service management for social internet of things systems. *IEEE transactions on dependable and secure computing,* 13**,** 684-696.
CHENAIL, R. J. 2012. Conducting Qualitative Data Analysis: Reading Line-by-Line, but Analyzing by Meaningful Qualitative Units. *The Qualitative Report,* 17**,** 266-269.
CHENG, J. W. & MITOMO, H. 2017. The underlying factors of the perceived usefulness of using smart wearable devices for disaster applications. *Telematics and Informatics,* 34**,** 528-539.
CHILISA, B. & KAWULICH, B. 2012. Selecting a research approach: paradigm, methodology and methods. *Doing Social Research, A Global Context. London: McGraw Hill*.
CHOU, M.-J., TU, Y.-C. & HUANG, K.-P. 2013. Confucianism and character education: a Chinese view. *Journal of Social Sciences,* 9**,** 59.
CLANDININ, D. J. 2006. Narrative inquiry: A methodology for studying lived experience. *Research studies in music education,* 27**,** 44-54.
CLANDININ, D. J. & CONNELLY, F. M. 2000. Narrative inquiry: Experience and story in qualitative research.
CLANDININ, D. J. & HUBER, J. 2002. Narrative inquiry: Toward understanding life's artistry. *Curriculum Inquiry,* 32**,** 161-169.

CLAYTON, E. W., EVANS, B. J., HAZEL, J. W. & ROTHSTEIN, M. A. 2019. The law of genetic privacy: applications, implications, and limitations. *Journal of Law and the Biosciences,* 6**,** 1-36.

COETZEE, L. & EKSTEEN, J. The Internet of Things-promise for the future? An introduction. IST-Africa Conference Proceedings, 11-13 May 2011 Gaborone, Botswana. IEEE, 1-9.

CORTI, L., DAY, A. & BACKHOUSE, G. Confidentiality and informed consent: Issues for consideration in the preservation of and provision of access to qualitative data archives. Forum Qualitative Sozialforschung/Forum: Qualitative Social Research, 2000.

COUGHLAN, T., BROWN, M., MORTIER, R., HOUGHTON, R. J., GOULDEN, M. & LAWSON, G. Exploring Acceptance and Consequences of the Internet of Things in the Home. 2012 IEEE International Conference on Green Computing and Communications, 20-23 November 2012 Besancon, France. IEEE, 148-155.

COWLING, M. A. 2016. Navigating the path between positivism and interpretivism for the technology academic completing education research. *In:* HARREVELD, B., DANAHER, M., LAWSON, C., KNIGHT, B. & G., B. (eds.) *Constructing Methodology for Qualitative Research.* London: Palgrave Macmillan.

CRESWELL, J. W. 2009. Mapping the field of mixed methods research. SAGE Publications Sage CA: Los Angeles, CA.

CRESWELL, J. W. & CRESWELL, J. D. 2017. *Research design: Qualitative, quantitative, and mixed methods approaches*, Sage publications.

CRESWELL, J. W. & POTH, C. N. 2017. *Qualitative inquiry and research design: Choosing among five approaches*, Sage publications.

CROSBY, M., PATTANAYAK, P., VERMA, S. & KALYANARAMAN, V. 2016. Blockchain technology: Beyond bitcoin. *Applied Innovation,* 2**,** 6-10.

DA XU, L., HE, W. & LI, S. 2014. Internet of things in industries: A survey. *IEEE Transactions on industrial informatics,* 10**,** 2233-2243.

DARDICK, G. S. Cyber Forensics Assurance. 8th Australian Digital Forensics Conference, 2010. Citeseer, 57.

DARZENTAS, D., HAZZARD, A., BROWN, M., FLINTHAM, M. & BENFORD, S. 2016. Harnessing the digital records of everyday things.

DAVIDSON, P. L. 2013. The Delphi technique in doctoral research: Considerations and rationale. *Review of Higher Education and Self-Learning,* 6**,** 53-65.

DE BRUYN, M. 2014. The protection of personal information (POPI) act: impact on South Africa.

DE KEYSER, A., SCHEPERS, J. & KONUŞ, U. 2015. Multichannel customer segmentation: Does the after-sales channel matter? A replication and extension. *International Journal of Research in Marketing,* 32**,** 453-456.

DELANDA, M. 2006. *A new philosophy of society: Assemblage theory and social complexity*, A&C Black.

DELANDA, M. 2016. *Assemblage theory*, Edinburgh University Press.

DENZIN, N. K. & LINCOLN, Y. S. 2011. *The Sage handbook of qualitative research*, Sage.

DEWEY, J. 1958. *Experience and Nature*, Dover Publications.

DEWEY, J. 1984. *The Later Works of John Dewey 1929: The Quest for Certainty*, SIU Press.
DIAMANTOPOULOU, V., ANDROUTSOPOULOU, A., GRITZALIS, S. & CHARALABIDIS, Y. 2020. Preserving Digital Privacy in e-Participation Environments: Towards GDPR Compliance. *Information,* 11**,** 117.
DINEV, T. & HART, P. 2006. An extended privacy calculus model for e-commerce transactions. *Information systems research,* 17**,** 61-80.
DLODLO, N., MBECKE, P., MOFOLO, M. & MHLANGA, M. 2015. The internet of things in community safety and crime prevention for South Africa. *Innovations and Advances in Computing, Informatics, Systems Sciences, Networking and Engineering.* Springer.
DOUGLAS, J. D. 1985. *Creative interviewing*, Sage Publications, Inc.
EBI, C. 2016. *Improving wastewater disposal with the help of the "Internet of Things"* [Online]. Online: Eawag: Swiss Federal Institute of Aquatic Science and Technology. Available: https://www.eawag.ch/fileadmin/Domain1/News/2016/1116/lorawan-schema_e.jpg [Accessed 16 October 2019].
EDELMAN, D. 2016. Edelman trust barometer 2016: Annual global study.
ELITE. 2019. *Target population differs from an accessible population* [Online]. Online: Elite Institute. Available: http://www.elitemv.com/2019/09/target-population-differs-from.html [Accessed 1 November 2019].
ENISA. 2017. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. Available: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot [Accessed 30 September 2019].
ETSI. 2019. Cyber Security for Consumer Internet of Things *Technical Specification* [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf [Accessed 31 October 2019].
FANTANA, N. L., RIEDEL, T., SCHLICK, J., FERBER, S., HUPP, J., MILES, S., MICHAHELLES, F. & SVENSSON, S. 2013. IoT applications—value creation for industry. *Internet of things: Converging technologies for smart environments and integrated ecosystems***,** 153.
FAROOQ, M. U., WASEEM, M., KHAIRI, A. & MAZHAR, S. 2015. A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications,* 111.
FEHÉR, B. 2011. Understanding the homeless experience in Hungary through a narrative approach. *European Journal of Homelessness _ Volume,* 5.
FERRAG, M. A., DERDOUR, M., MUKHERJEE, M., DERHAB, A., MAGLARAS, L. & JANICKE, H. 2018. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal*.
FLICK, U. 2002. Qualitative Research - State of the Art. *Social Science Information,* 41**,** 5-24.
FONG, L. H. N., LAM, L. W. & LAW, R. 2017. How locus of control shapes intention to reuse mobile apps for making hotel reservations: Evidence from chinese consumers. *Tourism Management,* 61**,** 331-342.

FOWLER, A., GOEL, S., HODGES, J. & MILLER, M. 2019. *Compliance Planning for California IoT Security Requirements* [Online]. Washington: Harris, Wiltshire & Grannis LLP. Available: https://www.hwglaw.com/compliance-planning-for-california-iot-security-requirements/ [Accessed 15 December 2019].

FROLOVA, E., BELIKOVA, K., BADAEVA, N., BELOZEROVA, I. & ULIANISCHEV, V. 2017. The concept of real right in India and South Africa: specifics of national regulation and trends of harmonization of law. *Journal of advanced research in law and economics,* 8**,** 799-812.

GAO, L. & BAI, X. 2014. A unified perspective on the factors influencing consumer acceptance of internet of things technology. *Asia Pacific Journal of Marketing and Logistics,* 26**,** 211-231.

GIBBS, G. R. 2007. Analyzing Qualitative Data. London, England: SAGE Publications, Ltd.

GOTTSCHALL, J. 2012. The storytelling animal: How stories make us human. *Scientific Study of Literature,* 2**,** 317-321.

GOV.ZA 2002. Electronic Communications and Transactions Act No 25 of 2002. *In:* PRESIDENCY, T. (ed.). Cape Town.

GOV.ZA 2005. Electronic Communications Act No 36 of 2005. *In:* PRESIDENCY, T. (ed.). Cape Town: GCIS.

GOV.ZA 2006. ICASA Amendment Act No 3 of 2006. *In:* PRESIDENCY, T. (ed.). Cape Town.

GOV.ZA 2009. Consumer Protection Act 68 of 2008. *In:* PRESIDENCY, T. (ed.) *526.* Cape Town: Republic of South Africa.

GREEN, J., WILLIS, K., HUGHES, E., SMALL, R., WELCH, N., GIBBS, L. & DALY, J. 2007. Generating best evidence from qualitative research: the role of data analysis. *Australian and New Zealand Journal of Public Health,* 31**,** 545-550.

HANCKE, G., MARKANTONAKIS, K. & MAYES, K. 2010. Security Challenges for User-Oriented RFID Applications within the" Internet of Things". *Journal of Internet Technology,* 11**,** 307-313.

HARMAN, G. 2008. DeLanda's ontology: assemblage and realism. *Continental Philosophy Review,* 41**,** 367-383.

HARWOOD, J., DOOLEY, J. J., SCOTT, A. J. & JOINER, R. 2014. Constantly connected–The effects of smart-devices on mental health. *Computers in Human Behavior,* 34**,** 267-272.

HASHEMI, S. H., FAGHRI, F., RAUSCH, P. & CAMPBELL, R. H. World of empowered IoT users. 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), 4-8 April 2016 2016 Berlin, Germany. IEEE, 13-24.

HELBERGER, N. 2016. Profiling and targeting consumers in the Internet of Things–A new challenge for consumer law. *Available at SSRN 2728717*.

HOFFMAN, D. L. & NOVAK, T. 2015. Emergent experience and the connected consumer in the smart home assemblage and the internet of things.

HOFFMAN, D. L. & NOVAK, T. P. 2017. Consumer and object experience in the internet of things: An assemblage theory approach. *Journal of Consumer Research,* 44**,** 1178-1204.

HOLLWAY, W. 2008. The importance of relational thinking in the practice of psycho-social research: Ontology, epistemology, methodology, and ethics. *In:* CLARK, S. (ed.) *Object relations and social relations.* London: Routledge.

HSU, C.-C. & SANDFORD, B. A. 2007. The Delphi technique: making sense of consensus. *Practical assessment, research & evaluation,* 12**,** 1-8.

HUSNJAK, S., PERAKOVIC, D. & JOVOVIC, I. 2014. Possibilities of using speech recognition systems of smart terminal devices in traffic environment. *Procedia Engineering,* 69**,** 778-787.

HUSSEIN, A. 2009. The use of triangulation in social sciences research: Can qualitative and quantitative methods be combined? *Journal of comparative social work,* 4**,** 1-12.

IRMAK, E. & BOZDAL, M. 2017. Internet of Things (IoT): The Most Up-To-Date Challenges, Architectures, Emerging Trends and Potential Opportunities. *International Journal of Computer Applications,* 975**,** 8887.

JACK, E. P. & RATURI, A. S. 2006. Lessons learned from methodological triangulation in management research. *Management Research News,* 29**,** 345-357.

JACOBS, W., STOOP, P. N. & VAN NIEKERK, R. 2010. Fundamental consumer rights under the Consumer Protection Act 68 of 2008: A critical overview and analysis. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad,* 13.

JAIRATH, N. & WEINSTEIN, J. 1994. The Delphi methodology (Part one): A useful administrative approach. *Canadian journal of nursing administration,* 7**,** 29-42.

JENNIFER, M. 2002. Qualitative researching. *University of Manchester, UK: Sage Publishings*.

JOVCHELOVITCH, S. & BAUER, M. W. 2000. Narrative interviewing. *Qualitative researching with text, image and sound***,** 57-74.

KANG, K., PANG, Z., DA XU, L., MA, L. & WANG, C. 2014. An interactive trust model for application market of the internet of things. *IEEE Transactions on Industrial Informatics,* 10**,** 1516-1526.

KATUU, S. & NGOEPE, M. 2015. Managing digital records within South Africa's legislative and regulatory framework. *In:* POPOVSKY, B. E., ed. 3rd International Conference on Cloud Security and Management ICCSM-2015, 23-25 October 2015 University of Washington-Tacoma. Academic Conferences and publishing limited, 59-70.

KHAN, R., KHAN, S. U., ZAHEER, R. & KHAN, S. Future internet: the internet of things architecture, possible applications and key challenges. 2012 10th International Conference on Frontiers of Information Technology, 17-19 December 2012 Islamabad, India. IEEE, 257-260.

KIVUNJA, C. & KUYINI, A. B. 2017. Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of Higher Education,* 6**,** 26-41.

KOTHARI, C. R. 2004. *Research methodology: Methods and techniques*, New Age International.

KOWATSCH, T. & MAASS, W. Critical privacy factors of internet of things services: An empirical investigation with domain experts. 7th Mediterranean Conference on Information Systems (MCIS 2012), 10 September 2012 Guimarães, Portugal. Heidelberg, Germany: Springer, 200-211.

LASTOVETSKA, A. 2019. *Blockchain Architecture Basics: Components, Structure, Benefits & Creation* [Online]. Online: MLSDev. Available: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture [Accessed 1 July 2019].
LEA, P. 2018. *Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security*, Packt Publishing Ltd.
LEE, I. & LEE, K. 2015. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons,* 58**,** 431-440.
LI, X., HESS, T. J. & VALACICH, J. S. 2008. Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems,* 17**,** 39-71.
LI, X. J. & WANG, D. Architecture and existing applications for internet of things. Applied Mechanics and Materials, 2013. Trans Tech Publ, 3317-3321.
LIANG, T.-P., LI, X., YANG, C.-T. & WANG, M. 2015. What in consumer reviews affects the sales of mobile apps: A multifacet sentiment analysis approach. *International Journal of Electronic Commerce,* 20**,** 236-260.
LUBORSKY, M. R. & RUBINSTEIN, R. L. 1995. Sampling in qualitative research: Rationale, issues, and methods. *Research on aging,* 17**,** 89-113.
MA, J., YANG, L. T., APDUHAN, B. O., HUANG, R., BAROLLI, L. & TAKIZAWA, M. 2005. Towards a smart world and ubiquitous intelligence: a walkthrough from smart things to smart hyperspaces and UbicKids. *International Journal of Pervasive Computing and Communications,* 1**,** 53-68.
MACINTOSH, R. 2009. Being clear about methodology, ontology and epistemology. *Being Clear About Methodology, Ontology and Epistemology*.
MADAKAM, S., LAKE, V., LAKE, V. & LAKE, V. 2015. Internet of Things (IoT): A literature review. *Journal of Computer and Communications,* 3**,** 164.
MAHESH, B., KUMAR, K. P., RAMASUBBAREDDY, S. & SWETHA, E. 2020. A Review on Data Deduplication Techniques in Cloud. *Embedded Systems and Artificial Intelligence.* Springer.
MANOGARAN, G., VARATHARAJAN, R., LOPEZ, D., KUMAR, P. M., SUNDARASEKAR, R. & THOTA, C. 2018. A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. *Future Generation Computer Systems,* 82**,** 375-387.
MANYIKA, J., CHUI, M., BISSON, P., WOETZEL, J., DOBBS, R., BUGHIN, J. & AHARON, D. 2015. *The Internet of Things: Mapping the value beyond the hype*, McKinsey Global Institute.
MARCIANO, R., LEMIEUX, V., HEDGES, M., ESTEVA, M., UNDERWOOD, W., KURTZ, M. & CONRAD, M. 2018. Archival records and training in the age of big data. *Re-envisioning the MLS: Perspectives on the Future of Library and Information Science Education.* Emerald Publishing Limited.
MARY, B. F. & AMALARETHINAM, D. G. Data Security Enhancement in Public Cloud Storage using Data Obfuscation and Steganography. 2017 World Congress on Computing and Communication Technologies (WCCCT), 2017. IEEE, 181-184.
MASSEY, A. K., EISENSTEIN, J., ANTÓN, A. I. & SWIRE, P. P. Automated text mining for requirements analysis of policy documents. 2013 21st IEEE International

Requirements Engineering Conference (RE), 15-19 July 2013 Rio de Janeiro, Brazil. IEEE, 4-13.
MATHABA, S., DLODLO, N., WILLIAMS, Q. & ADIGUN, M. 2011. The use of RFID and web 2.0 technologies to improve inventory management in South African enterprises. ICIME 2011-Proceedings of the 2nd International Conference on Information Management and Evaluation, 27-28 April 2011 2011 Ryerson University, Toronto, Canada. Online: Academic Conferences Limited, 300.
MCKNIGHT, D. H., CHOUDHURY, V. & KACMAR, C. 2002. Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research,* 13**,** 334-359.
MCQUEEN, M. 2002. *Language and power in nonprofit/for-profit relationships: a grounded theory of inter-sectoral collaboration.* Doctor of Philosophy, University of Technology, Sidney.
MEDAGLIA, C. M. & SERBANATI, A. 2010. An overview of privacy and security issues in the internet of things. *The internet of things.* Springer.
MEKKI, K., BAJIC, E., CHAXEL, F. & MEYER, F. 2019. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT express,* 5**,** 1-7.
MERETOJA, H. 2014. Narrative and human existence: Ontology, epistemology, and ethics. *New Literary History,* 45**,** 89-109.
MILLER, M. 2015. *The internet of things: How smart TVs, smart cars, smart homes, and smart cities are changing the world*, Pearson Education.
MILLER, T. & BELL, L. 2002. Consenting to what? Issues of access, gate-keeping and 'informed'consent. *Ethics in qualitative research***,** 53-69.
MOLLAH, M. B., AZAD, M. A. K. & VASILAKOS, A. 2017. Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications,* 84**,** 38-54.
MÜLLER, M. 2015. Assemblages and actor-networks: Rethinking socio-material power, politics and space. *Geography Compass,* 9**,** 27-41.
MUNOS, B., BAKER, P. C., BOT, B. M., CROUTHAMEL, M., VRIES, G., FERGUSON, I., HIXSON, J. D., MALEK, L. A., MASTROTOTARO, J. J. & MISRA, V. J. A. O. T. N. Y. A. O. S. 2016. Mobile health: the power of wearables, sensors, and apps to transform clinical trials. *Ann N Y Acad Sci,* 1375**,** 3-18.
MURPHY, M., BLACK, N., LAMPING, D., MCKEE, C., SANDERSON, C., ASKHAM, J. & MARTEAU, T. 1998. Consensus development methods, and their use in clinical guideline development. *Health technology assessment (Winchester, England),* 2**,** i-iv, 1-88.
MUYLAERT, C. J., SARUBBI JR, V., GALLO, P. R., NETO, M. L. R. & REIS, A. O. A. 2014. Narrative interviews: an important resource in qualitative research. *Revista da Escola de Enfermagem da USP,* 48**,** 184-189.
MVELASE, P., DLAMINI, Z., DLUDLA, A. & SITHOLE, H. Integration of smart wearable mobile devices and cloud computing in South African healthcare. eChallenges e-2015 Conference, 2015, 25-27 November 2015 Vilnius, Lithuania. IEEE, 1-10.
NAJJAR, Y. S. & AMER, M. M. B. 2016. Using a smart device and neuro-fuzzy control system as a sustainable initiative with green cars. *Journal of the Energy Institute,* 89**,** 256-263.

NCUBE, C. B. 2006. Watching the watcher: recent developments in privacy regulation and cyber-surveillance in South Africa. *SCRIPTed,* 3**,** 344.
NGULUBE, P. 2020. *Theory and theorizing in Information Science scholarship*, Hershey, IGI Global.
NORTHSTREAM. 2018. Connectivity technologies for IoT. Available: https://www.telenorconnexion.com/iot-insights/connectivity-technologies-for-iot/#gg-form [Accessed 01 May 2020].
NOVAK, T. P. & HOFFMAN, D. L. 2019. Relationship journeys in the internet of things: a new framework for understanding interactions between consumers and smart objects. *Journal of the Academy of Marketing Science,* 47**,** 216-237.
O'CONNOR, Y., ROWAN, W., LYNCH, L. & HEAVIN, C. 2017. Privacy by design: informed consent and internet of things for smart health. *Procedia computer science,* 113**,** 653-658.
ONWUEGBUZIE, A. J., FRELS, R. K. & HWANG, E. 2016. Mapping Saldana's Coding Methods onto the Literature Review Process. *Journal of Educational Issues,* 2**,** 130-150.
OUADDAH, A., ABOU ELKALAM, A. & AIT OUAHMAN, A. 2016. FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Security and Communication Networks,* 9**,** 5943-5964.
PALATTELLA, M. R., DOHLER, M., GRIECO, A., RIZZO, G., TORSNER, J., ENGEL, T. & LADID, L. 2016. Internet of things in the 5G era: Enablers, architecture, and business models. *IEEE Journal on Selected Areas in Communications,* 34**,** 510-527.
PALATTELLA, M. R., DOHLER, M., GRIECO, A., RIZZO, G., TORSNER, J., ENGEL, T. & LADID, L. J. I. J. O. S. A. I. C. 2016. Internet of things in the 5G era: Enablers, architecture, and business models. 34**,** 510-527.
PALMIERI III, N. F. 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**,** 37.
PAUL, P. K., KUMAR, K., CHATTERJEE, D., GHOSH, M., SHIVRAJ, K. & GANGULY, J. 2014. Information Science: The Multidisciplinary, Interdisciplinary field for Information cum Technological Solution for People and Wider Community. *International Journal of Information Science and Computing,* 1**,** 25-34.
PELAEZ, A., CHEN, C.-W. & CHEN, Y. X. 2019. Effects of perceived risk on intention to purchase: A meta-analysis. *Journal of Computer Information Systems,* 59**,** 73-84.
PEPPET, S. R. 2014. Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent. *Tex. L. Rev.,* 93**,** 85.
PERERA, C. 2017. *Sensing as a service for internet of things: A roadmap,* Lulu.com, Leanpub.
PERERA, C., RANJAN, R., WANG, L., KHAN, S. U. & ZOMAYA, A. Y. 2015. Big data privacy in the internet of things era. *IT Professional,* 17**,** 32-39.
PERERA, C., ZASLAVSKY, A., CHRISTEN, P. & GEORGAKOPOULOS, D. 2014. Sensing as a service model for smart cities supported by internet of things. *Transactions on Emerging Telecommunications Technologies,* 25**,** 81-93.
PIERRE, E. A. S. 2012. *Post qualitative research*, SAGE Publications.

PILKINGTON, M. 2016. Blockchain technology: principles and applications. *Research handbook on digital transformations*, 225.
PIWEK, L., ELLIS, D. A., ANDREWS, S. & JOINSON, A. 2016. The Rise of Consumer Health Wearables: Promises and Barriers. *PLOS Medicine,* 13**,** e1001953.
POMPONIU, V. 2012. Securing wireless ad hoc networks: State of the art and challenges. *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies.* IGI Global.
POWELL, C. 2003. The Delphi technique: myths and realities. *Journal of advanced nursing,* 41**,** 376-382.
PRIOR, B. 2019. *Vodacom launches new IoT gadgets for consumers* [Online]. Online: Mybroadband. Available: https://mybroadband.co.za/news/internet-of-things/312947-vodacom-launches-new-iot-gadgets-for-consumers.html [Accessed 19 October 2019].
PURCELL, A. 2018. *Three key ideas to help drive compliance in the cloud* [Online]. Online: IBM. Available: https://www.ibm.com/blogs/cloud-computing/2018/01/16/drive-compliance-cloud/ [Accessed 30 August 2019].
QU, C., TAO, M. & YUAN, R. 2018. A Hypergraph-Based Blockchain Model and Application in Internet of Things-Enabled Smart Homes. *Sensors,* 18**,** 2784.
RAO, B. T. & VURUKONDA, N. 2016. A Study on Data Storage Security Issues in Cloud Computing. *Procedia Computer Science,* 100**,** 128-135.
RAY, P. P. 2018. A survey on Internet of Things architectures. *Journal of King Saud University-Computer and Information Sciences,* 30**,** 291-319.
REWAGAD, P. & PAWAR, Y. Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing. 2013 International Conference on Communication Systems and Network Technologies, 2013. IEEE, 437-439.
RIGGINS, F. J. & WAMBA, S. F. Research directions on the adoption, usage, and impact of the internet of things through the use of big data analytics. 2015 48th Hawaii International Conference on System Sciences, 5-8 January 2015 Kauai, HI, USA. IEEE, 1531-1540.
ROOS, A. 2006. Core principles of data protection law. *Comparative and International Law Journal of Southern Africa,* 39**,** 103-130.
ROSE, K., ELDRIDGE, S. & CHAPIN, L. 2015. The internet of things: An overview. *The Internet Society***,** 1-50.
ROWE, G. & WRIGHT, G. 1999. The Delphi technique as a forecasting tool: issues and analysis. *International journal of forecasting,* 15**,** 353-375.
RSA 1996. Constitution of the Republic of South Africa (Act 108 of 1996). *Government Gazette No. 25799*.
SADEGHI, A.-R., WACHSMANN, C. & WAIDNER, M. Security and privacy challenges in industrial internet of things. Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE, 8-12 June 2015 San Francisco, CA, USA. IEEE, 1-6.
SALDAÑA, J. 2015. *The coding manual for qualitative researchers*, Sage.
SALGADO, J. & HERMANS, H. J. 2009. The return of subjectivity: From a multiplicity of selves to the dialogical self. *EJAP (test),* 1**,** pp. 3-13.
SAUER, G. 2017. A murder case tests alexa's devotion to your privacy. *Wired,* 28.

SCÂRNECI-DOMNIŞORU, F. 2013. Narrative technique of interviewing. *Bulletin of the Transilvania University of Braşov, Series VII: Social Sciences and Law***,** 21-28.
SCHLEICH, J., FAURE, C. & KLOBASA, M. 2017. Persistence of the effects of providing feedback alongside smart metering devices on household electricity demand. *Energy Policy,* 107**,** 225-233.
SCHMITT, C., MEIER, J., DIEZ, M. & STILLER, B. OTIoT—A browser-based object tracking solution for the Internet of Things. Internet of Things (WF-IoT), 2018 IEEE 4th World Forum on, 2018. IEEE, 445-451.
SCHNEIDER, M. & SOMERS, M. 2006. Organizations as complex adaptive systems: Implications of complexity theory for leadership research. *The Leadership Quarterly,* 17**,** 351-365.
SFAR, A. R., NATALIZIO, E., CHALLAL, Y. & CHTOUROU, Z. 2018. A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks,* 4**,** 118-137.
SHANG, X., ZHANG, R., ZHU, X. & ZHOU, Q. 2016. Design theory, modelling and the application for the Internet of Things service. *Enterprise Information Systems,* 10**,** 249-267.
SHANKAR, V., KLEIJNEN, M., RAMANATHAN, S., RIZLEY, R., HOLLAND, S. & MORRISSEY, S. 2016. Mobile shopper marketing: Key issues, current insights, and future research avenues. *Journal of Interactive Marketing,* 34**,** 37-48.
SILLARS, D. N. & HALLOWELL, M. R. 2009. Opinion-based research: Lessons learned from four approaches. Construction Research Congress 2009: Building a Sustainable Future, April 5-7, 2009 2009 Seattle, Washington, United States. Seattle, Washington, United States: American Society of Civil Engineers, 1499-1508.
SILVERIO-FERNÁNDEZ, M., RENUKAPPA, S. & SURESH, S. 2018. What is a smart device?-a conceptualisation within the paradigm of the internet of things. *Visualization in Engineering,* 6**,** 3.
SIVARAJAH, U., KAMAL, M. M., IRANI, Z. & WEERAKKODY, V. 2017. Critical analysis of Big Data challenges and analytical methods. *Journal of Business Research,* 70**,** 263-286.
SKULMOSKI, G. J., HARTMAN, F. T. & KRAHN, J. 2007. The Delphi method for graduate research. *Journal of Information Technology Education: Research,* 6**,** 1-21.
SMUTNÝ, P. Different perspectives on classification of the Internet of Things. 2016 17th International Carpathian Control Conference (ICCC), 29 May-1 June 2016 Tatranska Lomnica, Slovakia. IEEE, 692-696.
SOLUTIONS, E. R. 2012. Overview of Electronic Communications Regulation In South Africa. *South Africa. Available on URL: http://www. ellipsis. co. za/wpcontent/uploads/2012/03/Overview-of-Electronic-Communications-Regulation-in-South-Africa-2012. pdf*.
SOUTHAFRICA 2013. Protection of Personal Information Act. *In:* PRESIDENCY, T. (ed.). Cape Town: South Africa.
STANKOVIC, J. A. 2014. Research directions for the internet of things. *IEEE Internet of Things Journal,* 1**,** 3-9.

STAUNTON, C., ADAMS, R., ANDERSON, D., CROXTON, T., KAMUYA, D., MUNENE, M. & SWANEPOEL, C. 2020. Protection of Personal Information Act 2013 and data protection for health research in South Africa. *International Data Privacy Law*.

STOJANOVIC, V., FALCONER, R. E., ISAACS, J., BLACKWOOD, D., GILMOUR, D., KIEZEBRINK, D. & WILSON, J. 2017. Streaming and 3D mapping of AGRI-data on mobile devices. *Computers and Electronics in Agriculture,* 138**,** 188-199.

STOJKOSKA, B. L. R. & TRIVODALIEV, K. V. 2017. A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production,* 140**,** 1454-1464.

STOJMENOVIC, I. 2014. Machine-to-machine communications with in-network data aggregation, processing, and actuation for large-scale cyber-physical systems. *IEEE Internet of Things Journal,* 1**,** 122-128.

STOJMENOVIC, I. & WEN, S. The fog computing paradigm: Scenarios and security issues. 2014 Federated Conference on Computer Science and Information Systems, 7-10 September 2014 2014 Warsaw, Poland. IEEE, 1-8.

SUBASHINI, S. & KAVITHA, V. 2011. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications,* 34**,** 1-11.

SULTAN, N. H., VARADHARAJAN, V., ZHOU, L. & BARBHUIYA, F. A. 2020. A Role-Based Encryption Scheme for Securing Outsourced Cloud Data in a Multi-Organization Context. *arXiv preprint arXiv:2004.05419*.

SUNDMAEKER, H., GUILLEMIN, P., FRIESS, P. & WOELFFLÉ, S. 2010. Vision and challenges for realising the Internet of Things. *Cluster of European Research Projects on the Internet of Things, European Commision,* 3**,** 34-36.

SUTTON, J. & AUSTIN, Z. 2015. Qualitative research: Data collection, analysis, and management. *The Canadian journal of hospital pharmacy,* 68**,** 226.

TCHERNYKH, A., SCHWIEGELSOHN, U., TALBI, E.-G. & BABENKO, M. 2016. Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*.

THOMAS, D. R. 2006. A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation,* 27**,** 237-246.

THURMOND, V. A. 2001. The point of triangulation. *Journal of nursing scholarship,* 33**,** 253-258.

TIKKINEN-PIRI, C., ROHUNEN, A. & MARKKULA, J. 2018. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review,* 34**,** 134-153.

TIWARY, A., MAHATO, M., CHIDAR, A., CHANDROL, M. K., SHRIVASTAVA, M. & TRIPATHI, M. 2018. Internet of Things (IoT): Research, Architectures and Applications. *International Journal on Future Revolution in Computer Science Communication Engineering,* 4**,** 23-27.

TOMOVIC, S., YOSHIGOE, K., MALJEVIC, I. & RADUSINOVIC, I. 2017. Software-Defined Fog Network Architecture for IoT. *Wireless Personal Communications,* 92**,** 181-196.

TORRECILLA-SALINAS, C., DE TROYER, O., ESCALONA, M. & MEJÍAS, M. 2019. A Delphi-based expert judgment method applied to the validation of a mature Agile

framework for Web development projects. *Information Technology and Management*, 1-32.
UKWUEZE, F. 2016. Towards a new consumer rights paradigm: Elevating consumer rights to human rights in South Africa. *South African Journal on Human Rights,* 32, 248-271.
UNCTAD. 2016. United Nations Guidelines for Consumer Protection. Available: https://unctad.org/en/PublicationsLibrary/ditccplpmisc2016d1_en.pdf [Accessed 20 December 2019].
UNISA. 2013. *POLICY ON RESEARCH ETHICS* [Online]. UNISA. Available: https://www.unisa.ac.za/static/corporate_web/Content/Colleges/CGS/documents/Policy-on-Research-Ethics-rev-appr-Council-20.09.2013.pdf [Accessed 02 October 2018].
UNODC. 2016. *Intentional Homicide Victims* [Online]. Online: United Nations Office on Drugs and Crimes. Available: https://dataunodc.un.org/crime/intentional-homicide-victims [Accessed 22 April 2020].
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, 6-7.
VAZQUEZ-FERNANDEZ, E. & GONZALEZ-JIMENEZ, D. 2016. Face recognition for authentication on mobile devices. *Image and Vision Computing,* 55, 31-33.
VOEGTLE, M. G. L., SPAULDING, D. T. & KATHERINE, H. 2006. Methods in Educational Research. San Fransisco: Josey Bass.
WANG, C. C. 2017. Conversation with presence: A narrative inquiry into the learning experience of Chinese students studying nursing at Australian universities. *Chinese Nursing Research,* 4, 43-50.
WANG, Y.-P. E., LIN, X., ADHIKARY, A., GROVLEN, A., SUI, Y., BLANKENSHIP, Y., BERGMAN, J. & RAZAGHI, H. S. 2017. A primer on 3GPP narrowband Internet of Things. *IEEE Communications Magazine,* 55, 117-123.
WANT, R., SCHILIT, B. N. & JENSON, S. 2015. Enabling the internet of things. *Computer,* 48, 28-35.
WARNER, M., GARDNER, C., WYDEN, R. & DAINES, S. S. 1691-Internet of Things (IoT) Cybersecurity Improvement Act of 2017. Proc. US Congr., 2017.
WEBER, R. H. 2010. Internet of Things–New security and privacy challenges. *Computer law & security review,* 26, 23-30.
WEBER, R. H. 2015. Internet of things: Privacy issues revisited. *Computer Law & Security Review,* 31, 618-627.
WILLIS, K., DALY, J., KEALY, M., SMALL, R., KOUTROULIS, G., GREEN, J., GIBBS, L. & THOMAS, S. 2007. The essential role of social theory in qualitative public health research. *Australian and New Zealand journal of public health,* 31, 438-443.
WYMAN, O. 2015. *The Internet of Things: Disrupting traditional Business Models* [Online]. Oliver Wyman. Available: https://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/jun/Internet-of-Things_Report.pdf [Accessed 30 August 2018].

XU, Y., HUNT, T., KWON, Y., GEORGIEV, M., SHMATIKOV, V. & WITCHEL, E. 2017. EARP: Principled Storage, Sharing, and Protection for Mobile Apps. *GetMobile: Mobile Computing and Communications,* 20**,** 29-33.

YAN, Z., ZHANG, P. & VASILAKOS, A. V. 2014. A survey on trust management for Internet of Things. *Journal of network and computer applications,* 42**,** 120-134.

YILMAZ, K. 2013. Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education,* 48**,** 311-325.

ZHANG, W. & QU, B. 2013. Security architecture of the Internet of Things oriented to perceptual layer. *International Journal on Computer, Consumer and Control (IJ3C),* 2**,** 37-45.

ZHANG, Y., MAO, M., RAU, P.-L. P., CHOE, P., BELA, L. & WANG, F. 2013. Exploring factors influencing multitasking interaction with multiple smart devices. *Computers in Human Behavior,* 29**,** 2579-2588.

ZHAO, G., RONG, C., JAATUN, M. G. & SANDNES, F. E. Deployment models: Towards eliminating security concerns from cloud computing. 2010 International Conference on High Performance Computing & Simulation, 2010. IEEE, 189-195.

ZIEBLAND, S., COULTER, A., CALABRESE, J. D. & LOCOCK, L. 2013. *Understanding and using health experiences: improving patient care*, OUP Oxford.

ZIEGELDORF, J. H., MORCHON, O. G. & WEHRLE, K. 2014. Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks,* 7**,** 2728-2742.

ZIGURAT. 2019. *Internet of Things - One of the Build Blocks of a Smart City* [Online]. Online: Zigurat Globla Institute of Technology. Available: https://www.e-zigurat.com/blog/en/internet-things-one-building-blocks-smart-city/ [Accessed 30 August 2019].

ZIMMECK, S., WANG, Z., ZOU, L., IYENGAR, R., LIU, B., SCHAUB, F., WILSON, S., SADEH, N., BELLOVIN, S. M. & REIDENBERG, J. Automated analysis of privacy requirements for mobile apps. 24th Network & Distributed System Security Symposium (NDSS 2017), NDSS, February 26 - March 1, 2017. 2017 San Diego, California.

ZWICK, D. & DHOLAKIA, N. 2006. Bringing the market to life: Screen aesthetics and the epistemic consumption object. *Marketing Theory,* 6**,** 41-62.

ZYSKIND, G. & NATHAN, O. 2015. Decentralizing privacy: Using blockchain to protect personal data. Security and Privacy Workshops (SPW), 2015 IEEE, 21-22 May 2015 2015 San Jose, CA, USA. IEEE, 180-184.

ANNEXURE A: ETHICAL CLEARANCE

UNISA university of south africa

DEPARTMENT OF INFORMATION SCIENCE ETHICS REVIEW COMMITTEE

17 December 2019

Dear Mr Mfanasibili Ngwenya

DIS Registration #: Rec-051219

References #: 2019-DIS-0050

Name: M Ngwenya

Student #: 36092444

Decision:

Ethics Approval from 17 December 2019 to 17 December 2024

Researcher(s): Mr Mfanasibili Ngwenya
36092444@mylife.unisa.ac.za
082 998 9342

Supervisor(s): Prof MS Ngeoep
ngoepms@unisa.ac.za
012 429 6071

Data privacy, security and trust in "consumer internet of things" assemblages and associated mobile applications in South Africa.

Qualifications: Doctoral Study

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

ANNEXURE B: INTERVIEW SCHEDULE

1. Narrative Interviewing

I want you to tell me how experiences of how your life has changed for the better or worse since you installed the system whereby you control certain things via your smartphone. I want you to think about all the things you can manage and get more information from while using your smartphone or tablet. Think about your life before having such a system (past), your current situation (present) and your behavioural intentions (future) as if it were a novel. I want you to tell me about your concerns and benefits. There is no need to rush and so please give me details because I am interested in everything important to you. I will no longer ask questions henceforth. I will only take notes on the things I would like to ask you about later. If we do not have time today, maybe in the second interview.

2. Delphi Technique

A. Round One

- In your opinion, what are risk or issues that come with the adoption of the Internet of Things by consumers? If you can, give examples.
- With the risks or issues in mind, in your opinion, what is the role of regulators, smart device manufacturers, application developers and consumers, in curbing the problems and risks in consumer internet of things and associated mobile apps?
- What have the SA legislations done to address data privacy, security and trust issues when it comes to consumers of the Internet of Things?

B. Round Two

i. General

- What do you think are the main concerns of consumers of IoT in the South African environment?

- What can consumers do protect their personal information while using the CIoT assemblage?
- What do you think is the perception of consumers of IoT when it comes to technology's general security?
- Do you think consumers are willing to share private information?
- Do you think data privacy, security, and trust issues will prevent IoT Adoption?
- From your experience in the field of IoT,
    - Do consumers have any opinions on the risks in using IoT objects?
    - Are consumers willing to share private information?
    - Are consumers aware of the private information they share with the CIoT assemblage when using the services of CIoT?
    - Do the consumers know or even care where their personal information is stored, how secure is the storage and where is the storage?
    - Do consumers have any control over their data?
- Do CIoT service providers store information in one location or multiple locations?
- Do CIoT service providers act responsibly when dealing with consumers' data?

ii. Legal

- What legal instruments exist in South Africa to address the issues of data privacy, security and trust as far as consumer internet of things is concerned?
- What international legal instruments exist that South Africa can leverage on to address issues of data privacy, security and trust issues in South Africa in as far as CIoT is concerned?
- What challenges do you think such the use of international legal instruments can pose to the South African environment?
- What legal steps can service providers of CIoT (cloud providers, device manufacturers, application system providers, etc.) take to protect consumers' personal information while using CIoT?
- Do South African consumers have any legal recourse when their information become subject of abuse outside the borders of South Africa?

iii. Technical

- What are the technical steps that South African stakeholders can take to address issues of data privacy, security and trust issues?
- What technical approaches exist that can ensure that there is no compromise of personal information in the end-to-end communication of CIoT?
- What technical approaches exist that can ensure that there is no compromise of personal information when storing CIoT data?
- What technical approaches exist that can ensure that hackers do not hack CIoT systems?

C. Round Three

The following Round Three questions or statements came from consolidated Round Two answers. Please rank the statements according to your level of agreement with it. You may change the views you had in Round Two as you please and comment on your final rankings in the comments section. The research seeks to gain further insights from your comments. The first part of the statements is about legal frameworks, the second part is about technological approaches, and the last part is generic statements. You should rank each statement as follows:

Strongly Disagree _____ **Strongly Agree**

1 2 3 4 5 6 7

Legal Approach

Statement	Score	Comments
1. The South African regulators are doing enough to regulate the use of consumer IoT		
2. South African should learn from international legal instruments such as those from the European Union, the United Kingdom and the United States		
3. The POPI Act is the most appropriate legal instrument to use in South Africa to address CIoT challenges		

Statement	Score	Comments
4. The Electronic Communications Act is the most appropriate legal instrument that South Africa can use to address CIoT challenges.		
5. The Electronic Communications and Transactions Act is the most appropriate legal instrument that South Africa can use to address CIoT challenges.		
6. The Consumer Protection Act is the most appropriate legal instrument that South Africa can use to address CIoT challenges.		
7. Personal privacy should solely be the responsibility of the consumer		
8. The Authorities (ICASA) should hold CIoT providers accountable concerning the safety and privacy of consumers		
9. Every CIoT device should undergo heavy scrutiny before being allowed to be used in the South African environment		
10. South African Bureau of Standards is doing enough to enforce that all CIoT		

Statement	Score	Comments
devices are not a threat to South African consumers' privacy		
11. The Independent Communications Authority of South Africa is doing enough to enforce that all CIoT devices in the South African market are not a threat to consumers' privacy		
12. The Electronic Communications Act is capable of dealing with CIoT concerns		

Technological Approaches

Statement	Score	Comments
13. Device manufacturers use common default passwords on most CIoT devices		
14. Device password should be frequently changed		
15. Device password should be intricate and unpredictable		
16. Passwords are enough to protect the CIoT system from hackers		
17. Encryption should be applied in all CIoT devices		

Statement	Score	Comments
18. Devices should allow over the air software updates		
19. Consumers should buy CIoT devices from reputable original equipment manufacturers only		
20. Devices that are no longer use should be disconnected from the CIoT system		
21. Devices should only use open standards and avoid proprietary systems		
22. Personally identifiable information (PII) usually resides on the CIoT device		
23. Personally identifiable information (PII) usually resides in the cloud		
24. Location-based services are too dangerous for consumers		