Factors influencing user adherence towards privacy standards in the usage of Internet of Things devices in South Africa

A thesis submitted in partial fulfilment of the requirements of Master of Commerce at the Department of Information Systems University of Cape Town.

By Kizito Philip Bazanye (BZNKIZ002)

Supervisor: Doctor Walter Uys

Co-supervisor: Professor Wallace Chigona

ABSTRACT

Background: The Internet of Things (IoT) is considered an essential element of the Fourth Industrial Revolution (4IR). IoT devices are vulnerable to attacks. These vulnerabilities affect all aspects of daily life including retail and home automation interconnected by basic networking. The vulnerable end nodes may be machines, human to machine interactions, and the integration points of human-to-human communication.

Problem statement: The onset of the Covid-19 pandemic ushered in increased use of IoT devices. The increased use of IoT devices perpetuated negligent use and therefore cyber-attacks exposed South African IoT users' data harvested through these devices.

Purpose of research: The objective of the study is to conceptualise and understand what factors influence IoT device users to adhere to recommended IoT device privacy standards in South Africa.

Design/methodology/approach: This qualitative, interpretivist, cross-sectional exploratory research was guided by a three-phase approach using Activity Theory. The ontological stance adopted is subjectivism. The interview questions were derived from the Activity Theory model and themes identified in the literature reviewed. The qualitative data collected from the semi-structured interviews was analysed using deductive thematic analysis by linking of elements to the six components of Activity Theory.

Findings: The lack of privacy adherence is driven by a lack of trust in IoT devices and service providers as well as convenience and health factors. Additionally, users' personality, awareness and surroundings are major influencers to IoT device privacy standards' adherence.

Contribution and implication: This study conceptualises how IoT device privacy standards adherence can further be promoted with the increased adoption of such technologies. Further research may need to examine the specific impact of legislation on users and IoT device privacy. Additionally, the impact of third-party IoT service providers on IoT privacy models in South Africa needs to be investigated.

Key Words

Internet of Things, South Africa, Privacy standards, Adherence, Activity Theory.

Plagiarism Declaration

I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.

I have used the APA sixth edition convention for citation and referencing. Each contribution and quotation in this proposal from the work(s) of other people has been attributed and has been clearly cited and referenced.

This thesis is my own work part of which appeared in earlier coursework deliverable submissions including an assignment titled "IoT Privacy Management Issues: A Retrospective-Prospective Review" submitted on May 14th, 2020. A Masters' research proposal titled "User adherence towards privacy standards in the usage of IoT devices in Africa" submitted on May 28th, and literature review titled "User adherence towards privacy standards in the usage of IoT devices in Africa" submitted on July 17th, 2020.

I have not allowed and will not allow anyone to copy my work with the intention of passing it off as his or her own work.

I acknowledge that copying someone else's work, or parts of it is wrong and declare that this is my own work.

Signature: Signed by candidate Date: 8th February 2022

Acknowledgment

"*I can endure all these things through the power of the one who gives me strength*": - Philippians 4:13.

I would like to thank the Lord Jesus, for without Him, nothing would be possible.

A big thanks to my South African and Ugandan families, this has been a rollercoaster and no man is an island. Special thanks to My parents Mr. and Mrs. John-Mary Kiwanuka, my sister, Winnifred. Brothers, Denis, Lawrence, Felix, Frank, and Joseph.

Special thanks to my main supervisor Dr. Walter Uys for the guidance and the enlightening talks. To Professor Wallace Chigona, the co-supervisor, thank you for bringing the perspective of fellow students that further helped broaden my thinking.

To the I.S Master's class of 2020 that endured the pandemic, we have made history!

Table of Contents

List of Figures

List of Tables

Acronyms

Term	Description/Definition
5G	Fifth Generation
APIs	Application Programming Interfaces
AT	Activity Theory
AUCCSPDP	African Union Convention on Cyber Security and Personal Data Protection
CCSA	Competition Commission of South Africa
CCTVs	Closed-Circuit Television
CHAT	Cultural-Historical Activity Theory
DCTT	Digital Contact Tracing Technology
FTTH	Fibre-To-The-Home
HCI	Human-Computer-Interaction
ICASA	Independent Communications Authority of South Africa
IDC	International Data Corporation
IIoT	Industrial Internet of Things
IoT	Internet of Things
IS	Information Systems
MTR	Mobile Termination Rates
MUIPC	Mobile Users Information Privacy Concern Model
NB-IoT	Narrowband Internet of Things
OTT	Over-The-Top
POPIA	Protection of Personal Information Act
RFID	Radio Frequency Identification
SIoT	Social Internet of Things
SNS	Social Network Services

"THE MOST PROFOUND TECHNOLOGIES ARE THOSE THAT DISAPPEAR.
THEY WEAVE THEMSELVES INTO THE FABRIC OF EVERYDAY LIFE
UNTIL THEY ARE INDISTINGUISHABLE FROM IT"
(WEISER, 1991, pp. 94–100)

1. Introduction

This Chapter will be introducing some pertinent definitions, components, and characteristics of IoT, followed by an exploration of the research problem. This Chapter states the main research questions and the objective of the study.

1.1 Key definitions

1.1.1 Internet of Things (IoT)

The term "Internet of Things" (IoT) was coined by Kevin Ashton in 1999 when integrating Radio Frequency Identification (RFID) antenna into objects for retail tracking (Dries, 2018). For this research, IoT is a network of physical and virtual internet connected objects that allow humans to react and modify their environments. Several complementary definitions have been made for the term IoT. **Table *1*** depicts a few more definitions of IoT from some of the reviewed work with a brief theme indicator of what the definition entails.

Table 1: *Sampled literature summary of IoT definitions from the various authors reviewed.*

	(Brill & Jones, 2017; Sikder et al., 2018)	(Atzori et al., 2017)	(Bailey, 2015)	(Brous et al., 2020)	(Ng & Wakenshaw, 2017)	(Subahi & Theodorakopoulos, 2019)	(Dlamini, 2017)
Internet Connected/Networked	✓	✓	✓	✓			✓
Sensors	✓	✓			✓		✓
Wireless	✓		✓		✓		
Low-cost						✓	
Data and Storage	✓	✓	✓				
Everyday Objects		✓		✓			

Most definitions explored in Table one envisage a concept of networking or interconnectedness which is characteristic of IoT.

1.1.2 Thesis definition of a user

For this research, a user is any individual who seeks to benefit from functionality provided by IoT devices.

1.1.3 What is IoT privacy

IoT is evidently becoming one of the most important conduits of human genius demonstrated by the integration of different objects and systems virtually communicating with each other. The integration points of these objects must be secured both physically and virtually to mitigate existential threats to IoT objectives. The security in this respect refers to privacy and therefore, some scholars have had varying views on what privacy in general should be, with some referring to it as dispositional and situational privacy (Padyab & Ståhlbröst, 2018). Privacy is generalised as the control whether personal data can be gathered, processed, stored, and re-used (Kokolakis, 2017). Combining privacy and IoT thus makes this study's working definition of IoT privacy as "the extent to which information is collected, shared, or used in a specific context" (Karpf, 2017). IoT continues to undergo evolution that will carry on for a few more years with the discovery of newer technologies.

1.1.4 What is adherence

Adherence more often than note is interchangeably used with other words like "concordance" and "compliance". However, for this thesis, adherence is defined as the following of and conformance to the prescribed security and privacy recommendations regarding proper use of IoT devices.

1.2 The components and characteristics of IoT

IoT can be termed as building blocks of existing technology stacks. It is made up of hardware and software. Sikder et al. (2018) identify IoT architecture to comprise of four major components: sensing, network, data processing, and application layers. The sensing layer collects data from the real world through sensor hubs and these may include motion sensors. The network layer follows with its main purpose of serving as a conduit from the sensing layer, then the data processing layer follows on as the data handler from all these layers. This culminates in the application layer which is user centric. IoT is characterised by complexity, heterogeneity, context-aware and low-energy features of most devices that are interconnected to collect and or process data from dynamic environments (Atlam & Wills, 2020).

1.3 Problem statement

Privacy and security in IoT are ongoing discourses in information Systems (IS) research (Roman et al., 2013; Sen et al., 2018). The Covid-19 pandemic and associated lockdowns from early 2020 have led to the increased use of IoT devices and the proportionate increase in ransomware attacks. South Africa was ranked fourth according to number of cyber-attacks, with a total of 10.574 million by mid-2021 (SonicWall, 2021). The SonicWall (2021) report showed that the first six months of 2021 saw a reported 304.7 million total number of cyber-attacks surpass the total of 304.6 million recorded in 2020. These attacks seek regular device users' information through nefarious means.

There have been privacy related breaches reported in prominent media within the last four years involving IoT devices including smart Televisions, Ring door cameras (Brewster, 2017; Holmes, 2019; Wolfe & Ries, 2019) and connected smart cars like Tesla (Winder, 2020) (Winder, 2020). As recently as 2019, there was a reported 50.43% increase in IoT malware-based attacks originating in Egypt on South African consumer routers (ATLAS Security Engineering and Response Team (ASERT), 2019). The increased privacy related incidents and cyber-attacks can be attributed to the proportionate increase in individual user uptake and consumption of IoT devices, for the sole benefit of daily task automation.

In addition, IoT device users unconsciously shun privacy controls and policies afforded to them by device manufacturers (Tawalbeh et al., 2020). The negligence of privacy controls and policies open room for IoT device focuses to shift towards data collection (Rutledge et al., 2017), and this leaves many IoT devices and IoT users as targets since privacy is relegated to the background. Consequently, possible solutions to better privacy controls lead to change in business models, though the several business models are geared towards IoT adoption and very few of them have a measurement aspect for adherence (Palattella et al., 2016). These business models leave users with cybersecurity vulnerabilities leading to privacy breaches inadvertently.

The Fifth generation (5G) communication standard is infiltrating more rural areas since approval of more spectrum by the regulatory body in 2020 (Independent Communications Authority of South Africa, 2020, 2021). Several sectors in South Africa will be boosted by the dependence of IoT applications on 5G. These sectors include e-Health services and e-Education. However, given the communication speeds afforded by 5G, there arises the need to secure data transferred over these networks from the more than four hundred 5G ready devices. Therefore, it is very important for the end users to adhere to the recommended privacy standards of these devices.

1.4 Research questions and objective

There is a need to illustrate what a researcher seeks to know about the views and intentions of the individuals involved in any social setting (Agee, 2009). This illustration is achievable through questioning with the intention of exposing the underlying views and intentions. Agee (2009) notes that qualitative questions direct both the theoretical and methodological aspects of the study.

Figure *1* demonstrates the process followed for the formulation of the research questions. It includes the planning stage, collecting search terms and keywords, exploration of the located literature, discovery, defining and formulating the research questions and lastly, reflecting on the questions to gauge the ethical impact. Reflexivity is emphasis on awareness of the researcher's involvement in the process of research (Carpenter, 2018).

Figure 1: *Research question formulation*

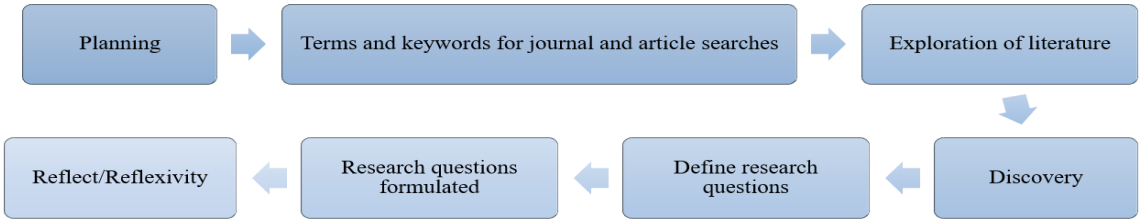
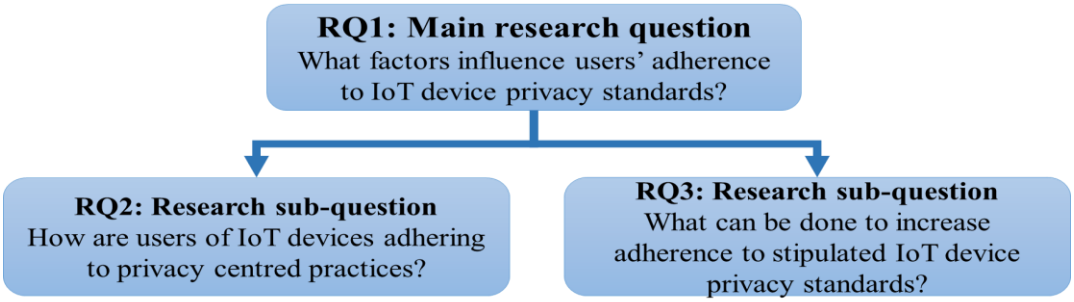


Figure 2: *Research questions derived from literature and guided by theory.*



The questions in **Figure *2*** are drafted following the process described in **Figure *1*** in conjunction with the gaps identified in the literature reviewed. Research Question One is as follows: What factors influence users' adherence to IoT device privacy standards? The research sub question attempts to understand how IoT device users are adhering to privacy centred practices. The third question aims at enquiring about what can be done to increase adherence to stipulated IoT device privacy standards. The objectives of this study are laid out in Table 2.

Table 2: *Research objectives*

Question	Objective
What factors influence users' adherence to IoT device privacy standards?	To understand the factors influencing users' adherence towards privacy standards in the use of IoT devices in South Africa.
How are users of IoT devices adhering to privacy centred practices?	To interpret how users are keeping to the prescribed IoT privacy standards.
What can be done to increase adherence to stipulated IoT device privacy standards?	To formulate a conceptual framework

1.5 Layout of thesis

This document is structured as highlighted in Table 3. The introduction has been covered in this chapter. The literature review is covered in Chapter two, it covers some of the work done by authors in the field of the Internet of things (IoT). Chapter three details the theoretical and conceptual frameworks that guide this study. The research design and methodology adopted for this study are covered in Chapter four. The data analysis is explored in Chapter five and the findings presented in Chapter six. In Chapter seven, a conclusion to the research is drawn.

Table 3: *Layout of thesis*

Chapter	Title
1	Introduction
2	Literature review
3	Theoretical and conceptual framework
4	Research design and methodology
5	Data analysis
6	Research findings
7	Conclusion
References	
Appendix	

1.6 Summary of chapter

IoT involves multiple sensors and devices networked, responsible for data creation and processing. The growth of IoT opens specific risks due to the increased uptake of IoT related technologies by users adapting to the Covid-19 pandemic. This study's objectives seek to conceptualise, understand what influences users to adhere to recommended IoT device privacy standards. The Chapter that follows analyses the literature to this effect.

2. Literature review

This chapter analyses the work of other scholars in respect of understanding the factors driving users to adhere or not, to the recommended IoT device privacy standards. The literature was sourced from internet sources including but not limited to Google Scholar, EBSCOHost, Springer, ScienceDirect, conference proceedings like IEEE and other academic journals. The keywords used included: Internet of Things (IoT), privacy, Covid-19 and IoT, internet privacy standards, privacy adherence.

2.1 Introduction

Several scholars have had varying takes on what privacy in general should be, for instance Padyab and Ståhlbröst (2018) referring to it as dispositional and situational privacy. The privacy studies done are mostly subjective and cultural (Williams et al., 2018). Other scholars including Kokolakis (2017) classify privacy into three aspects, physical area privacy, privacy of person and informational privacy.

A quantitative investigation of attitudes towards data privacy reported that a majority 32% of IoT users sought process control and transparency regarding the data collected about them (Wickramasinghe & Reinhardt, 2019). The Wickramasinghe and Reinhardt (2019) study revealed a willingness by users to reform attitudes towards understanding of privacy risks. However, the Wickramasinghe and Reinhardt (2019) study stopped short in identifying the factors that influence users to adhere to the recommended privacy safeguards in the use of IoT devices. It is the aim of this study and literature review to understand the works of other scholars regarding the privacy phenomenon.

2.2 Accountability, standards, laws, and regulations awareness

Effects of IoT on data privacy policies have been noted to result in persistent data privacy risks associated to how organisations collect and disclose sensitive individual data (Brous et al., 2020). Consumers were observed to lean towards retailers and organisations that prominently displayed privacy policies (Kokolakis, 2017). This was because consumers felt better protected by these displayed privacy policies. Consumer awareness in this instance influenced their interaction with the retailer since there is an indication of protection of their information and intent of accountability.

On 1st July 2020, South Africa's Protection of Personal Information Act (POPIA) of 2013 aimed at the processing of personal information by companies and other agents was

implemented (South-African Government, 2013). Due to the ensuing Covid-19 pandemic and its effects of individuals remote working, the POPIA legislation is much welcomed in South Africa (Job, 2020).

The onset of new legislation has led to new mandates to organisations consisting of accountability, processing limitations, audit and risk among others aimed at ensuring compliance and adherence (Kandeh et al., 2018). The POPIA should be a blueprint in guiding not only organisations, but individuals on how to adhere to privacy standards. Individuals should have an idea regarding what data is collected about them from the various devices. However, as with all new legislation, to bolster better understanding, adherence and interpretation, awareness training needs to be carried out. In addition, the use of technology to contact trace Covid-19 infections is a huge basis for debates. There is an intersection of POPIA legislation and the need to limit the spread of the virus, raising privacy concerns (Viljoen et al., 2020). Therefore, legislators need to be accountable to all stakeholders of the POPIA to improve adherence.

The Fifth Generation (5G) standard for communication was approved for use in South Africa on the back of a spike in broadband services' demand due to the Covid-19 pandemic (Independent Communications Authority of South Africa, 2020). However, a report from the same organisation recommended a mitigation of cyber-security risks associated with the adoption of 5G (Independent Communications Authority of South Africa, 2021). The mitigations include designing security into policies by amending of the Electronic Communications Act of 2005. These mitigations point to willingness by the regulators to have more safeguards for protecting privacy. Since 5G has been seen to be a major catalyst for faster communication links between devices, using some IoT devices becomes easier. The increased speed compounds the increase in data transfer and unforeseen breaches.

As of 2020, only 18 of 55 African countries have been involved in the African Union Convention on Cyber Security and Personal Data Protection (AUCCSPDP). The legal framework for Cyber-security and Personal Data Protection meant for African Union member states was signed on July 27, 2014, in Equatorial Guinea. This convention "requires all states to establish an independent administrative authority tasked with protecting personal data" (Ball, 2017, p. 164). The convention mandates all African states to constitute independent administrative authorities charged with personal data protection activities. The slow adoption of the continent-wide initiative is an indicator of attitudes held by African governments to the idea of a cyber privacy standard to form part of legislation to guide IoT users.

Internet of Things (IoT) users have been found to be more aware of issues that could impact IoT usage especially mobile devices (Foltz & Foltz, 2021). Rutledge et al. (2017) concur to some extent that keeping to the policies has been proven to be tough for both individuals and entities since regulations vary greatly. Privacy regulations are designed with the end user in mind. Efforts have been made to ensure some level of automation is used in the improvement of IoT privacy policies to make them user centric (Shayegh et al., 2019). User centricity would be paramount in enhancing adherence levels.

From an accountability perspective, it is paramount that any information system stakeholders are aware of their duties and obligations regarding trust in the system in question. The emphasis should be on the need for legal frameworks to guide rights and responsibilities that can be used to hold entities liable to any breaches (Singh et al., 2018).

Brill and Jones (2017) point out Issues relating to stifling innovation in industries in terms of tough laws in the name of data protection. These are major hurdles to any newcomers and existing players in adhering to these data protection measures. For any Innovation to happen, it must be guided by favourable existing policies that make adherence a viable option (Sollins, 2019).

The Competition Commission of South Africa (CCSA) concluded that the South African prepaid data prices charged by the major network operators were exorbitant. A subsequent recommendation for remediation was issued by the national government to facilitate investment incentives directed towards Fibre-To-The-Home (FTTH) providers to rollout networks in low-income areas (Competition Commission of South Africa, 2019). This approach will hopefully positively influence adherence to prescribed standards because of sound regulatory policies as manifested by the South African Competition Commission. A reduction in cost to access of internet might in turn lead to better attitudes.

Device manufacturers have been found not to fully comply with their own issued IoT device privacy policies (Subahi & Theodorakopoulos, 2018). The non-compliance signifies that what IoT device manufacturers state in the privacy policies greatly varies from what their IoT devices portray. Therefore, the risk is born by the end user whereby the grey area between actual behaviour of IoT device and what is stated in the documentation is easily exploited by hackers. These exploitations can eventually lead to cyber-security breaches given the purpose of the IoT device involved.

2.3 Behavioural attitudes and patterns

Subahi and Theodorakopoulos (2019) deduced that many technology users are not aware of the data that is collected about them. This has led to the combination of IoT and surveillance (Alsmirat et al., 2017). The attitude and lack of awareness in the use of IoT devices is being exploited for surveillance purposes. Anjomshoa et al. (2017) identified a rise of Social Internet of Things (SIoT) having studied the behaviour relating to users' activities on connected devices (behaviometrics). Evidence of this concept is demonstrated in the efforts of several countries and governments using sensors and Bluetooth on smartphones for contact tracing in the attempt to curb the Covid-19 coronavirus spread (Cho et al., 2020). However, it cannot be concluded if the attitudes towards contact tracing were positive.

Atzori et al. (2017) demonstrate that in society, smart systems in IoT assist in tracking both online and physical malicious behaviours by collecting data. Patterns can emerge in the data collected to show unwanted behaviours in society that should assist in maintaining security and privacy. A use case is in the curb of bullying with the use of mobile devices and mobile applications by simply using the volume controls on the device (Mohalder et al., 2019). There is a potential of introducing further sensors including cameras with facial identification to locate perpetrators. The use of sensors can be analysed to influence adherence to any laws by perpetrators.

There is a habit of not updating default settings since they work straight out of the box. Users find these default settings hard to find or rather inconvenient to amend (He, 2019). He identified that most users carry on the habit on most of their IoT devices. A pattern develops whereby if they do not see any justification for tinkering the device's settings, there is no compelling reason to treat the other devices owned separately other than convenience according to Zheng et al. (2018). These attitudes towards learning about IoT devices occasionally mean IoT device users are non-adherent.

2.4 Sensitisation on IoT

Users have been found to be the most vulnerable link in any IoT ecosystem (Chong et al., 2019). Chong et al. (2019) suggested that device manufacturers need to be proactive about informing users regarding their safety and information when using inter-connected devices. Alert and vigilant users of IoT devices could possibly thwart privacy breaching incidents through better knowledge of information collected about them. Additionally, Chong et al. (2019) proposed intelligent training systems that learn user's behaviors and adjust the instruction manuals. These manuals would be tailored to match the users' usage profiles.

There is a challenge of redefining curricula whereby students must be prepared for digital problem-solving skills (World Economic Forum, 2018). According to a survey by the World Economic forum (2018), it was found that 54% of student respondents preferred computer science the most compared to several other subjects inclusive of English and Mathematics. To that effect, a recommendation of changing curricula would align with the increasing wave of IoT with preparing current students for future job roles associated with IoT. With the increased education that is based on curricula with IoT in mind, the greater the awareness of users to the benefits of IoT (Nelke & Winokur, 2020). Nelke and Winokur (2020) are proponents of sensitisation through education to achieve greater awareness around benefits of IoT.

For students and teachers alike, a matter of not adhering to new technology standards could mean not getting or providing an education. IoT is an instrumental means in the adaptation of most traditional learning practices to transition to smart online approaches (Makarova et al., 2018). For instance, real time lecture feedback and IoT based smart labs assist closing the feedback loop for both students and teachers from a lecture point of view (Gul et al., 2017). Gul et al. (2017) further note that this aspect of IoT comes in tow with its own demerits which include cost, security, and privacy. Should there be any privacy breaches, teachers' and students' personal information that may include financial and medical details would be at the mercy of attackers. It is therefore evident that for any student or Instructor in a bid to achieve a good education, they must decide whether to adhere or not to the standards set forth.

At the University of KwaZulu-Natal in South Africa, 91% of academics believed that there is a substantial benefit in the use of ubiquitous computing to promote productivity of lecturers (Motala & Padayachee, 2018). Motala and Padayachee (2018) additionally found that through conducting classes remotely, 86% agreed that lecturer flexibility and convenience was boosted. The proof of benefits of remote learning boosted by IoT is evident and as noted earlier by Gul et al. (2017), all these lecturers are vulnerable to privacy breaches in remote teaching. Safety is paramount when interacting with IoT.

2.5 Safety and security

In South Africa, with the high reported crime rates mostly involving burglary and household crimes (Statistics South Africa, 2019), IoT has assisted in the aspect of community safety and policing (Birhane, 2020; Dlodlo et al., 2015). The opportunity cost to these communities involves embracing surveillance and therefore adherence to the community standards of having these IoT installations is paramount. Activities in many public places are surveilled with the use of Closed-circuit Television Cameras (CCTVs) (Dlodlo et al., 2015).

Dlodlo et al. (2015) identified behavioural traits as variables that can be used as part of a system architecture to be implemented for the purpose of deterrence and policing.

National power grids and utilities have deployed IoT installations that are aimed at serving communities. Daily operations are automated and monitored with a variety of sensors and cameras as nodes in these vast IoT networks. However, privacy is seldom an afterthought since concerns arise regarding mission critical utility installations being compromised for ransom by criminals. IoT enabled utilities are compromised with denial-of-service attacks affecting entire communities (Kolias et al., 2017). According to INTERPOL's Cyberthreat Assessment publication, South Africa has the third highest victim count as a result of cybercrime (Dolley, 2021; INTERPOL Cybercrime Directorate, 2021). An electricity utility was compromised leading to unprecedented blackouts (BBC, 2019). The effects of these cyber-attacks focus the importance of adherence to basics of privacy at a mission critical utility utilising IoT devices.

2.6 Home and health IoT

On 11 March 2020, the coronavirus outbreak was declared a pandemic (World Health Organization, 2020). The outbreak has negatively impacted economies, global markets, world travel and widespread panic buying by individuals (Jones et al., 2020). Contact tracing which is the tracking down of individuals in contact with any persons that tested positive, became a plausible solution for governments and health departments alike to effect easing of restrictions.

Singapore launched a Bluetooth based TraceTogether application to aid the contact tracing effort (Fathin, 2020). Fathin (2020) noted that the major privacy concerns manifest in the lifespan of these contact tracing applications, and whether if they will be decommissioned or repurposed at the end of their intended life spans. In addition to unknown lifespan, if people decide not to adhere by leaving their phones at home to make the Digital Contact Tracing Technology (DCTT) even more difficult to fully utilise (Kahn, 2020).

Sub-Saharan Africa is projected to have a population of 8.5 billion by the year 2030 (United Nations, 2019). The UN also notes that the world population is aging at a faster rate and therefore healthier lifestyles are required. Individuals have turned to IoT in the form of fitness and sleep monitoring (Haghayegh et al., 2019). Individuals engage with IoT devices with the motive of enhancing quality of life (Swaroop et al., 2019) and to lead healthier lifestyles.

Users of IoT devices have been found to prefer the conveniences provided by IoT implementations in a home setting compared to the potential risks to privacy (Zheng et al., 2018). It is worth noting that users considering the convenience of home IoT technology is only detrimental to their privacy as noted by Zheng et al. (2018). These attitudes towards home

automation inadvertently influence adherence to the standards designed by the manufacturers of these devices to preserve privacy.

With 5G gaining popularity in applications to benefit IoT, there has been a spike in applications for health monitoring purposes (Kelly et al., 2020). The spike in monitoring will aid faster IoT Based architectures that will enable scaled and decentralised data processing for healthcare according to Kelly et al. (2020). These authors are however sceptical about enforcement of data security across IoT health devices. Privacy is however a major point of contention in the IoT health sector.

2.7 Cost and profit factors in relation to IoT

Even though the focus of this work is on the end user, the other stakeholders in IoT influencing adherence cannot be ignored. One of the major stakeholders investing in IoT are the large corporations which are mostly driven by profitability (Burtch et al., 2018). Corporations such as Apple, which started up the Apple HomeKit (Feiler, 2016), Samsung started up Samsung Smart Things and Google's Android Things that is used in Raspberry Pi (Chibuye & Phiri, 2017). It becomes pertinent that most of the supporting applications installed on IoT devices come at an additional cost and require more permissions than they need to function (Fernandes et al., 2016). Fernandes et al. (2016) managed to hack their app and trigger fake fire alarms and steal phone lock codes. This is an illustration that the existing mainstream platform and solution providers exacerbate privacy related issues by making daily use more costly and complicated. There is a need to address the question of privacy as existing mainstream platform and solution providers seem to be overlooking.

Furthermore, in Uganda, the government introduced and imposed the Over-The-Top (OTT) tax intended to curb social media usage despite the dismal compliance levels from the populace (Asiimwe, 2019). This tax significantly increased the cost of access to internet. Asiimwe (2019) observes that the compliance of such a tax is related to the education level. The noncompliance in the long run results into nonadherence to a standard meant to foster privacy by individuals. Such taxes like OTT have been found to hinder the realisations of African digital goals like the Science, Technology, and Innovation Strategy for Africa 2024 (STISA-2024) (African Union Commission, 2014; Kasadha et al., 2019). Therefore, the propensity to consume is compounded by tax having a knock-on effect on the retail sector.

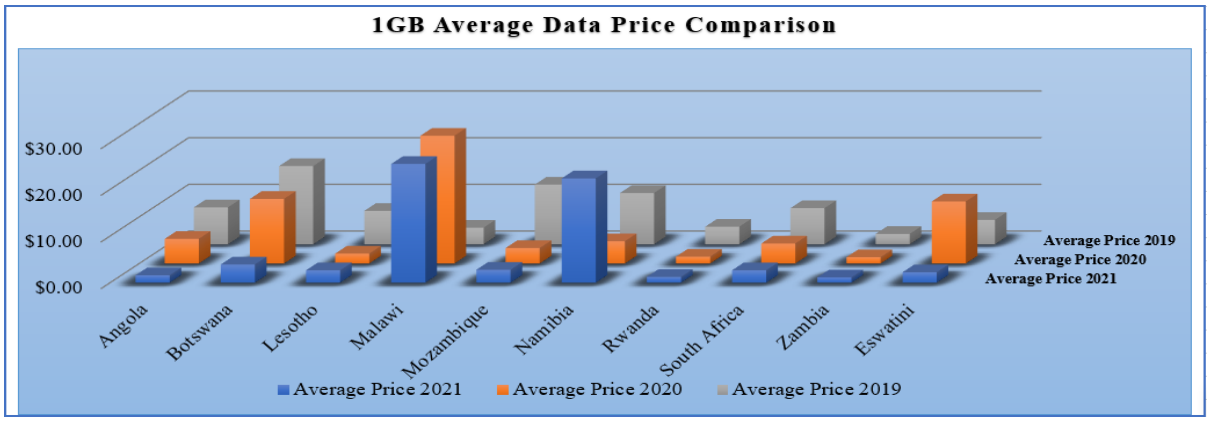
South African retailers' adoption of IoT is slow due to the focus on business processes first, and then gradual use of IoT as an enabler (Dlamini, 2017). Dlamini reiterates the cost of this approach as a major challenge despite the benefits to South African retailers investing in IoT.

For instance, retailers deploy IoT tools to execute behavioural analysis of customers whilst in stores which put their privacy in question. It stands to be proven if customers' privacy rights are not infringed upon by these very retailers in pursuance of profits and customer experience improvement.

Mobile Termination Rates (MTRs) are the price that mobile network operators charge each other for call switching between their networks (Hawthorne, 2018). Hawthorne (2018) identified the decline of MTRs by more than 90% between 2009 and 2017. The benefits in the drop-in rates were not fully passed on to the final consumer in South Africa. The decline in these rates has seen consumers incurring higher costs in running IoT devices that utilise the South African Mobile network provider services.

Nevertheless, South Africa has been observed to have some of the most expensive mobile data prices in Southern Africa based on the cost of 1GB of data, in comparison to countries including Zambia and Lesotho as of 25th February 2021 (www.cable.co.uk, 2021). **Figure *3*** summarises the data in Appendix G which speaks to the cost of 1GB of data in dollar terms.

Figure 3: *2019-2021 Average 3-year mobile data cost in select Southern Africa countries*



Note. Adapted from https://www.cable.co.uk/mobiles/worldwide-data-pricing/2021/mobile_data_price_comparison_data.xlsx by www.cable.co.uk

When internet access is expensive, it renders some users unable to update critical firmware and software. This inability exposes users as targets for cyber-attacks.

2.8 Related research on user adherence

The majority of user adherence research appears to be centred in the health IoT field focusing on medicine adherence and monitoring using IoT (Aldeer et al., 2018). Within this aspect, users concerned themselves with being monitored in addition to the privacy and safety of their medical data. The monitoring happens with various IoT devices such as heart rate

monitors and sleep trackers. Some specific devices such as smart wireless pill bottles are smartphone app linked to ensure reminders are sent to patients to adhere to their recommended pill regimens (Mishra & Rasool, 2019). The motive of these innovations is to ensure adherence to treatments and does not consider the privacy and security of user data.

Research into smart-homes revealed a lack of interoperability understanding of complexity of IoT devices influencing adherence (Zeng et al., 2017). Furthermore, the lack of technical ability to isolate IoT device dedicated Wi-Fi networks rendered users non-adherent and consequently vulnerable to attacks. Zeng et al, (2017) additionally elaborated on some users having ultimate trust in entities handling their data. Therefore, users deemed themselves adherent based on fully trusting the device manufacturers with their data.

2.9 State of IoT and future direction

IoT device management is fast becoming a significant pillar in IoT to aid in curbing malware. The IDC forecasted 79.4 zettabytes of data to be generated by IoT devices (IDC, 2020). Kolias et al. (2017) observed that due to the distributed nature of devices interconnected in IoT, there is a challenge of a growing number of IoT malware and botnets. Mirai is a type of malware that infiltrates IoT networks. Data generated opens up an entirely new challenge for data management (Hejazi et al., 2018). The IoT device management market is to the utmost degree unregulated and is characterised by low adherence to data protection laws.

Fifth Generation (5G) networks are becoming an aid for IoT and its associated industries therefore "by 2023, 80% of Industrial Internet of Things (IIoT) gateway vendors will offer 5G communications modules in at least one of their gateway products" (Gartner, 2020). The industrial, manufacturing and retail sectors will have highly automated workflows and production lines which in turn points to highly developed economies through 5G and how it will be used to effectively enable further IoT adoption. Palattella et al. (2016) concludes that despite 5G being one of the fastest wireless network enablers of IoT, it still faces the known wireless network issues including radio costs and power consumption. Furthermore, 5G has security and privacy challenges as well that can impact security (Sicari et al., 2015). Additionally, 5G network speeds accentuate data transfer rates and therefore can be misused for malware spread to all interconnected IoT devices.

Geo-politics is taking centre stage in the influence of IoT implementations and related technologies like 5G. The main example of political disagreements is the United States' ban on Chinese Company, Huawei Technologies in the context of its technologies being a security risk (Shepardson, 2020). Consequently, the United Kingdom followed suite with the ban of

Huawei technologies from being used in any 5G infrastructure by 2027 (Kelion, 2020). A ban of cheaper communication equipment could have a cascading effect on privacy standards adherence from an affordability point of view.

A scheme for privacy preserving IoT device management based on blockchain technology is possible to observe how information can be stored in public ledgers (He et al., 2018). He et al. (2018) discussed an attribute-based encryption that can be combined with a time-bound key management technique for transaction verification. The verification will ensure data that is collected is only used by the intended recipients only.

2.10 Gaps Identified

Most of the research reviewed focused mainly on developed countries at the expense of developing countries. More research needs to be done in understanding the factors influencing users to adhere to privacy controls whilst using IoT devices from a developing countries' perspective. The literature review has highlighted a pattern highlighting the need for more research in adherence to privacy policies in the consumption of IoT related devices and services.

The recommendations from the World Economic Forum (2018) are dedicated towards e-learning and updating of curricula to focus on teaching subjects that will boost knowledge in the IoT domain. The recommendations must be inclusive for disadvantaged communities in developing countries. Important elements like funding and adherence tracking models are not identified in detail.

Communication technologies in the form of 3G are the predominant technology in use in Africa (Cousin et al., 2018). Therefore, 5G rollout plans should be better detailed and not just depended on the slow speeds and developed nation infrastructure blueprints.

The study done by Motala and Padayachee (2018) had no provisions for synthesising whether adherence to privacy by academic respondents to ubiquitous computing in conducting classes remotely would be observed therefore leaving a gap in the study of the adherence phenomenon.

2.11 Concepts derived

This research is guided by the following concepts identified from literature reviewed in the preceding sections. The concepts are used in the formulation of the study research question. They are summarised in **Table *4***.

Table 4: *Literature derived constructs/themes*

Theme	References	Concept
Accountability, standards, laws, and regulations awareness	Brous et al., (2020). Foltz and Foltz (2018). Singh et al. (2018). Pepper and Botes (2020). Job (2020). Viljoen et al. (2020). Subahi and Theodorakopoulos (2018). South African Government (2013). Kandeh et al. (2018). Independent Communications Authority of South Africa (2021)	Accountability, Risk, Tech savviness.
Behavioural attitudes and Patterns	Anjomoshoa et al. (2017). Kokolakis (2017). Atzori et al. (2017). Cho et al. (2020).	Attitudes
Sensitisation on IoT	Makarova et al. (2018). Gul et al. (2017). Motala and Padayachee (2018).	Online study/teaching sessions, Group discussions, Smart labs, Education levels.
Safety and community	Birhane (2020). Dlodlo et al. (2015). H. Lin and Bergmann (2016). Ndubuaku and Okereafor (2015)	Physical Safety Consent to being monitored in community, Perceived security.
Home monitoring	Kahn (2020). Kelly et al. (2020). Swaroop et al. (2019. Haghayegh et al. (2019). Zheng et al. (2018)	Quality of life. Sleep monitoring, Home Automation
Access to Technology/Platforms	Bailey (2015). Ndubuaku and Okereafor (2015). Cousin et al., (2018). Hejazi et al. (2018). Kolias et al. (2017).	Number of devices owned, Platforms of devices, Pervasiveness (availability of IoT devices), Network access connection speed.
Cost and efficiency	Asiimwe (2019). Fernandes et al., (2016). Competition Commission of South Africa (2019). Cable.co.uk (2021).	Open-Source Solutions/Proprietary solutions. Smart-home implementations.

2.12 Summary of chapter

The literature review shows many potential determinants of adherence to privacy standards ranging from the need to benefit from the use of technology and the behavioural aspects pertaining to the IoT device users. Cost and profit factors play substantial role to the phenomena under study with some users aiming to obtain cheaper devices with inadequate privacy controls. This Chapter has explored what authors believe to be the future of IoT. Various themes have been identified to assist in drafting a conceptual framework that is detailed in the following Chapter. The following Chapter reviews the theoretical and conceptual framework adopted for this study.

3. Theoretical and conceptual frameworks

3.1 Introduction

The previous Chapter dealt with an investigation of studies and works of other authors in relation to the IoT privacy standards adherence phenomenon. The following sections review the guiding frameworks adopted for this research. Agee (2009) notes that during the research design process, the theory shapes the methods and connects the research to the field. The choice of a theory is also subjective, considering the researcher's background and interests (Walsham, 2006). In this Chapter, Activity Theory (AT) is adopted as a guiding theoretical framework and a conceptual model that has been drafted from the concepts derived from the literature review as a support to this study. Motivation Theory is briefly explored a possible theory that could have been adopted to guide the study.

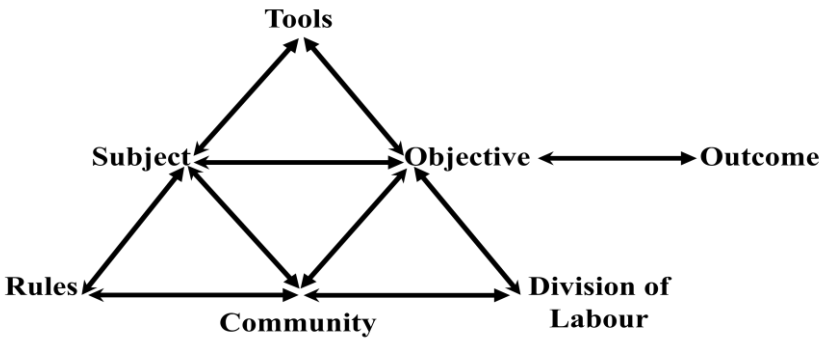
3.2 Activity Theory

Activity Theory (AT) is well suited to explain this research phenomenon due to its rich guiding principles which cater for the dynamics of environment, history, culture role, complexity, and rules. AT was first applied in Information Systems as a theory at the International Federation for Information Processing (IFIP) Working Group (WG) 8.2 Copenhagen conference that took place from 14th to 16th December 1990 (Nissen et al., 1991). AT is "all about 'who is doing what, why and how'" (H Hasan & Kazlauskas, 2014, p. 9). AT was initiated by the founders of the cultural-historical school of Russian psychology that is philosophically rooted in the works of Karl Marx (Engeström & Miettinen, 1999; Kuutti, 1996). Engeström and Miettinen (1999) suggest that AT has two continously operating intertwined processes at every level of human interaction. These processes are namely externalisation and internalisation, through which the researcher approaches phenomenon as an outsider and at the same time interacts with those individuals to get their interpretations of the activity in question.

Activity Theory is a a form of socialcultural analysis whereby all human activity transforms over time and is spread over individuals and associated cultures (Jonassen & Land, 2014). AT has six main components, namely; the main subject, object, tools, rules, community and division of labour contributing to the outcome (Engeström, 1987) when viewed from a system point of view and as illustrated in **Figure *4***. Kuutti (1996) identified AT to form a common lense guiding the increased Human-Computer-Interaction (HCI) qualitative Information Systems research. AT "focuses on studying and gaining better an understanding of the context

of human activities within social systems and environment" (Iyamu & Shaanika, 2019, p. 166). Therefore, this research draws attention to human users interacting with various computer systems inter-connected over the internet.

Figure 4: *Activity triangle* (Adapted from Engeström, 1987, 2014)



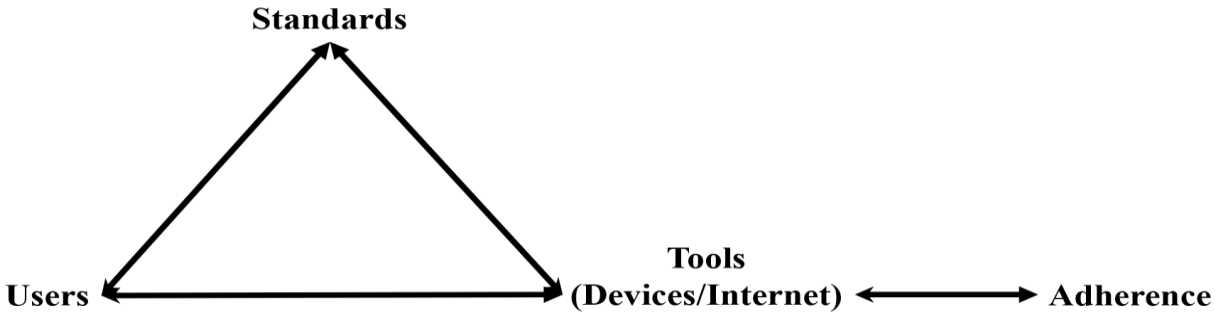
In this study, first generation AT is used in its purest form in comparison to the newer generations of AT like Cultural-Historical Activity Theory (CHAT) because of the necessity to adhere to Iyamu and Shaanika's (2019) three phase approach. This approach posits the use of AT by firstly selecting the AT as the study's theory, secondly, identifiying the elements of analysis and lastly, linking these analysis elements with the six AT components. On the other hand, CHAT seeks to grasp a systems' view and not just its components using a three pronged approach. First and foremost, collective human action, secondly, adaptation of tools for learning and communicating and finally, use of community as pillar for interpretation (Foot, 2014). Therefore, CHAT is rendered inadequate for the purpose of this study due to the limitations in approach. Activity Theory provides a heuristic basis for identifying the change in behaviour of actors of IoT which include users, business, and governments (Fu & Wu, 2018). Knowledge generation is a human activity that depends on processes, theories, facts, methods, and techniques used by researchers (Carson et al., 2011; Iyamu & Shaanika, 2019).

Karanasios and Allen, (2018) conclude AT to have the assisting ability of addressing the challenge of analysing interactions between technology and actors. A further assertion by Iyamu and Shaanika (2019) illustrates that, vis-à-vis information systems artefacts, no action of activity is complete by a single actor, but rather a mutually exclusive interaction between technology and humans completing the action.

Therefore, AT is used in line with the subjectivism ontological stance of this study as described in the philosophical considerations in Chapter four. IoT has many facets that involve human activity which can be tied back to user choice of adherence or non-adherence to the

prescribed privacy standards. **Figure *5*** illustrates how AT relates to this study. There is an intersection how users choose to interact with IoT standards. The main objective is adherence to privacy in the usage of IoT devices, which are the tools. There are rules which are the policies and "Human beings determine themselves through objects that they create" (Lektorsky, 1999, p. 66).

Figure 5: *AT triad for this study (Adpted from Engeström, 1999, p. 30)*

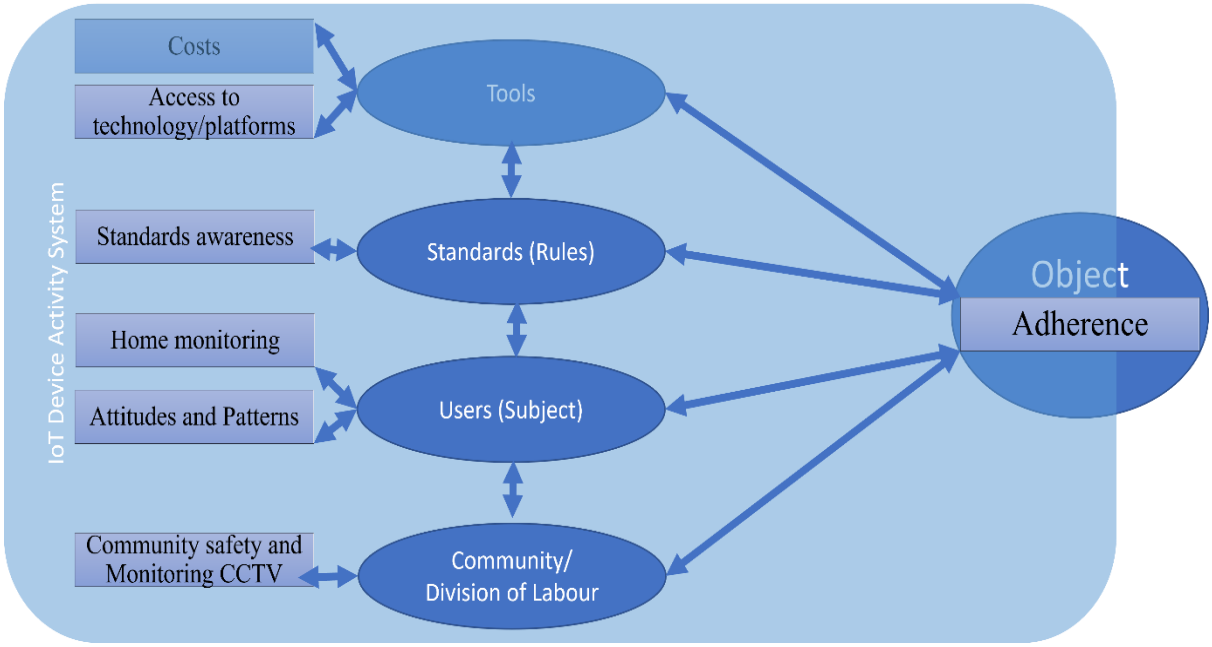


3.3 Conceptual framework

From the summarised literature reviewed in Chapter two, the phenomenon under study informs the conceptual model in **Figure *6***. The model has been used to create the interview questions as highlighted in Appendix C of this document. As demonstrated in the previous section and contextualising this study with AT.

The model speaks to the "tools" node, which symbolise the IoT devices, related services and supporting infrastructure inclusive of networks. The "subject" node represents the users of the "tools", there are "rules" that must be followed in this system which represents some of the privacy standards and policies. The model has a "community" node which is made up of the other stakeholders including government legislators and device manufacturers. "Division of labour" states the tasks that have to be done for the entire network to attain the "objective", which is the end goal of the activity. These nodes are further detailed sub-sections the follow. **Figure *6*** illustrates that all the nodes work together as a network or system to influence adherence or non-adherence.

Figure 6: *Conceptual model for IoT user privacy adherence patterns*



Inversely, if any of the nodes are removed from the network, the whole system ceases to function as a network aimed at achieving the adherence objective. The relationship of these nodes is discussed in the following subsections.

3.3.1 Tools

In the context of this study, tools can refer to any implement virtual or physical, that assist IoT device users in the objective of adherence. Tools represent the means through which the subjects in the phenomenon carry out an activity (Benson et al., 2008) or interact with the object, according to Kuutti (1996). For this research, tools include the physical devices and corresponding related services associated to IoT devices. These include but not limited to applications, subscriptions, and add-on third-party services. The associated cost of running these devices is also analysed. The cost includes maintenance, security, and data.

3.3.2 Subject

The subject, in relation to this study, is the unit of analysis, which is the IoT device human user. The Subject makes use of the tools, within the activity system to be able to achieve their objective. Subjects can also be a portrayal of "both individual and social nature of human activity as reflected through collaborations and consultations in order to satisfy a shared objective" (Mwanza, 2001, p. 3). In the conceptual model in **Figure *6***, subject has a few determining factors, which include personality habits. The habits influence the magnitude of adherence.

3.3.3 Rules

Rules are very essential for any system to achieve viability. For this study, rules include terms and conditions, privacy policies, Government legislation including the POPIA as gazetted by the South African Government (2013) and terms of services as stated by the device manufacturers. Benson et al. (2008) classify rules as directives governing performance of an activity.

3.3.4 Community

The community node in the conceptual model can be interpreted as the surroundings of the subject interacting with the tools. In the context of this study, subjects interact with the community directly or indirectly using tools and rules facilitated by a communication medium, with the sole goal of achieving the objective. Users of IoT devices cannot use these devices in isolation, they interact with other users and limitations on how these devices can be used in the form of rules. Mwanza (2001) suggests that a subject is a member of the community and therefore cannot be studied in isolation. The suggestion pertains to how the subject interacts with the objects and other subjects.

3.3.5 Division of labour

Kuutti (1996) suggests that division of labour is where the community is implicitly and explicitly acting on processes aimed at converting the object into an outcome. In this conceptual model, division of labour signifies the roles and responsibilities of the system actors. These actors include the IoT device user and the other users, legislators, the supporting services, and service vendors relating to the IoT devices. In line with subjectivism, social phenomena are a result of consequence and perceptions of social actors (Saunders et al., 2009). Engeström (1987) identifies division of labour as an effect of contrasting individual action and collective activity.

3.3.6 Object

The object is the goal for all activities in the activity system. Kuutti (1996) alludes to all actions in the activity system by the "subject", being aimed at achieving an outcome. For purpose of the conceptual model, the outcome is, determining if there is adherence or non-adherence to the "rules", which as highlighted earlier, pertains to the privacy guidelines

governing use of IoT devices. **Table 5** links the components of Activity theory, to this study's conceptual model.

Table 5: *Linking AT components to this study's conceptual model*

AT triangle component	**Conceptual model link**
Tools	Devices and cost, Software updates.
Subject	IoT Device end-user, personality, Habits, User IT education background, tech savviness. User attitudes.
Rules	Terms and conditions, Government legislation, Privacy policies, Terms of Service, Terms of use.
Community	Other IoT device users, third-party service providers, Government legislators, Technology Corporate companies.
Division of labour	What a user does to be adherent, what device manufactures do to ensure adherence, what the government is doing to ensure privacy.
Object	This is the motive; it involves the penultimate outcome of what a user intends to achieve by using a given IoT device.

3.4 Summary of chapter

This Chapter has introduced the theoretical and conceptual frameworks that underpin this study. The conceptual framework is informed by the literature and the main study's theoretical framework. The following Chapter details the research design and methodology through which a detailed account of how the research will be carried. The Chapter states the philosophical guiding principles relating to this study.

4. Research design and methodology

4.1 Introduction

This Chapter details the approach for this qualitative research. Saunders et al. (2009) argue that in a research design, a researcher must describe the where, how and the who regarding the intended research. The focus of all qualitative studies should be on understanding phenomena under exploration rather than exclusively on the participants, reader, or researcher (Creswell & Poth, 2016). Creswell and Poth (2016) further elaborate on the impact to the qualitative study of researchers imposing their own perspective, paradigms, and beliefs. Furthermore, arguably the main advantage in employing interpretive research for a study is that it is well suited for exploring hidden attestations behind complex social phenomena. Therefore, the research approach of this study was interpretivist in nature with the aim of understanding the world as it is at a level of a subjective IoT device user.

4.2 Research philosophy

With the motive of generally understanding alternative viewpoints, it is essential for a researcher to be cognisant of the assumptions upon which their own perspectives are based (Burrell & Morgan, 2017). Saunders et al. (2009) highlight that the philosophical considerations of research relate to the view of the relationship between the nature and the process of developing knowledge. The purpose of considering a philosophy of research is to reiterate and understand the researcher's choices considered for a philosophical research position (Carson et al., 2011). This research position has an impact on how and why the research is being carried out including impact on the gathering of reliable data.

Furthermore, Burrell and Morgan (2017) argue that there is a convenience in the conceptualisation of a study's assumptions. Creswell and Poth (2016) identify five philosophical assumptions that determine a qualitive research approach for an individual and these are: - ontology (nature of reality), epistemology (how a researcher knows that reality), axiology (values in research), rhetorical (language of research) and methodological. Carson et al. (2011) identify ontology to be reality where it is possible to get knowledge about a reality, epistemology is the connection of a researcher to the reality and methodology being the techniques to discover the referenced reality.

For this study the ontological, epistemological and methodology considerations are posited in sub-sections 4.2.1, 4.2.2 and 4.2.3.

4.2.1 Ontological considerations

Creswell and Poth (2016) classify ontology to deal with the nature of reality which is viewed subjectively by multiple participants in a study. Saunders et al. (2009) consider ontology to be concerned with the nature of social phenomena as entities. The Table 6 briefly summarises some of the aspects of ontology.

Table 6: *Summary of ontological aspects from Saunders et al. (2009, p110).*

Objectivism	Alludes to social entities existing with a purpose, independently from social actors responsible for their existence.
Subjectivism	Social phenomena are a consequence of perceptions and followed actions of social actors responsible for their existence.

This study followed subjectivism as an ontological stance since adherence is an action that is believed to be subjective. Objectivism is not adopted for this qualitative study due to the nature of IoT and the users. Objectivism posits that social entities exist independent of the respective social actors. The phenomenon of IoT adherence does not exist independently from users, and this is backed up by the different themes highlighted in this study's literature review summary in Chapter one. In addition, the objectivist position is contrary to the subjectivist position in the sense that, the truth is only but a matter of credibility (Saunders et al., 2009; Slevitch, 2011). Therefore, objectivism would not have been a good fit for this qualitative study.

Slevitch (2011) draws my attention to the fact that the choice of ontological stance has an impact on the epistemological and method choices. She highlights the fact that the "Qualitative methodology does not pursue objectivity and generalisability, because both conditions are viewed as unachievable from ontological and epistemological perspectives." (p.78).

4.2.2 Epistemological Considerations

Epistemology is a branch of philosophy that is concerned with "the researcher's view regarding what constitutes acceptable knowledge" (Saunders et al., 2009, p. 119). Burrell and Morgan (2017) provide an explanation of epistemological considerations being what forms knowledge, ideas, and assumptions that a researcher can deem to be true or false. **Table *7*** lays out the summary of the epistemological considerations.

Table 7: *Summary of epistemological interpretivism from Saunders et al. (2019.p114-116).*

Interpretivism	Essential for a researcher to adopt an empathetic stance, to understand differences between humans in our role as social actors and to be a part of the social world of the research subjects to understand the world from their point of view.

For this study, a belief is held that adherence to privacy is subjective and there was assurance that quality data was collected to justify this claim. For this reason, interpretivism is adopted with an in-depth analysis of current understanding of the IoT device privacy adherence phenomenon. The generation of knowledge is a human activity (Zachariadis et al., 2013). It is very essential to understand the differences between humans as social actors in IoT privacy adherence. Saunders et al. (2009) highlight the need for a researcher to focus on the details of a situation to obtain the subjective meanings.

4.2.3 Methodology

Saunders et al. (2009) identify the methodology as a reference to how a study should be done. Burrell and Morgan (2017) draw attention to the philosophical assumptions bearing implications on the ways in which a researcher obtains and investigates knowledge.

Table *8* summarises the methodology section.

Table 8: *Research dimension summary*

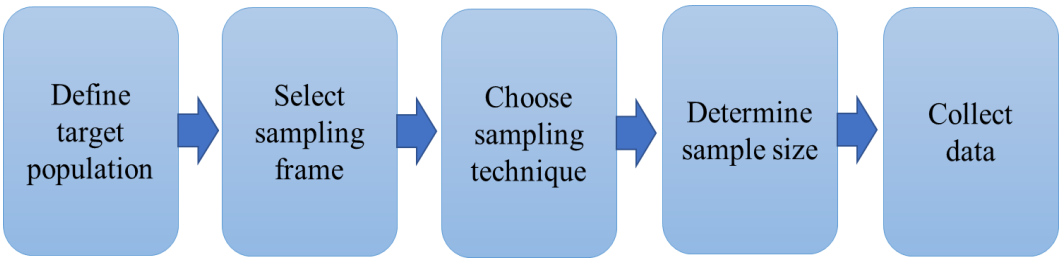
Design Element	Aspect	Justification	References
Research Methodology	Qualitative	This research is intended at understanding the factors influencing users and their privacy behaviours in the use of IoT devices, using qualitative methods.	(Creswell & Poth, 2016; Saunders et al., 2009)
Research approach	Exploratory	Research questions have been derived from the theory.	(Saunders et al., 2009)
Research Philosophy perspective	Interpretivist	There is human interest in the study and an attempt to understand what meaning people assign to privacy.	(Creswell & Poth, 2016; Myers, 2019; Saunders et al., 2009; Walsham, 2006)
Research Philosophy	Ontology	This study follows subjectivism as an ontological stance since adherence is subjective.	
	Epistemology	This study adopts interpretivism.	
Research timeframe	Cross-sectional	Due to time constraints of a 2-year master's study course requirement.	(Saunders et al., 2009)
Research Tool	Semi-structured interviews	Due to the Covid-19 pandemic restrictions from government and chosen paradigm.	

Design Element	Aspect	Justification	References
Data analysis	Thematic analysis. Microsoft Teams	Nvivo tool has the features to extract recurring themes. Microsoft Teams offers multiple options for carrying out interviews and offering transaction tools for analysis later.	
Data collection	Sampling. Pilot	It is time consuming to collect data from the entire population given the Masters' course time constraints as illustrated in the timeline Section 4.8	(Taherdoost, 2016; Walsham, 2006)
Data management	Password protected files stored on the university repository	Data storage should be in line with the ethical considerations of confidentiality.	

4.3 Sampling

The unit of analysis is users with internet connected devices. The non-probability-based judgement sampling technique was used for this study. Taherdoost (2016) highlights those inferences or generalisations can be made about a population by sampling which is not time consuming, but very subjective. Saunders et al. (2009) states that it is not feasible to study entire populations, therefore sampling methods are used. **Figure *7*** illustrates the sampling design criteria adopted.

Figure 7: *Sampling Process, Adapted from (Taherdoost, 2016, p. 19)*



4.3.1 Research participants

Table *9* lists the rationale for the research participants who were required to consent and be over the age of 18 years so as to participate in the study. The reason for the age restriction is since age 18 is considered the legal age of consent in South Africa and respondents can therefore comprehend privacy policy wording that is usually attached to device documentation. The participants are required to own and use atleast one internet connected device.

Table 9: *Design criteria for this study*

Unit of Analysis /Target Population	Smart Tv Owners, individuals with CCTV installations General IT savvy users, owns a laptop, smartphone
Study Parameters	Smart TV internet controls, Frequency of use of online provisions, Level of Home IoT Usage e.g., home automation, Smartphone, and fitness tracker data usage, fitness monitoring.
Sampling frame	Interview links sent out to respondents over the age of 18 years. Respondents required to have internet connected devices.
Estimated cost	All costs regarding research were covered by the researcher.
Estimated Time	2-8 Months
Sampling Technique	Non-probability based - Judgement sampling

4.4 Data collection, analysis, interpretation, and validation

Data collection and analysis is an iterative process that can be initially guided by theory (Walsham, 2006). Saunders et al. (2009) elaborate on the need of conducting semi-structured interviews to avoid any forms of bias for instance there is an emphasis on appearance of the interviewer to the interviewee affecting credibility. Therefore, due to the current government regulations regarding social distancing to stop the spread of the Covid-19 coronavirus (Pieterse, 2020), remote interviews were virtually held via Microsoft Teams in line with the regulations. A consent letter was provided to the participants, through which participants were informed of necessary recording of information and sessions no more than fifteen minutes in duration.

4.4.1 Thematic analysis

The collected data from initial pilot study and final interviews was analysed and interpreted in the context of the study using deductive approaches and Nvivo Software for two-stage coding and thematic analysis.

4.4.2 Validation

Various methods are used for data validation in qualitative research. These methods include member-checks where respondents review comments and further reliance on the reader to gauge validity (Soiferman, 2010). Saunders et al. (2019) highlights validity to be concerned with whether the results obtained are related to the study objective. Follow up questions were drafted as part of validating initial responses from pilot respondents.

4.5 Resources required

For this research, online content, electronic journals, and library material relevant to the study were utilised. Time is a very important element in interviewing participants therefore, interviews were scheduled appropriately. A good and stable internet connection was a necessity to be able to get responses to the pilot study survey and subsequent interview questions. In addition, participants were required to have access to Microsoft Teams software as the preferred medium of conducting the interviews due to its recording and transcribing capabilities.

4.6 Ethics and confidentiality

Ethics in computer related studies is the perception of something being good or right, and socially appropriate (Stahl et al., 2016). In developing good research questions, a researcher "requires understanding that inquiries into other people's lives are always an exercise in ethics" (Agee, 2009, p. 440). This research involves ethically collecting data from users of internet connected devices with sensors including fitness trackers. Therefore, ethical approval from the Commerce Faculty Ethics Committee was obtained and is attached to Appendix A of this document.

The collected data was anonymised and stored in line with the University of Cape Town's Research data management policy (University of Cape Town, 2018). The data is stored in a password protected location for the duration of the research, to uphold the ethical and moral principles expected of privacy research studies. No participants are identifiable with the collected data.

4.7 Instrument design

In line with the interpretivist epistemological stance, semi-structured interview guide was developed using the conceptual model described in section 3.3. A pilot survey was sent out to respondents and the instrument in Appendix C was finalised. With these semi structured interviews, Interviewees were probed to explain and clarify their pilot responses, for those that were involved in the pilot and new respondents to the finalised instrument. This was done as a follow-up with aim of understanding and validating the meanings they attach to the phenomenon. The Appendix section of this document contains the pilot study sample questions and finalised interview guide. A pilot study of 26 participants was conducted to finalise this instrument, to ascertain possible duration of interviews, preferred medium of interviews and general comments.

4.7.1 Identified literature themes linked to research instrument.

Table *10* speaks to the identified theme linkage to the study research instrument, which is developed in Chapter four.

Table 10*: Summarised themes from literature reviewed with link to instrument.*

Theme	References	Sub themes	Pilot Question link
Accountability, standards, laws, and regulations awareness.	(Ball, 2017; Brous et al., 2020; Foltz & Foltz, 2020; Independent Communications Authority of South Africa, 2020, 2021; ISO/IEC, 2015; Job, 2020; Kandeh et al., 2018; Pepper & Botes, 2020; Shayegh et al., 2019; Singh et al., 2018; South-African Government, 2013; Subahi & Theodorakopoulos, 2018; Viljoen et al., 2020).	Accountability, Risk, Tech savviness.	Section 3 - PQ2, PQ5, PQ6, PQ10 Section 4 - PQ1, PQ2, PQ5, PQ6, PQ8 and PQ10
Behavioural attitudes and Patterns.	(Anjomshoa et al., 2017; Atzori et al., 2017; Cho et al., 2020; Fu & Wu, 2018; He, 2019; Kokolakis, 2017; Tawalbeh et al., 2020).	Attitudes towards privacy.	Section 3 - PQ1, PQ5 and PQ8 Section 4 - Q1, PQ3 and PQ4
Safety and security	(Dlodlo et al., 2015; H. Lin & Bergmann, 2016; Ndubuaku & Okereafor, 2015).	Physical Safety Perceived security.	Section 3 - PQ8, PQ11 Section 4 - PQ3 and PQ7
Fitness, contact tracing and sleep monitoring.	(Haghayegh et al., 2019; Kahn, 2020; Kelly et al., 2020; Swaroop et al., 2019).	Quality of life like sleep monitoring.	Section 4 - PQ9 Section 3 - PQ3
Access to Technology platforms.	(Bailey, 2015; Cousin et al., 2018; Hejazi et al., 2018; Kolias et al., 2017; Ndubuaku & Okereafor, 2015).	Number of devices owned, Platforms of devices, Pervasiveness (availability of IoT devices), Network access connection speed.	Section 3 - PQ3 and PQ9 Section 4 -PQ4 and PQ8
Cost efficiency	(Asiimwe, 2019; Dlamini, 2017; Fernandes et al., 2016; Karanasios & Allen, 2018; Shuhaiber et al., 2019).	Open-Source Solutions/Proprietary solutions. Smart-home implementations. Maintenance costs like software updates and new versions.	Section 3 - PQ4
Community	(Birhane, 2020).	Consent to being monitored in community	PQ4

4.8 Research timeline

This study was cross sectional in nature and Table 11 reflects this study's timeline.

Table 11*: Research Timeline*

Activity	Start date	Projected completion
Draft Proposal	04 February 2020	28 February 2020
High Level Proposal	28 February 2020	20 May 2020
Literature Review	28 February 2020	17 July 2020
Research Objective Review	17 July 2020	20 August 2020
Research Design	21 August 2020	30 October 2020
Research Ethics Application Form	2 November 2020	30 November 2020
Data Collection Pilot	29 November 2020	4 April 2021
Data collection and analysis	5 January 2021	31 January 2021
Interviews and transcription	28 June 2021	30 July 2021
Findings analysis and conclusion	01 August 2021	30 October 2021
Grammar editing	01 November 2021	15 January 2022
1st Draft to Supervisor	15 January 2022	01 February 2022
Review and corrections from Supervisor	01 February 2022	10 February 2022
Final Dissertation submission	08 February 2022	

4.9 Summary of chapter

In this Chapter, rationalisation for this study following a subjectivism ontological stance in concurrence with an interpretivism epistemological consideration was discussed. The qualitative methodology followed, and the data collection methods utilised for this study were detailed. The next Chapter focuses on the analysis of the collected data.

5. Data analysis

The previous Chapter illustrated the research design and methodology followed by this study. This Chapter aims to analyse the data collected as laid out in the research design and methodology Chapter. Analysis is the second step of the three-phase approach of application of Activity Theory according to the Iyamu and Shaanika (2019) three-phase approach. The analysis is discussed using the lens of AT in conjunction with the conceptual model. The Chapter is laid out as highlighted in Table 12.

Table 12: *Research analysis chapter layout*

Section	Title
5.1	Introduction to analysis
5.2	Tools
5.3	Subject
5.4	Rules
5.5	Community
5.6	Division of labour
5.7	Object
5.8	Summary to analysis

5.1 Introduction

A pilot study is essential in fine-tuning the interview questions and procedures (Creswell & Poth, 2016). For this research, a pilot survey was disseminated to random participants and received a total of twenty-six responses. Coding of these responses began with five primary codes, awareness, devices, security, cost, and habits. Two levels of coding were applied using Nvivo qualitative analysis software. Subsequent thematic analysis showed additional themes that formed part of the data.

The qualitative data was collected from semi structured interviews conducted virtually via Microsoft Teams. The pilot analysis culminated in the revised instrument in Appendix D, whose responses were analysed. Thematic analysis done resulted in additional themes not catered for in the original conceptual model but contributed to a revised conceptual model.

5.1.1 Demographic profile of respondents

Appendix E represents the characteristics of the respondents to this study. From a total of 31 respondents, 17 are female and 14 are male. All participants were required to be above 18 years of age. The respondents belong to a variety of professions including medicine, marketing, investments, human resources, and information technology. From a qualifications

point of view, two respondents reported having a matric certificate as their highest qualification. One respondent reported a certificate qualification. Seven respondents were undergraduates pursuing their first qualification, one respondent has a diploma, and five have bachelors' degrees. 11 respondents hold honours degrees as the highest qualification. Three respondents hold masters' degrees, and one respondent has a Master of Business Administration (MBA) qualification.

5.2 Tools

The tools represent the artefacts used by the subjects to assist in achieving the objective. Some of the IoT devices listed by the participants included laptops, smart phones, smart fridges, smart TVs, car tracking units, community policing Closed-Circuit TV (CCTV), smart fitness trackers, Wi-Fi Routers, and tablets. This analysis illustrates how tools and associated factors influence user adherence. According to the analysis, tools are comprised of device settings, related services, and costs. These concepts as discussed below.

5.2.1 Device settings influencing adherence

The device settings are the basic configuration of a user's IoT device(s) that influence them to be adherent or otherwise. When asked if they were aware of any issues in relation to their devices, some participants admitted to knowledge of some of the issues on their devices and had several mitigating ways of dealing with them. Table 13 highlights the mitigations which are majorly software and device settings best practices.

Table 13: *Device issues and mitigation*

Issue	Mitigation
Unnecessary permissions.	Turning on airplane mode, deny permission requests. Two Factor Authentication (2FA) for the online accounts, fingerprint scanners, and to some, physical restraints for movable devices including laptops in the form of laptop cables.
Accessibility and ease of use.	Downloading additional software for facilitating easier device operation.

Some participants exhibited the knowledge of various physical and software measures they can use to be adherent to IoT device privacy standards, for instance, Respondent_6 stated that his company appeared to always track him and that the personal assistant, on his device, Siri "is always listening". He appears to understand how to limit these settings physically by

turning on airplane mode on his device. This finding is consistent with the literature by H. Lin and Bergmann (2016) through which they recommend automatic configuration for updates.

5.2.1.1 Unnecessary permissions

Respondent_4 highlighted an issue regarding the device settings whereby more and more of these associated IoT device applications request for permissions to sensors and features deemed unnecessary. For instance, she described how an attempt to upload a photo, led to a prompt for the app to access her contacts. She inadvertently decided not to adhere by denying all requests, whether the device settings requests are for her benefit or not.

> *For example, yesterday, I wanted to send a picture via Instagram, and before I could send it, ... "Do you want Instagram to access your photos, your contacts?" and I just clicked deny, deny, deny. Some of these apps, when you click deny, you cannot use them anymore (Respondent_4)*

The comment asserts the findings by Fernandes et al. (2016) whereby different implementations for IoT incorporate design flaws that exposed features with more permissions than necessary.

5.2.1.2 Ease of use/accessibility

The ease of use associated to IoT devices combined with the user attitudes of not tampering with the default device settings leaves the users non-adherent to recommended IoT device privacy settings. For example, Respondent_3 and Respondent_7 concur that settings are not as easy as plug and play, as advertised by the manufacturers

Opinions varied when it comes to a causal link between privacy standards adherence and ease of access of these settings for some users who are not technologically inclined. Respondent_7 made a case for her grandmother not being able to access these settings on some of her internet connected devices due to the nature of complexity in locating them. Issues arise when the elderly in this instance are not able to adhere to privacy standards and a henceforth an easy target for privacy related breaches.

> *I do not think it is easy to get to those settings, I think uhm, I think about people like my grandmother, would never ever be able to find them, they are usually decoupled from the apps, they are usually somewhere else like in your device's settings, you can go and find app settings, you can go and see for every app what is allowed, it is not simple, yeah! (Respondent_7)*

For Respondent_5, there seemed to be issues that arose from her device ownership in terms of answering Q10. She said, “I was promised that it is a plug and play! You know. I am saying that I was promised that the router would be a plug and play, now I am having to download software”. This finding shows that the non tech savvy participants find the interfaces hard to use and not as easy to update as advertised leaving them with outdated devices and therefore non-adherent.

5.2.2 Related Services

These are mutually exclusive services rendered in conjunction with the IoT device to function in the activity system. Concerns of third-party actors in IoT device usage ecosystem remarkably struck a chord with most participants, for instance, Respondent_9 appeared to disclose that there were no alternatives from a device perspective, leaving third parties as the only option. She said, “Well, no, but I think with some of the cases, it is not like you have much of a choice, it is, sort of like a by-product of using the device!”. Table 14 highlights the issues and mitigation.

Table 14: *Related service issues and mitigation*

Issue	Mitigation
Third-party Applications	Installing authorised or recommended applications only.
Limited choices	Abandoning use of applications due to lack of alternatives and miss out on enjoying Device in question.

5.2.2.1 Limited choices

However, one of the most remarkable aspect, Respondent_10, Respondent_9, and Respondent_5 admitted to only being compelled to adhere to privacy standards because it was the only choice, any other option would mean losing out on enjoying the benefits of the services. For instance, Respondent_5 commented about giving location permissions to devices in her possession being inevitable if she wanted to enjoy the benefits of applications requiring the GPS sensor on her device.

> *Most of the time, you not accepting it, means that you get to miss out on a feature, or some kind of improvement you know. You would go onto an App like Uber, and it might just be a trivial example, right, you would go onto an App like Uber, and then you want to order food to be delivered to your house, so it would not make sense for me to not share my location (Respondent_5)*

Additionally, sometimes participants found themselves forced to use third-party services yet again due to employer requirements leading them to subscribe to privacy as defined by their employers. For instance, Respondent_10 required a third-party application to be able to access company resources, otherwise she admitted there was no other way if she wanted to work remotely.

> *Well, I think in some instances, we do not have a choice! Because it asks you to set it up. If I have to think about, our work, uhm, in order for us to setup Teams on our phones, first you have to accept that the [employer] becomes, you know, sort of an administrator on your phone, Uhm you and of giving away rights there and then it also asks you to setup a third-party administrator, and if you do not do it, you cannot have Teams (Respondent_10)*

5.2.3 Costs factor

The multi-faceted costs of using IoT devices incurred by the owners pose a substantial threat to adherence. These costs consist of penalties, connectivity, and web-based costs. Table 15 highlights the issues and mitigation that include software best practices like clearing browser cookies, due diligence on mandated application permissions on devices and consuming cheaper internet packages to curb connectivity costs.

Table 15: *Cost factor issues and mitigation*

Issue	Mitigation
Penalties	Turning on airplane mode, deny permission requests
Connectivity	Downloading additional software for ease and having added Sim Card for internet access purposes. Finding cheaper data/internet packages
Web-based costs	Clearing cookies

5.2.3.1 Penalties

Respondent_1 alluded to the fact that a negative incident witnessed from the community might nudge them into reading the terms and conditions more often. He inferred that the penalties of an economic nature incurred by another member known to him would be motivation enough to start reading policy documentation.

> *Until someone experiences like a very, very bad thing then you know, or the moment there is any negative economic effect or any undesirable negative*

effect, even though it's not economic but any negative effect which most of the time is economical then I will start reading (Respondent_1)

An inference can therefore be asserted that the level of penalties attached to non-adherence is a determining factor to IoT device privacy standards adherence.

5.2.3.2 Connectivity activity costs

With respect to Interview question 10 seeking to understand the frequency of which IoT device users update the underlying software of their devices, it is found that some users only preferred to update only via Wi-Fi as opposed to mobile data. As mentioned in the literature review in Section 2.6, the analysis of this study is consistent with the Hawthorne (2018) study that the increasing connectivity costs associated to IoT device influenced the non-adherence to privacy standards as often, users shun updating their devices due to the high cost of downloading updates. For instance, Respondent_4 argues for the case of only using Wi-Fi because "data would run out, and I would end up buying more data. I do not want to do that".

Data is costly, I will use public Wi-Fi like at a place I trust, so like those flexible workspaces, I am comfortable to use it there, and there it would be my preference to rather use their data than my own (Respondent_7)

Respondent_7 indicated the preference to public Wi-Fi compared to her own mobile data which is corroborated by literature Section 2.2 in which the South African Competition commission report finds that prices high and not affordable by the poorer populace.

In addition, the preference of public Wi-Fi leaves these users open to malware and man-in-the-middle attacks therefore deeming the user non-adherent to privacy standards. This is the view shared by Respondent_3. "Uhm its free Wi-Fi that I do not trust normally, so with my own router, I can feel a bit more secure, but then, but you cannot be 100% secure, so I avoid using free Wi-Fi and stuff" (Respondent_3).

5.2.3.3 Web based costs

Respondent_1 and Respondent_10 said they did not mind if their privacy is breached if benefit in terms of reduced prices because of targeted advertising. The goods or content they would have searched for using IoT devices, seemed to be digitally tracked. For instance, Respondent_1 commented about liking his experience with recommendations from his music service subscription and a popular online shopping outlet, which offered him items at

discounted prices though he is also aware of the negative effect should his personal information be misused.

> *If I am playing music with Apple music then suddenly they are recommending music that other people are listening to who listen to music I listen to, I don't mind, suddenly like Black Friday is around the corner and I am getting a recommendation from Takealot about my personal information like something I was googling from a while back and it's a good offer, a good recommendation, I don't mind, its giving me a gain, as much as its invasion of my privacy, but like I wouldn't have found it, because I wasn't even looking you know, so, yeah, like I can be very complacent if there is like a positive effect but if there is a negative effect then it will be very undesirable (Respondent_1)*

In a similar finding, Respondent_10 did not mind the aspect of social engineering as She stated when browsing for a particular brand of handbags, she considered expensive, only for the related advertisements to appear on her husband's social media page. She explained:

> *I was just talking to my husband about it, and suddenly, that on his Facebook, He had Michael Kors coming up! And we were trying to figure out how is that possible because he surely does not follow Michael Kors in any shape or form. But We literally just spoke about it and the next time he picked up his phone, he had the sale of those bags coming up (Respondent_10)*

She went on to concede that "typically, with the ads, I find it makes my life better, I do not really mind it, I do end up spending a bit more". Her view is consistent with literature article by Kokolakis (2017) through which it was concluded that individuals are ready to part with personal information in exchange for a reward.

5.3 Subject

The subject refers to the individual utilising an IoT device and their perception of factors that affect their adherence to privacy standards. Table 16 demonstrates some of the issues and corresponding mitigation.

Table 16: *Subject (User) issues and mitigation*

Issue	Mitigation
Awareness	Self-education
Understanding of Privacy	
Personality	Attitude change and adoption of privacy-centric habits
Trust	Use of recommended privacy-centric devices/services
Fear	Users to get more acquainted with and read IoT standards

The biggest mitigant is self-education, through which users of IoT devices increase awareness from their own free will. Changing of attitudes and habits can also be mitigating factors to the highlighted trust issue.

5.3.1 Awareness

Awareness can be termed as the perception of potential factors by a user, that could affect their privacy. The awareness theme speaks to the knowledge and awareness node of this study's conceptual model. Within this theme it can be disclosed that very many a user is not fully aware of their rights and responsibilities when it comes to IoT device privacy. If a user is not aware that adhering to privacy standards stipulated to them is for their own good and protection, it becomes pertinent that nonadherence to standards might be happening subconsciously. There was a sense of lack of awareness from some Participants when answering questions probing the awareness construct. First and foremost, Respondent_10 acknowledged the insufficient awareness and education about devices and supported services when answering Q6. Respondent_10 said:

> *But I think that just talks to the education and the awareness, about... uhm, you know, is there sufficient education and awareness? … I think that there is a lot of education and awareness about those… I do not want to sound ignorant, but I do not think we are taking the time to educate ourselves about it! (Respondent_10)*

On the same note, there is a distinct lack of knowledge regarding South Africa's new Protection of Personal Information Act (POPIA) with most users not aware of this regulation's repercussions and benefits afforded to them as citizens from a privacy point of view. However, the users who exhibited awareness of this legislation have a better chance of knowing how their data is processed and revocation steps in case it fell in the wrong hands. This theme has been identified as one of the most important in understanding adherence since most other factors determining adherence stem from the knowledge of their existence by users.

In terms of awareness of the POPIA legislation by the South African government, Respondent_2 indicated knowledge of it, but it was unclear to her. She said, "I have heard of it, but I do not exactly know what it is!" pointing to a specific need of raising awareness of the legislation and how it can based be used to adhere to privacy standards.

Respondent_4 displayed his awareness of the kind of information collected about her and She also demonstrates knowledge of how to limit the unconsented access to her information through settings:

> *When you read or see videos and they tell to always turn off your Bluetooth off, your location off, so I always make sure I turn them uhm I always turn them off, because the video I once saw, it is that they can actually track you if your location is on, they can track and they can even see what you are doing! (Respondent_4)*

Within this awareness theme, positive awareness was identified as a sub theme whereby many participants demonstrated knowledge of the legislation. For instance, some participants including Respondent_1, Respondent_3 and Respondent_5 acknowledged knowing the about the POPIA legislation that is pro information protection.

5.3.2 Subjects' understanding of privacy

To ensure understanding of the purpose of the study, and to gauge participants understanding of the meaning of privacy, participants were asked to give their definitions. Table 17 is an excerpt of these definitions and associated encompassing theme.

Table 17: *Participants' definitions of privacy*

Respondent	Definition quote	Recurring theme
Respondent_1	"My ability to control when I want some to see it versus when I do not want someone to see it"	Restricted access, secret
Respondent_2	"What you or what the internet space allows you, the information it allows you or them, to store on their end from everything you are researching and doing on the internet"	Internet, information
Respondent_3	"The ability to, sort of to do whatever I want, whenever I want and not to be observed or be monitored by anyone, not having my activities being tracked down"	Surveillance, freedom
Respondent_4	"I think keeping everything to myself, like password information even though nowadays we are using a lot of things, so you just want to keep it to yourself so that nobody accesses it"	Information, secret, Restricted access,

Respondent	Definition quote	Recurring theme
Respondent_5	"Privacy is the ability to be protected from people who could gain your personal information for malicious purposes"	Information
Respondent_6	"…it is having my data secure so that it is not shared with anyone without my consent or approval"	Data, restricted access, consent, secret
Respondent_7	"Right to have personal information, kept, uhm, private, [laugh] so in other words for other services or companies not to retain that information when I am interacting on the internet"	Internet, Information, Surveillance, restricted access
Respondent_8	"Privacy is being able to do my work on the internet, without worrying that someone is trying to follow up on what I am doing and trying to take advantage of my information and abuse it to their advantage"	Internet, information
Respondent_9	"What I do on my devices being restricted to my knowledge, yeah, and not any one being able to access information… and I think if someone wants to use that information, I should be notified of it"	Restricted access, information, consent, secret
Respondent_10	"Only me having access to that information, so not having that information openly shared with the government"	Information, Restricted access, secret

There were recurring themes in these privacy definitions and the standout elements were personal information and secrecy.

5.3.3 Personality

The theme on personality speaks to attitude and habits exhibited by participants. Table 18 highlights the issues and mitigation including change of mindset and positive habitual changes.

Table 18: *Personality issues and mitigation*

Issue	Mitigation
Attitudes	Change of mindsets or point of view in relation to privacy standards
Habits	Pay more attention to repetitive tasks that pose risk to privacy
Anxiety	Spend less time around IoT devices and reduction of screen time

5.3.3.1 Attitudes

Attitudes are a construct of how an individual perceives something. IoT device users interviewed demonstrated varying attitudes towards privacy, these attitudes are grouped as negative and positive attitudes.

5.3.3.1.1 Negative attitude

Respondent_10 retorted "Uhm you know, on a certain level, I am not that important for anyone, to want to take my data" when asked if she actively takes any steps to secure her data. However, Respondent_4 appeared to approach the same question with a varying attitude. She said, "I do not allow for my information to be shared because some require consent and others I do not know, I try to avoid them". She later reneged on this further into the interview regarding the reading the privacy policies of her devices, which turned out to be negative and consistent with most of the interview participants.

> *Yeah, it is too long, and sometimes, maybe I will start reading and then, I, like sometimes it is too much information and then sometimes it has things you do not understand, and you just leave it… then it becomes that thing of ahh, I am not the only one who is using it, so, and probably whatever happens it is not just me! (Respondent_4)*

Respondent_5 when questioned why she does not read privacy related documentation, she responded with "that is because the reason I do not read them already is because I think they are long, you know, tedious!".

Kokolakis (2017) however states that attitudes vary depending on personal information in question and if the user stands to gain. This is evident in the response from Respondent_7 in which she acknowledges comfort in devices having access to her fitness tracker geographical information since it in return facilitates her personal fitness goals with fitness metrics.

Furthermore, negative sentiments were voiced regarding the trust afforded to third parties involved in the users' ecosystems. Respondent_6, in response to Q5 said, "I use them, but I do not trust them. Those third parties are using my information also". These sentiments can be detrimental to the user if there is no trust especially if a third-party is responsible for critical operations on devices including sensors and communication modules in IoT devices.

5.3.3.1.2 Positive attitude

Some participants exhibited positive attitudes towards better privacy practices. These included Respondent_10, Respondent_5. Case in point was when Respondent_5 admitted that despite her paranoia, she skims through privacy policies.

> *I am very paranoid and think that maybe somebody is watching me read these things, so I open it and literally just browse like I run my eyes through it not even proper perusing where I could actually make sense of what is in there (Respondent_5)*

Other participants including Respondent_7 professed to being more diligent when reading documentation only when they were short and to the point. When asked if they would adhere to privacy related documentation, Respondent_7 responded in the affirmative.

5.3.3.2 Habits

Habits are the routine subconscious actions carried out by an individual. They are a subtheme forming part of the personality theme. Respondent_1 exhibited some practices that determined their adherence or non-adherence outcomes. On answering the question if they believed to be adherent to reading privacy policies, Respondent_1 retorted "No, no unless if they are enforced, if I remember, but otherwise I do not explicitly adhere" and added "Yeah, no I do not check those I just kind of trust the vendor implicitly" signifying a bad habit in not reading policy documentation meant to guide his interaction with IoT devices. It can therefore be assumed that the vendor is exonerated from breaches should they sell off the data to another entity if it is explicitly stated in the policies, to the detriment of the respondent's privacy.

Respondent_1, Respondent_2, Respondent_5, Respondent_6, Respondent_7 and Respondent_10 disclosed that they frequently clicked "accept" without reading through the documentation. This finding can be interpreted as a disappointing habit amongst most of the participants. However, when asked if they are willing to change this habit, affirmative responses were received. "Yeah, I would, I mean right now, in some cases I do not even bother, it depends on the, the reputation of the company" said Respondent_1.

5.3.3.2.1 Connectivity habits

Another sub theme within habits found is the preference of using Wi-Fi to connect IoT devices. Several reasons given included, convenience, the cost of purchasing mobile data bundles and variance in network speeds that affect some device functionality. For instance,

Respondent_8 said, “mostly I use my Wi-Fi when I am home, and I use my mobile when I am moving around.”

> *The cost implication is, I do not really like buying data, when I have Wi-Fi, but Wi-Fi is not mobile. So, Mobile data is almost a necessary evil because I have to travel and if I am travelling and then I need to be online to reach people, but if I hardly went out, I would not use mobile, I would prefer the Wi-Fi (Respondent_8)*

Respondent_6, who is software developer by profession, placed more emphasis on security being the reason for him to use Wi-Fi. He said, “I use Wi-Fi mostly, because I think my network is properly secured, I can setup a proper network.” This demonstrated that Respondent_6 got into a habit of ensuring that his network was fully secure for the sake of his privacy and devices.

5.3.3.2.2 Online habits

Respondent_6 alluded to the fact that his online behaviour is being tracked for advertising and marketing purposes on the back of the internet searches performed.

> *It is all about behaviour on the internet, so they are collecting, uhm, what do I normally visit the most, so they want to just market stuff based on my profile. Yeah, so I think they are just collecting the behaviour like of for when I search for games, I know all the apps will just show me games now. (Respondent_6)*

An additional aspect brought to light was activity tracking in the form of what music is preferred. Respondent_1 did not seem to mind the use of his music listening activity to recommend more of the type of music he listens to. He said, “If I am playing music with Apple music then suddenly, they are recommending music that other people are listening to who listen to music I listen to, I don’t mind” said Respondent_1.

5.3.3.3 Anxiety

This is the feeling of unease regarding use of IoT device. Participants exhibited anxiety in their responses. For instance, when responding to Q5 about third parties, Respondent_5 expressed anxiety when she said, “I have generally never thought of it, hearing you say that actually makes me a bit anxious”. Respondent_1’s anxiety was brought to light should his information be compromised, referring to identity theft as his biggest worry, due to the associated consequence of impersonation.

Yeah, I think anything like if its identity theft you know, where people can go and kind of like pretend to be me, then yeah that is a problem. If suddenly my accounts, uh someone is just transacting on my behalf, that would be a problem and if of course they expose like pictures or messages, I do not want out there, then that is a problem (Respondent_1)

The repercussions from stolen information incidents may suddenly influence him to be proactive about his privacy whilst using the IoT devices in his possession. Similarly, Respondent_10 also demonstrated anxiety when mentioning the 2021 July unrest in South Africa (Bhattacharya & Rach, 2021). Respondent_10 associated the increased volume of marketing calls she was receiving, to information that might have been stolen in the looting.

I am a lot more aware now when I get people phoning me, for Tekkie sales, and I think you know with the unrest that happened recently, I am not sure about you, but I got a lot of calls about insurance… you know, I did ask them, where did you get my details from and certain instances, they are buying it from companies who have your information (Respondent_10)

For Respondent_3, companies that can remotely take control and take information without consent, invoked anxious thoughts of Him not having any control on his device.

With regards to phones, I realised that the phones we do not really own, I saw when the emerging of this corona virus came through, I had already seen something like covid what-what app, so they have the ability to install stuff on my device without my consent! (Respondent_3)

Respondent_4 spoke of the frequency of change of privacy policy and other documentation. She disclosed issues regarding the policies that made her anxious, including the rate at which the responsible device manufacturer for instance, insert clauses in the documentation, fine print indemnifying them from informing her about changes to the documents, of which she already granted consent.

But then even if you have read everything, they might change whatever they may change about the privacy and you are not aware of and because you clicked agree from the beginning, you have agreed to even the changes that they make that you are not aware of (Respondent_4)

Finally, it appears that some IoT device features cause the owners to be apprehensive. “I think the issue that I am most uncomfortable with these devices is, some of these devices have the ability to record sound” (Respondent_7). This level of anxiety is further elaborated in Respondent_6’s responses about the personal assistant on their device “Yeah, there is such, it is never sleeping so Siri is always listening”. Open microphones especially through applications not granted consent influence adherence. This is because such applications may need access to the microphone to perform tasks on a given IoT device or network.

5.3.4 Trust

Trust is the individual quality of honesty, safety and reliability related feelings accorded to third parties. There is a considerable level of trust attributed to specific manufacturers since users frequently resolve to automatic update settings for their devices as opposed to manually updating them. For instance, when responding to Q10 about his IoT devices’ frequency of installation of updates on his devices, Respondent_1 exhibited values of trust when he said, “I do not check those I just kind of trust the vendor implicitly”.

However, this becomes problematic if the updates rolled out for these devices are laden with malware and the user unwittingly installs the updates on their devices. The blind trust for vendors as said by Respondent_1 is a huge risk factor in adherence should the updates not be scrutinised. This risk is heightened by Respondent_5, who when responding to Q6 said, “inserting some form of spyware without me knowing that I have actually given them permission online to be able access things like my camera and microphones” to justify the risk of not doing due diligence on changes to software.

> *Before I did not really like pay much attention to this stuff but now with the POPI Act, I just kind of feel like you know the Government kind of watching over anyone kind of wrongdoing kind of thing. So, I do not even have to, I will even pay less attention (Respondent_1)*

Respondent_1 showed his level of trust in the Government when questioned about legislation awareness. He said he trusted the government to oversee this legislation achieve its main objectives.

5.3.4.1 Distrust

Respondent_3 showed a lack of trust in public Wi-Fi provisions due to security considerations. This signifies that in that respect, Respondent_3 is security conscious and concluded that he takes his security seriously and therefore adherent.

> *Uhm its free Wi-Fi that I do not trust normally, so with my own router, I can feel a bit more secure, but then, but you cannot be 100% secure, so I avoid using free Wi-Fi and stuff (Respondent_3)*

When answering Q5, Respondent_8 demonstrated his anti-trust in third-party providers and services for reasons he attributed to not knowing how these entities turn a profit. This may imply that should a third-party be a critical component in aiding adherence, Respondent_8 would be influenced not to be adherent due to no trust in these third parties.

> *I usually try to put things like ad blockers and try to put anti-virus here and there, but I do not trust them, and I do not even trust the third-party authenticator, because how do I trust you, when I do not know what is in it for you? Especially most of the password protectors are free, and I am asking myself, Okay I will give you my password, but how do you make your money? because I do not know whether I will give you my information, but I do not know if you will sell it (Respondent_8)*

Respondent_6 displayed a mistrust of enforcement of the POPIA on the side of the multinational companies operating within the South African borders.

> *Uhm, the problem is that the data is stored in Silicon Valley somewhere, So I doubt they are going to abide to those laws extremely, but they might change some few rules, but not to the extent of our POPIA Legislation (Respondent_6)*

This would indirectly make them appear non-adherent to legislation since their data appears not to be protected, based on authority of the companies responsible for the processing of their information through IoT devices.

5.3.5 Fear

Fear is the emotion brought about by freight or worry towards a situation. Participants stated that the fear of reprisal drove them to be adherent to privacy standards. This is evident in Repsondent3's answer to Q3, where She laments about the fear of some device capabilities

being used as listening devices in the form of microphones. “I think the issue that I am most uncomfortable with these devices is, some of these devices have the ability to record sound”, said Respondent_3. Likewise, for Respondent_7, the fear of loss of information and discovery of location through open microphones on IoT devices.

> *I know they could have a vulnerability and that information can be breached and people can therefore learn where I live, Uhm So like I am aware of that, but my biggest insecurity, is the data that can be recorded by putting on a microphone! (Respondent_7)*

Alongside the theme of fear, paranoia manifests as the idea of being tracked for marketing, advertising and surveillance purposes, results in some individuals ramping up their privacy settings on IoT devices. Location requirements from some IoT devices including cellphones in most cases raised questions of necessity for some users since they are not sensitized as to the purpose of the collected location data.

5.3.5.1 Associated consequences

Some participants acknowledged consequences as a driving factor to adherence. When answering Q8 regarding reading of the “rules”, documents including privacy policies, Respondent_1 referred to only start reading these rules only to avoid being penalised by fine print in such documentation. When probed further, Respondent_1 did say that reading the documentation was dependent on the value he attached to devices. “Yeah, like the risk of experiencing the ramifications” said Respondent_1.

> *For normal day-to-day stuff I seldom read them, for my insurance, I will read the insurance but if it’s my car, I will have to read it, if I am buying a new phone, and Telkom or whomever is on contract, I might need to pay a little bit more attention because I don’t want to be caught out (Respondent_1)*

In addition, Respondent_1 vowed only to read the privacy related documentation if the consequences outweighed the benefits of reading.

> *Whether be it as by review whether be it as by previous history in penalty, the moment there is like a perceived probable penalty where I might lose out in one way or another that is meaningful then I will start reading (Respondent_1)*

For Respondent_4, the consequences of trusting a third-party with their data is a major

factor. For instance, Respondent_4 hinted at consequences of bad password practices for devices including loss of personal information especially banking information.

> *Because anybody can take my account and access it and do whatever they want to do like I could be hacked so, you know with this thing, with like, the problems that you would hear whatever banks were hacked and people's account and passwords, you know and their data is all over, I would not allow a third-party to have my password (Respondent_4)*

This is detrimental if the associated IoT device has a security feature controlled by a third-party for instance, login Application Programming Interfaces (APIs) plugins from social media providers.

5.4 Rules

For this study, rules consist of terms and conditions, legislation from the Government, privacy policies from device manufacturers. This theme analyses awareness of the "rules", as per AT, in this regard pointing to Government's legislative interventions amongst other acceptable device usage guidelines. Table 19 highlights the issues and mitigation.

Table 19*: Rules related issues and mitigation*

Issue	Mitigation
Legislation awareness	Training and more sensitisation regarding legislation and it's intended benefits.
Documentation	Reading summarised and clear documentation on privacy

5.4.1 Legislation awareness

In Q7, participants were asked if they were aware of any legislation meant to assist them with protection of their data from bad data processing tendencies by companies. With the signing of the Protection of Personal Information Act (POPIA) into law on 1st July 2020 of South Africa, a new dawn of legislation was ushered in. Participants were asked if they understood what this legislation meant in terms of their IoT privacy.

Noteworthy responses were found including a mistrust in Government's ability to enforce this legislation. Respondent_8 emphasised that "if the government can do more, then that would be good, I do not know if they have the capability to do more". Indicating a mistrust in the enforcement capabilities of the government contrary to the findings of a study by Job

(2020). However, Respondent_8's declarations are aligned with the findings of Viljoen et al. (2020) that criticises the failure in protection of constitutional rights of users.

Respondent_10 believed that despite a few gaping issues, the Government can still do a lot more to ensure proper data practices.

> *Yes, so I feel like there are still loopholes that need to be tied up before you can really say that your information is being utilised and only consented by you. I think it is the right way forward, but there is still a lot of work to be done (Respondent_10)*

Contrary to most participants, Respondent_2 appeared to have heard of the POPIA legislation but did not know exactly what it entailed. "I have heard of it, but I do not exactly know what it is" said Respondent_2. This finding is significant in that it demonstrates that there will be less adherence, if the populace does not know that they have legal recourse should their data be misused. This means there is a lack of thorough sensitisation on the part of the legislators.

> *I think it is a start, you know, and uhm I do find it to be a bit stringent, you know, But I really, really would like it to get to a point where I do not get any form of spam, you know (Respondent_5)*

However, Respondent_5 was optimistic about a time when she will no longer receive any form of spam and spoke of the legislation being stringent signifying a bit of knowledge on what the POPIA legislation is about.

5.4.2 Privacy policies, Terms and Conditions, privacy policies

Reference is made to Q8 in the Interview schedule in Appendix D, answers to which most of the participants seemed to complain about the length of this type of documentation through which a lot of important information is laced with technical jargon making it hard to comprehend. For instance, Respondent_2, a travel consultant said, "It should be much shorter, uhm there should not be a lot of technical jargon, because that definitely puts some of us off!". The same sentiments were echoed by Respondent_1 when he said, "yeah some of them have a lot of fine print, uhm, I do read some, but not for my devices". This subtheme coincides with the attitude theme in which users tend to shun reading information on their own.

5.4.2.1 Clarity

It was observed that some of the participants found the terms and conditions to be unclear. A possible explanation is the fact that the IoT device manufacturers or authors of the documentation in some instances reserve the right to change them at any time.

> *I think what is not clear for me, is that the privacy standards and regulations keep changing, and it is very difficult to keep up, and keep aware of what is it, what do I need to do, to ensure that, you know, my privacy settings and standards are enabled (Respondent_10)*

The other point of contention among some participants is the use of jargon too technical to the ordinary user.

> *I think there is still some grey areas and because it is legislation, you know I think for the most part it is always, the jargon is always technical in terms of it. It is language that I think for the most part lawyers tend to understand (Respondent_9)*

Some instances of non-adherence can be attributed to users unwittingly accepting policies that are lengthy, updated overnight or laced with complicated legal terms. “It is also written in jargon so even if you read the whole thing, you do not understand it” said Respondent_7. Other participants claimed the length of this documentation to be off-putting, “sometimes it is too much information and then sometimes it has things you do not understand, and you just leave it” claimed Respondent_4.

5.5 Community

As discussed in sub-section 3.3.4, the “community” themes arising from the analysis of this study identify how the “subject” interacts with the other components in the activity system. Table 20 highlights the issues and mitigation that includes understanding of device settings better and the differences between security monitoring and illegal activity tracking.

Table 20: *Community related issues and mitigation*

Issue	Mitigation
Surveillance and paranoia	Understand difference between security monitoring and illegal tracking of activity on IoT devices
Speculation	Make use of device settings
Community effect	Not to solely rely on what others do to be adherent, but to devise own reasons for adherence

5.5.1 Surveillance and paranoia

This is the User day-to-day monitoring by a third-party without their consent. Confirming the findings of Alsmirat et al. (2017), this surveillance theme in the community is a major talking point to which Respondent_3 in his definition of privacy alludes to when he mentions it to be "the ability to, sort of to do whatever I want, whenever I want and not to be observed or be monitored by anyone, not having my activities being tracked down". It is a poignant aspect of many users' internet experience with several government and private entities tracking their activity for security purposes. Furthermore, He put forward his observations about someone else having the ability to remotely enable features on his device without his consent for purposes of contact tracing with the emergence of the Covid-19 pandemic.

> *I saw when the emerging of this corona virus came through, I had already seen something like covid what-what app, so they have the ability to install stuff on my device without my consent! You understand, so I do not have uhm sort of a say on my devices, so that as well for me takes away my privacy, So I do not understand what they are doing (Respondent_3)*

In response to Q6, Respondent_3 further elaborated on location, age and shopping patterns being some of the datapoints collected about him "because they follow me around, ah yeah, In-fact at the top is my shopping patterns, they need to know who I am, how old I am, my gender". These suspicions link to the theme of paranoia as one of many factors influencing adherence. Respondent_4 voiced her concern regarding surveillance when she said, "I was also surprised that you know Google can see like what you are Googling stuff". Similarly, Respondent_5's sentiments towards reading terms and conditions because "I am very paranoid and think that maybe somebody is watching me read these things, so I open it and literally just browse like I run my eyes through it". The level of paranoia may be construed as a form of adherence due to suspicions that another member of the community is possibly monitoring.

The network of AI powered CCTV cameras around a few Gauteng suburbs dubbed "Vuma Cam" cited by a Birhane (2020) article, was discussed by Respondent_7 as something she did not consent to in her community when she said, "Yeah, it is an interesting thought what could happen! And those Vuma Cams, as well, it takes it to another level! Because where do you consent to that?". The sentiment s in agreement with the work of Dlodlo et al. (2015) as well in which CCTV is used as an IoT tool to bolster security in the community. The monitoring

influences behaviours of potential criminals who realise that IoT devices in operation and force them to adhere.

5.5.2 Community effect

The community effect subtheme explores the impact the community has on a user's decision to adhere. For instance, when asked if he would change his behaviour and adopt more reading of his device associated policies, Respondent_1 said he would only pay more attention to these documents only if he witnessed several other users penalised. "So, it is more statistical if I am buying something that I know historically people have kind of complained then that will get me a reading", said Respondent_1.

> *Yeah, it is just that, it is also quite statistical, like if I hear about people saying that so and so got caught up by an MTN contract and now they have to pay a penalty then I start reading more, if I hear so and so lost their car after paying it off, you know then I will start reading like eh what is going on? (Respondent_1)*

In addition, Respondent_1 also hinted at reliance on the community for his adherence when he mentioned that if the device got a bad review from the other users, he would not be keen on owning it or even be more careful in terms of reading the policies if it is already owned should there be potential incurrence of a penalty.

> *Whether be it as by review whether be it as by previous history in penalty, the moment there is like a perceived probable penalty where I might lose out in one way or another that is meaningful then I will start reading (Respondent_1)*

Community reviews were further cast into the limelight when Respondent_7 referred to a story of how a voice assistant (Alexa) enabled smart speaker device disclosed private conversations of its owner. This seemed to be a determinant factor that influences Respondent_7's awareness of privacy and adherence thereof.

> *I heard a story about I think it was Alexa, who recorded a man's like personal conversation with his wife or something, and it was leaked somewhere along the line, so I mean It would probably take a situation like that to be a little closer to home uhm, uhm for me to be a more aware (Respondent_7)*

Social media was highlighted by Respondent_4 as an influencing factor. The use of social media applications including TikTok, a short video service, through which Respondent_4 learnt from a social media video that one of the major big companies involved in IoT can track her internet searches. This finding is on par with Atzori et al. (2017) study through which they disclosed significant undertakings to exploit social platforms for IoT device integration.

> *I think when I was on TikTok, a while ago that is when I realised that there are somethings that I was not aware of that happen… I surprised that you know Google can see like what you are Googling and stuff (Respondent_4)*

5.5.3 Speculation

Speculation is the act of making a conclusion, without having enough information on the facts on hand. It can be concluded that some of the participants in the interviews attached heavy meaning to making unproven assertions, for instance, Respondent_8 speculated that big corporates are above the law and that they cannot be reined in for wrongdoing in respect of privacy.

> *I think, all information about us is collected, because things like Google, we never log out of our emails again, on our phones now, my email is always online on Google, and I know that Google does not care about privacy that much (Respondent_8)*

Repondent8 demonstrated speculative sentiments towards the services he consumes which may in turn lead to mistrust of these services leading to non-adherence.

5.6 Division of labour

Division of labour deals with who plays what role when IoT devices are involved within the IoT device ecosystem. Table 21 highlights the issues and mitigations including better governance and use of certified service providers.

Table 21: *Division of labour related issues and mitigation*

Issue	Mitigation
Government policy makers	Encourage policies that considerably cater for all groups in the population
Government policy enforcers	Better governance on how companies handle user data
Educators	Easy to read user manuals and user self-education
Service providers	Only use of certified/recommended service providers

5.6.1 Government policy makers

For some participants as part of their individual definition of privacy, associate policing to the government. Respondent_10 mentioned that she entrusted government to ensure the policing of information safeguards.

> *So, I think just uhm, having the information that is on there, uhm, only me having access to that information, so not having that information openly shared with the government, uhm any security aspects within country, like policing or whatever (Respondent_10)*

Her statement hinted at adherence on condition of proper policing by the government regarding access of her private information restricted. This finding is consistent with theme of trust whereby users have reservations on trusting another party with ensuring their privacy.

5.6.2 Government policy enforcers

Node addressing government policy enforcement themes as identified by participants. Some companies are viewed as enforcers of legislation according to some participants due to their reputation and this plays a part in adherence. Respondent_1 acknowledged the level of trust afforded to the big corporates when asked if they would be more attentive when to be more adherent. He said, "Yeah, I would, I mean right now**,** in some cases I do not even bother, it depends, the reputation of the company also helps". But there seems to be alternative views on this as stated by Respondent_8, the level of trust given to big corporates since they are the largest primary points of data collection, is a contention.

> *I think, all information about us is collected, because things like Google, we never log out of our emails again, on our phones now, my email is always online on Google, and I know that Google does not care about privacy that much (Respondent_8)*

Respondent_7 referred to the other stakeholders, the companies, in her definition of privacy in this activity system. These companies process the data collected via the IoT devices. She defined privacy as "the right to have personal information, kept, uhm, private, so in other words for other services or companies not to retain that information when I am interacting on the internet".

Additionally, Respondent_8 disagrees with the role corporates play in the enforcement of the "rules" in the form of legislation by Government, for instance the POPIA.

No, I do not think so, because I think that big corporates always abuse the regulations and then they go to court and take years, so by the time they finish a case in ten years from now for example if they are sued for POPIA, I would have made a lot of losses (Respondent_8)

When probed if He believed the legislation would assist in personal information collection limitation, He pointed out the tendency of lengthy litigation by these deep-pocketed protected companies to afford legal bills. This also forms part of the costs' theme.

5.6.3 Educators and sensitisers

This theme identifies stakeholders within this activity system that guide users on the best practices in the form of education about these devices. It is corroborated by the Chong et al. (2019) and Nelke and Winokur (2020) study that attempted to evaluate the benefits of introducing an IoT course in curricula for students to share experiences between the academics and the industry.

If you have to think about uhm, your phones and your apps that is on there, I think that there is a lot of education and awareness about those, but in terms of your devices connecting, uhm, I do not think there is that much education about it… I do not want to sound ignorant, but I do not think we are taking the time to educate ourselves about it! (Respondent_10)

Respondent_10 confirmed that IoT device users can be educators by sensitising other users.

5.6.3.1 User self-education

On the element of awareness regarding risky settings, for instance, unrestricted microphone access on devices compromising privacy, Respondent_10 remonstrated with fellow users who do not educate themselves in terms of getting the knowledge about their devices. This theme corresponds to the personality attribute of attitudes towards determining if they want to educate themselves more about the devices in their possession. This finding is consistent with the Tawalbeh et al. (2020) and Chong et al. (2019) study which found that most privacy breakdowns are consequences of lack of awareness on users' behalf.

I think that there is a lot of education and awareness about those, but in terms of your devices connecting, uhm, I do not think there is that much education about it. Or we are educating ourselves, I do not want to be ignorant, I do not

want to sound ignorant, but I do not think we are taking the time to educate ourselves about it! (Respondent_10)

Respondent_5 voiced similar sentiments regarding users educating themselves about their own privacy.

You know, so uhm, it is just about being that cautious, and also just understanding as a consumer, you know, uhm as a person that you know, you have got a right to privacy and just educating yourself about that (Respondent_5)

It is noteworthy that IoT device users can also play this role of educators through their experiences.

I think I would tell a person that be careful of what you pass through your email, if there is information really important that you do not want to be on the internet, please do not pass it through your email or your phone, or anything, find a different way of passing it on to the person you want to give it to. Because once it goes through an internet medium, then you have no control over who is going to see it (Respondent_8)

Respondent_8 advised of vigilance by users when using IoT devices and associated services especially laptops and related services whilst using the internet.

5.6.3.2 Easy to read user-manuals by device manufacturers

Device manufacturers are responsible for easy-to-read guides on how users can best make use of their IoT products. Respondent_2 argues about such documentation being laden with a lot of technical jargon and found it to be disconcerting.

There should not be pages and pages, paragraphs, and paragraphs of things to click on and most of the time that are repetitive, uhm they should use a lot more images some of us do not like to read (Respondent_2)

Respondent_2 prescribed for more user-friendly approaches to documentation including the use of more images and legible fonts. Subahi and Theodorakopoulos (2018) had a related finding whereby the IoT devices in question behaved inconsinstently to what was written in the privacy policies.

5.6.4 Service Providers, device manufactures and third-party companies

This sub-theme illustrates all the enablers of support services to IoT devices. Participants had mixed discourse in terms of entrusting middlemen with their data. Respondent_7 pointed out the role of these companies in the retention of user information.

> *Okay cool. So, I think it is, it is the right to have personal information, kept, uhm, yeah private, [laugh] so in other words for other services or companies not to retain that information when I am interacting on the internet (Respondent_7)*

Respondent_1 raised an important issue of reputation of the company handling his data, to the extent that if it is reputable enough, he will happily part with his information once requested.

> *I do not trust their ability to safeguard my credit card details, I will accept, but not capture my sensitive details and all of that. But if its Apple or Google, then I am most likely just to accept even if they are saying that they need my details (Respondent_1)*

However, if he deems a company not to be reputable enough, he does not feel comfortable leaving personal information in its hands, therefore influencing adherence to data processing and other privacy policies.

5.7 Object

The object is a consequence of a "user" interacting with all the other components in the Activity system. Or simply put by Kuutti (1996), the desired outcome. The analysis shows how users are motivated to achieve their intended or unintended goal of adherence or non-adherence. This is the penultimate node in the study's activity system.

When asked directly what he thought influenced his adherence, Respondent_3 said that "the world, our world, my data is a cheque book to someone else, so people/organisations go through even unspeakable means to spy on my habits, makes me want my privacy more" which profoundly underpins an influence of the value of his data as a currency. This points to "organisations" referred to by Respondent_3 having an objective of collecting his data for profit purposes. The work of Burtch et al. (2018) confirms this theme in totality regarding big corporates investing in IoT with an objective of profiting. Table 22 highlights the issues and mitigation including analysis whether there are benefits to be realised from adherence.

Table 22: *Objective related issues and mitigation*

Issue	Mitigation
Non-adherence	Logically weighing cons for or against compliance.
Perceived benefits	Users must confirm advantages before using IoT devices.

5.7.1 Non-adherence

There was evidence of no intentions of adherence by some participants through which they shunned their own privacy. For instance, in this theme Respondent_1 disclosed it outright that he does not understand the policies he said, "No because I did not read them", making him non-adherent. Similarly, Respondent_7 said, "most of the time I just "Accept", [Laugh]". Signifying a trend of participants not reading or understanding the policies meant to make them adherent. Respondent_10 followed the same trend and admitted to not changing the default settings on her devices.

5.7.2 Perceived benefits

Perceived benefits concern participants' apparent benefits in adherence/non-adherence. Some of the participants admitted to adherence due to the associated benefits they would enjoy.

> *Even on my laptop, sometimes they say hey, when you are using this app, or whatever, would you like to send anonymous reports about your usage, I say yes, I mean, if it is going to help you improve this free thing that I am getting then sure! (Respondent_1)*

Respondent_1 showed straight forward adherence by virtue of brand of device in their possession or resulting service they intend to enjoy. Respondent_1 said, "if its Apple or Google, then I am most likely just to accept even if they are saying that they need my details".

5.8 Summary of chapter

The analysis revealed the concepts coded from participants' responses which were laden with scepticism and others with willingness to be more adherent. The responses from the transcribed interviews, were coded using Nvivo, from which recurring themes were isolated. These themes were grouped into meaningful groupings in accordance with Activity Theory. This analysis is the second phase of a three-phase approach for using Activity Theory posited by Iyamu and Shaanika (2019). Selecting of Activity Theory as the study's theory was the first phase. For the next Chapter, associations between the concepts are mapped and outlier determinant factors that underpin user adherence to IoT privacy standards are disclosed leading to a revised conceptual model of this study.

6. Research findings

The third and final approach phase of the three-phase approach of Activity Theory is linking the analysis elements with the components of the theory. The purpose of this Chapter is to present the findings from the analysis done in the previous Chapter.

6.1 Introduction

This study has assessed the factors influencing adherence to IoT device privacy standards using Activity Theory. This assessment was done by using a survey and virtual interviews. The interviews conducted virtually had various participants, whose demographics are highlighted in Appendix E.

Overall, most participants are non-adherent, either through factors of their own making or external factors. These included behaviour, attitudes, habits of users, fear, trust in the devices and knowledge of legislation. It was also apparent that sensitisation of users on their privacy is paramount to drive better privacy practices according to some of the study participants.

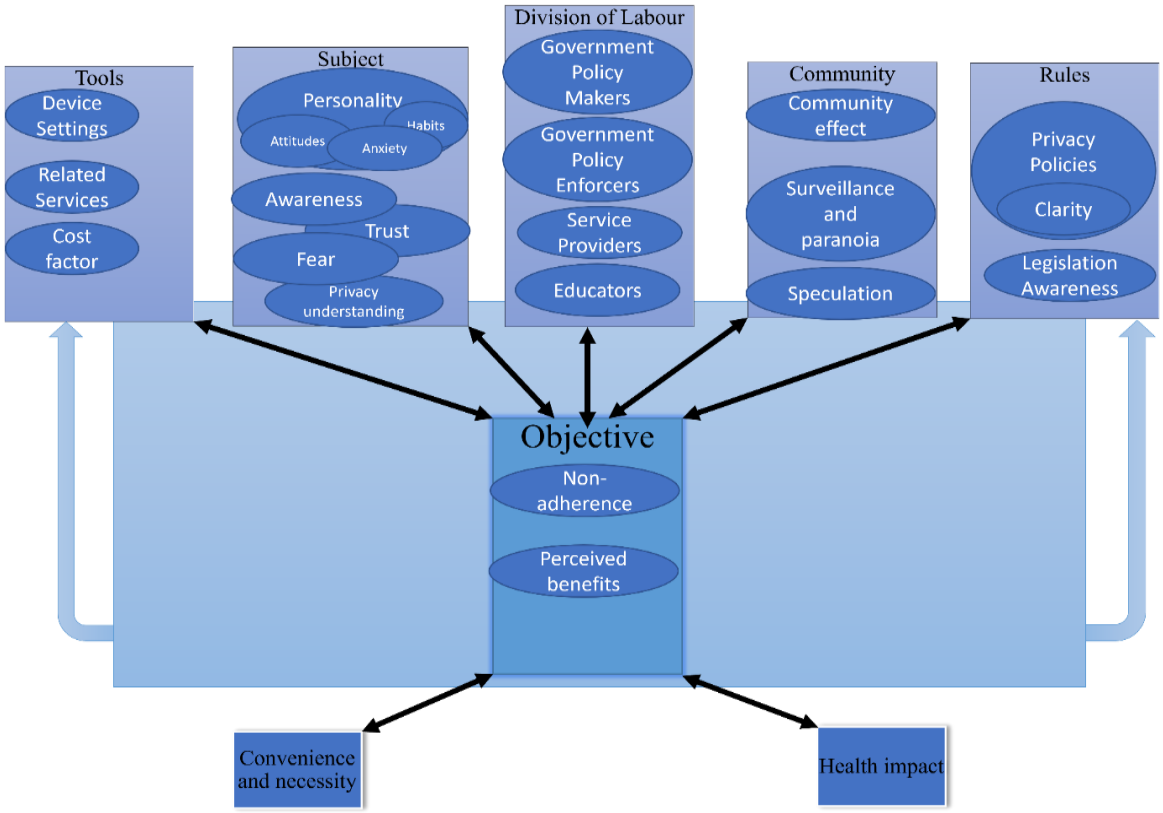
This Chapter presents the findings from the analysis done in the previous chapter. Additionally, this Chapter details a revised conceptual model, contradictions to theory, linking of themes and propositions.

6.2 Revised conceptual model and findings

The key findings were examined in accordance with the phenomenon under investigation guided by the third phase of using Activity Theory according to Iyamu and Shaanika (2019). Where applicable, existing literature has been sourced to concur with this study's findings.

In cases where no existing literature is matched, the findings have been explained with a theory. Based on the analysis in Chapter five, a revised conceptual model is presented below to include the outlier concepts highlighted in Section 6.3.

Figure 8*: Revised conceptual model*



The model in **Figure *8*** highlights the updated constituents of the model in **Figure 6**. The "tools" node discussed in sub-section 6.2.1 caters to additional factors including device settings and related services as contributing factors to adherence. The "rules" node is updated to reflect clarity and legislation awareness to aid in understanding of policies as detailed in sub-section 6.2.5. From a "subject" point of view, the personality is an overarching factor linked to privacy understanding, fear, and trust. The following sub-sections discuss the revised conceptual model.

6.2.1 Tools

In comparison to the originally proposed conceptual model, the revised model illustrates the component factors of device settings (Section 5.2.1), related services (Section 5.2.2) and cost factors (Section 5.2.3).

When these components are combined, they influence the objective of privacy adherence. Some IoT device settings and permissions are not user friendly and sometimes require additional tools or software or service to fully be usable to users who intend to be adherent to the recommended IoT device standards. These additional tools come at a cost to the user, further impeding adherence.

This finding in relation to devices settings is consistent with the research done in this area with the application of a Mobile Users Information Privacy Concern Model (MUIPC) to determine user alteration of privacy settings within the IoT Environment (Foltz & Foltz, 2021). Tables 23 and 24 highlight this section's propositions including device type influencing adherence decisions.

Table 23: *Proposition: Tools or devices and related services as influencing factors*

Proposition	Related Concept	Quote(s)
The type of device and associated third parties influence users' privacy adherence decisions during use of IoT devices.	Tools	"Ahh, I use them, but I do not trust them. Those third parties are using my information also" (Respondent_6). "Uhm, biggest concern, uhm, it is them sharing my data with third-party companies, I do not like that" (Respondent_6). "Because now, they are giving an open access to data that I do not want to be share" (Respondent_6).

Table 24: *Proposition: Device settings and related services as influencing factors*

Proposition	Related Concept	Quote
Incentivised IoT devices easily part with their personal data in exchange for rewards and freebies, leaving their privacy at risk.	Costs	"Typically, with the ads, I find it makes my life better, I do not really mind it, I do end up spending a bit more" (Respondent_10)
The level of penalties attached to non-adherence is a determining factor to IoT device privacy standards adherence.	Penalties	"The moment there is any negative economic effect or any undesirable negative effect, even though it's not economic but any negative effect which most of the time is economical then I will start reading" (Respondent_1)

The tools are responsible for several propositions that influence adherence to IoT device privacy standards. However, they work in tandem with other factors like costs and associated penalties to the use of the IoT devices.

6.2.2 Subject

The original model represented the subject bearing user attitudes and home monitoring as influencers to adherence. The revised model shows a multitude of factors which include the personality of a user, awareness, trust, fear and understanding of privacy as driving factors to

the objective of adherence. Tables 25, 26 and 27 highlight this section's propositions which are hinged around the IoT device user and their associated traits like paranoia and level of trust.

Table 25: *Proposition: User and device specific factors influence adherence*

Proposition	Related Concept	Quote
Users underestimate their position in the ecosystem of IoT device privacy. There is a user inferiority complex attitude towards their personal data.	Subject	"So, Uhm you know, on a certain level, I am not that important for anyone, to want to take my data" (Respondent_10)
Device Settings, ease of use influence adherence. Due to the multitude of manufacturers, there are various unstandardised ways of user interfaces that are not user friendly.		*No, I do not think it is easy to get to those settings, I think uhm, I think about people like my grandmother, would never ever be able to find them, they are usually decoupled from the app, they are usually somewhere else like in your device's settings, you can go and find app settings (Respondent_7)*

Table 26: *Proposition: Fear as an influencing factor*

Proposition	Related Concept	Quote
Personality determines level of trust, linking attitudes to trust whereby it takes a good impression by the device manufacturers to obtain the trust of a user.	Fear and paranoia	*But then even if you have read everything, they might change whatever they may change about the privacy and you are not aware of and because you clicked agree from the beginning, you have agreed to even the changes that they make that you are not aware of… then they make changes after because you have agreed from the beginning, it means you have agreed even to the new changes unaware of it! (Respondent_4)*

Table 27: *Proposition: Consequence for subject as an influencing factor*

Proposition	Related Concept	Quote
Associated consequences of non-adherence are a driving factor to IoT Privacy adherence.	Consequences	*For normal day-to-day stuff I seldom read them, for my insurance, I will read the insurance but if it's my car, I will have to read it, if I am buying a new phone, and Telkom or whomever is on contract, I might need to pay a little bit more attention because I don't want to be caught out (Respondent_1)*
Fear of retribution drives IoT Privacy standards adherence due to associated consequences.	Fear	On third parties - "Biggest concern, uhm, it is them sharing my data with third-party companies, I do not like that. Because now, they are giving an open access to data that I do not want to be shared" (Respondent_6)

In agreement with the findings of Kokolakis (2017), attitudes differ subject to sensitivity of information a user is willing to part with. Users need to be educated further on implications of non-adherence and the meaning of their privacy to increase awareness. Foltz and Foltz (2021) concur with this finding through which User attitudes towards privacy need to change further in favour of privacy. For this study's purpose, this is to facilitate better adherence.

6.2.3 Division of labour

In the original model, it was perceived that "Community" and "Division of labour" were tightly coupled but in the revised model, it is evident that the distinction of third parties like legislators, educators and policy enforcers form part of factors that influence adherence. Third-party stakeholders in the IoT device activity system are influencers of user decisions towards adherence or lack of there-of. Table 28 highlights this section's propositions which points to the involvement of stakeholders in influencing of IoT device adherence.

Table 28: *Proposition: Division of labour as an influencing factor*

Proposition	Related Concept	Quote
Proper government policing and enforcement determines the level of IoT privacy standards adherence.	Division of labor	*I think what is not clear for me, is that the privacy standards and regulations keep changing, and it is very difficult to keep up, and keep aware of what is it, what do I need to do, to ensure that, you know, my privacy settings and standards are enabled (Respondent_10)*
Legible privacy standards documentation can be a determinant of IoT privacy standards adherence.	Manufacturer literature legibility	"There should not be pages and pages, paragraphs, and paragraphs of things to click on and most of the time that are repetitive, uhm they should use a lot more images some of us do not like to read" (Respondent_2)

This subsection's finding is consistent with the Wickramasinghe and Reinhardt (2019) study which concluded with an emphasis on users being involved in privacy related solutions meant to enhance privacy.

6.2.4 Community

The community in the revised models shows the impact of speculation, paranoia surveillance on the IoT device user which has been revealed as an influencing factor to adherence. Hearsay from fellow users in the IoT activity system about IoT devices and adherence influences the decisions to adhere to standards. This finding can be linked to the

viral rumoured health risks of 5G technology highlighted by Respondent_1's remarks. Since there are elements of social media community and its influences on user IoT privacy adherence, it is appropriate to apply the Actor Network Theory (ANT). Table 29 highlights this section's proposition that speaks to how the community plays a role in IoT device privacy adherence.

Table 29: *Proposition: Community as an influencing factor*

Proposition	Related Concept	Quote
A User's surrounding community greatly influences their decision regarding adherence to IoT Privacy standards.	Community	*Until someone experiences like a very, very bad thing then you know, or the moment there any negative economic effect or any undesirable negative effect, even though it's not economic but any negative effect which most of the time is economical then I will start reading (Respondent_1)*

6.2.5 Rules

The former conceptual model only demonstrates the impact of standards' awareness in comparison to the latter model that additionally speaks to legislation awareness and clarity of the policies as factors influencing adherence. **Table 30** highlights this section's proposition.

Table 30: *Proposition: Rules as influencing factors*

Proposition	Related Concept	Quote
IoT Privacy standards are dynamic and therefore hard to adhere to due to constant evolution.	Rules/Legislation	*I think what is not clear for me, is that the privacy standards and regulations keep changing, and it is very difficult to keep up, and keep aware of what is it, what do I need to do, to ensure that, you know, my privacy settings and standards are enabled (Respondent_10)*

Some of the standards are dynamic, ambiguous, and too lengthy which inadvertently inhibits user adherence. This finding concurs with the literature of Shayegh et al. (2019) through which the aim is to automate improvement of IoT privacy policies with the intention of making them user centric.

6.2.6 Objective

The sole objective from the previous model point of view was purely adherence, however, the revised conceptual model goes on further to reveal the influence of non-adherence and perceived benefits as drivers of adherence to IoT device privacy standards. The perceived associated benefits of adherence are an incentive for users to better focus on their IoT device

privacy. Self Determination Theory (SDT) can be applied in this instance to assist in explaining this finding relating to intended benefits of IoT devices use.

Figure *8* further elaborates the updated conceptual nodes of the "community" and "division of labour" as separate nodes that are indicative of the effect of the surroundings of a user. Different stakeholders and the community in the Activity System are respective influencers in user adherence. The model finally shows that there are additional causative factors to user adherence and these factors consist of health, convenience and necessity and they are discussed in Section 6.3 that follows. **Table *31*** highlights this section's propositions.

Table 31: *Proposition: Intended use of IoT device as an influencing factor*

Proposition	Related Concept	Quotes
Users are after functionality of the IoT devices and purely just accept IoT privacy standards for the sake of it.	Adherence/ Non-adherence	"If its Apple or Google, then I am most likely just to accept even if they are saying that they need my details" (Respondent_1)
User IoT privacy adherence is driven by brand loyalty and manufacturer.		

6.3 Contradictions to AT/Unlinked study Constructs

This section explores some of the unlinked codes according to AT, which applies "the term contradiction to indicate a misfit within elements, between them, between different activities, or between different developmental phases of a single activity. Contradictions manifest themselves as problems, ruptures, breakdowns, clashes" (Kuutti, 1996, p. 16). Elements and activities within a system seldom contradict each other to delay any intended progress of the entire system.

6.3.1 Health impact contradiction

When Respondent_1 answered Q15 regarding the cost of mobile data, He hinted on the potential of owning 5G enabled phone to enjoy faster and cheaper connectivity for his device. However, Respondent_1 pointed out the speculative potential health impact based on what he heard people say. Another reported issue arises out of the need for contact tracing with the motive of reducing the spread of the Covid-19 coronavirus. The contradiction manifests in such a way that devices designed for communication are repurposed to enable contact tracing. The contradiction strains the intended use of the communication system.

6.3.2 Convenience and necessity

It is apparent that conveniences underpin some of participants' adherence tendencies. The ease of use or none thereof of IoT devices influences the level of privacy standards adherence. Some devices have user friendly interfaces that enable users to locate privacy settings faster. In addition, users find it necessary to alter their behaviours with the motivation of benefitting from the secure use of their IoT devices.

There are inconveniences and non-adherence consequential to lengthy privacy standards in the form of user manuals and documentation laden with technical jargon. The documentation was found hard to read and comprehend. Calls to simplify IoT device accompanying documentation to aid standards' adherence were recurring from most of the participants.

Another point of contention raised by some participants talking to convenience was the issue of placing features to only be accessed only and only if the user has accepted the terms and conditions. This can be construed as leading to non-adherence if there is no failsafe to ensure users privacy if the said features are designed to collect discreet private information. **Table *32*** highlights the key propositions of this section.

Table 32: *Proposition: Convenience and health as influencing factors*

Proposition	Related Concept	Quotes
Convenience factors are one of the driving forces of IoT device privacy standards adherence	Convenience	"If its Apple or Google, then I am most likely just to accept even if they are saying that they need my details" (Respondent_1).
Health considerations when using IoT devices are an influencing factor when considering privacy adherence	Health	"I kind of get sceptical on whether you know what I am about to buy this phone is there like a disclaimer on their liability for health" (Respondent_1).

6.4 Linking themes

In this subsection, theme relationships and precedence as laid out in the thematic framework is discussed. The linkage is explained with a sample quote reference from the participants in the following subsections.

6.4.1 Devices vs Rules

The devices' linkage to rules in the context of this study is elaborated by the measures in the form of contact tracing using Bluetooth sensors on smartphones. The rules aspect speaks

to the requirement by governments to follow the recommendations of having these Bluetooth device settings switched on by users. This initiative has the motive of mitigating the spread of Covid-19. Some IoT Devices users decided not to be adherent to such rules requesting them to have settings always on, on their device for contact tracing purposes. Viljoen et al. (2020), Pepper and Botes (2020) highlight the necessity of the technological interventions in keeping settings to enhance adherence.

6.4.2 Costs vs Convenience

There is a level of convenience attached to a user permitting their personal information be processed by associated IoT device services to provide meaningful recommendations and reduced prices in the form of sales. This finding is consistent with the work of Zheng et al. (2018) discussed in Section 2.6 paragraph four, in which a similar finding regarding exposure of users to huge risks associated to focusing on the benefits of IoT provisions, at the cost of privacy.

6.4.3 Fear vs Community

The fear of hackers and loss of information, for example through social engineering. Social media community to which a user belongs can influence adherence. If a user receives a chain message on social media for example, which details the consequences of a friend whose privacy has been breached. The fear generated from viewing a post of this nature might influence an IoT device user to be more mindful of their own privacy. This finding is consistent with literature by Atzori et al. (2017) whereby they studied how IoT smart systems assist in security aspects by tracking malicious behaviour in the community.

6.4.4 Community (Government enforcers) vs Rules (POPIA) vs Division of labour vs attitudes

Mixed sentiments were voiced regarding better enforcement of "rules" that come in the form of the POPIA legislation by the government enforcers representative of "Division of labour". Additionally, attitudes towards the "rules" were observed to be an influencing factor backed up by comments from participants highlighting vigilance to trends that put their privacy at risk. Wickramasinghe and Reinhardt (2019) delved more into the impact of user attitudes on their privacy.

6.4.5 Cost factors vs Division of labour

The relationship between “Division of labour” and the costing theme is depicted in Section 5.6. Employers are expected to enforce existing policies and should bear the cost of running IoT devices in the instances where users need specific IoT devices to fulfil their roles in the companies they work for. Therefore, the ownership of running costs of IoT devices is born by the employers which financially shields the employees.

6.4.6 Rules (terms and conditions) vs Division of labour.

Participants challenged the legislators responsible for the drafting of the “rules” to make them conveniently legible as discussed in Section 5.4.2. The rules should be easy to comprehend, to facilitate an understanding on who is responsible for what aspects pertaining to a user’s IoT device privacy. This ranges from who manages the data from the user’s IoT devices, to who stores the data and finally what the user needs to do to ensure adherence.

6.4.7 Division of labour vs awareness

According to some participants, companies are to some extent liable to their privacy. They attribute most of the privacy related incidents to the IoT device manufacturers. There are sentiments that third parties in the form of service providers are responsible for implementing privacy safeguards for data harnessed from IoT devices. Some users are also aware of their role in ensuring their safe utilisation of IoT devices.

6.4.8 Awareness and device settings

There was a considerable level of awareness portrayed regarding device settings and how they could be detrimental to a user’s privacy. For instance, location settings are some of the device settings that are considered unnecessary due to physical security threats posed.

6.4.9 Awareness vs Rules

There was a recurring theme regarding awareness of the “rules” in respect of POPIA but no clarity on its significance and how it affects the end-user. A lot of sensitisation regarding legal recourse in case of privacy breaches because of use of IoT devices is required.

6.4.10 Speculation vs cost

Participants identify a linkage between the theme of cost and speculation. The lack of knowledge regarding electricity costs relating to IoT device consumption leads to speculation based on hearsay regarding durability of IoT devices in question.

6.4.11 Anxiety and trust

When third parties are involved with the user's device daily operations as illustrated in section 5.6.45.6.4, anxiety builds as to what their exact role is. There seems to be no clarity between the IoT device users and the third parties.

6.5 Propositions

In **Table *33***, the propositions from the subsections of Section 6.2 are consolidated. "During the theory-development process, logic replaces data as the basis for evaluation. Theorists must convince others that their propositions make sense if they hope to have an impact on the practice of research" (Whetten, 1989, p. 491). In this instance, propositions summarise possible explanations to the phenomena under study.

Table 33: *Propositions summarised*

ID	Proposition	Section
1	The type of device and associated third parties influence users' privacy adherence decisions during use of IoT devices.	5.2.2 and **Table *23***
2	Users are incentivised to part with their personal data in exchange for rewards and freebies, leaving their privacy at risk.	5.2.3 and **Table *24***
3	The level of penalties attached to non-adherence is a determining factor to IoT device privacy standards adherence.	
4	Users underestimate their position in the ecosystem of IoT device privacy. There is a user inferiority complex attitude towards their personal data.	0 and **Table 25**
5	Device Settings, ease of use influence adherence. Due to the multitude of manufacturers, there are various unstandardised ways of user interfaces that are not user friendly.	
6	Personality determines level of trust, linking Attitudes to trust whereby it takes a good impression by the device manufacturers to obtain the trust of a user.	5.3.5 and **Table *26***
7	Associated consequences of non-adherence are a driving factor to IoT Privacy adherence.	5.3.5 and **Table *27***
8	Fear of retribution drives IoT Privacy standards adherence due to associated consequences.	
9	IoT Privacy standards are dynamic and therefore hard to adhere to due to constant evolution.	5.4.2 and ***Table 30***
10	A User's surrounding community greatly influences their decision regarding adherence to IoT Privacy standards	5.5.3 and **Table *29***
11	Proper government policing and enforcement determines the level of IoT privacy standards adherence.	5.6.4 and **Table *28***
12	Legible privacy standards documentation can be a determinant of IoT privacy standards' adherence.	
13	Users are after functionality of the IoT devices and purely just accept IoT privacy standards for the sake of it.	5.7.2 and **Table *31***
14	User IoT privacy adherence is driven by their loyalty to the device brand and manufacturer.	
15	Convenience factors are one of the driving forces of IoT device privacy standards adherence	6.3.1/6.3.2 and **Table *32***
16	Health considerations when using IoT devices are an influencing factor when considering privacy adherence	

As showed in **Table *33***, there was a total of sixteen propositions from the analysis findings. These propositions are concerned with several key factors that can be linked back to the components of Activity Theory. Some of the propositions point to individual user personalities as influencing factors to adherence. In addition, users are driven by trust in IoT devices and service providers, fear and speculation in the systems involving the IoT devices. Convenience and health factors were the contradictions to the model but were also contributors to adherence.

6.6 Summary of chapter

The findings introduced the updated conceptual model which speaks to the themes with linkages to the literature reviewed. These themes were strongly evident in the analysis and henceforth state in this Chapter as findings. However, more themes not catered for in the original conceptual model came to light as they are regarded as contradictions to AT. The findings concluded with propositions revolving around the users' personality and their surrounding were major influencers of adherence to IoT device privacy standards.

7. Conclusion

The previous Chapter postulated the findings of this study which highlighted the factors influencing IoT device Privacy standards adherence. In this Chapter, the study is concluded. This Chapter summarises and states the limitations of the study. Additionally, the contribution and implications of the study are discussed. The future research is also discussed in this chapter.

7.1 Summary of study

The objectives of this research were threefold, firstly, to understand the factors influencing users' adherence to IoT device privacy standards. Secondly to inquire about the "how" users are presently adhering to privacy centred practices and lastly, to explore what measures can be enacted to increase adherence to the said standards.

7.1.1 Literature review

Literature from different authors and scholars in relation to the phenomena was reviewed which informed the conceptual model. This conceptual model was further revised after more information came to light from the thematic analysis of the interview transcripts.

7.1.2 Theoretical framework

Activity Theory (AT) was selected as the theoretical framework underpinning this study. A three-phase approach to using AT was employed to understand, identify, and link analysis elements to the components of AT.

7.1.3 Methodology

A qualitative research methodology informed this exploratory study. The study followed an interpretivist research philosophy perspective. The ontological stance adopted is subjectivism and interpretivism from an epistemological perspective.

7.1.4 Data collection and analysis

Semi-structured interviews were remotely held and recorded. Recordings from the remotely held interviews using Microsoft teams were transcribed, coded, and themed in Nvivo using the attached thematic analysis framework in Appendix F. The analysis revealed that user personalities and other external factors like third-parties impact IoT device privacy adherence.

7.1.5 Key findings

Some of the findings of the thematic analysis revealed several factors influencing IoT privacy adherence, and they included but not limited to: - Users' personality and their surroundings, trust, fear, and speculation. Among the new findings not originally conceptualised, were convenience and health factors which were illustrated accordingly in the revised conceptual framework detailed in **Figure *8***, in Section 6.2.

7.2 Limitations of the study

It is appropriate to base knowledge claims on careful qualitative analysis of a sample and considerations of its similarities between occurrences in other settings (Seddon & Scheepers, 2012). In general, there are several assumptions that were made in respect of applicability of this study on the general population and not just as a sample. Seddon and Scheepers (2012) theorise that it is important to specify the boundary conditions to justify the soundness of a study. To some extent, the claims are supported by the literature and therefore, the assumption of this qualitative study, which is affixed by non-probability-based sampling, generalises the participants detailed in Appendix E to be representative of the population.

This study has the following additional limitations and respective mitigations

1) **For this study, IoT Devices owned were restricted to a home setting.**

IoT devices can be operated in a variety of settings including, industrial, city-wide implementations. The pilot and subsequent interview participants had all encountered internet connected devices within their homes.

2) **Only participants above eighteen years of age were allowed to participate.**

The age limitation condition was to ensure that only users deemed to be competent enough to comprehend any standards in the form of legal material pertaining to their IoT devices. This was mitigated on the survey questionnaire through the "age" entry to ensure that only participants' responses above 18 years of age are obtained.

3) **Due to the nature of restrictions owing to Covid-19, interviews had to be virtual, and participants were not comfortable being video recorded. Body language queues could therefore not be picked up**.

The use of Microsoft teams could only allow the recording of voice interviews. These recording transcripts were revisited through two levels of coding, to ensure more themes are picked up and to compensate for the in-person interviews.

4) **Network quality kept on dropping during the scheduled Microsoft Teams interview calls.**

For some of the participants, they were advised to use mobile hotspots whenever their Home Fibre connection disconnected. Participants were offered mobile data refunds to mitigate the cost of conducting these interviews virtually.

5) **Environment as mediating factor impact on adherence**

For this study, he environment as a mediating artifact according to Activity Theory was limited to the actual IoT device(s) in the control of the user.

7.3 Contribution and implication to theory

As demonstrated in the findings, the factors influencing adherence can be explained by existing theory to some extent. However, making use of the guidelines of AT, leaves room for improvement to the framework to cater for the outlier elements related to the activity system and phenomena under investigation. Wickramasinghe and Reinhardt (2019) researched into user attitudes in IoT device use and impacts on privacy, however, this research focusses on the factors influencing adherence, to which "attitudes" surfaced as a factor. Therefore, this study has contributed to literature on IoT device privacy and to the growing body of Information System research on IoT.

7.4 Future research

The Impact of third-party services on IoT privacy standard adherence (including voice assistants, Siri, Cortana, Alexa, Bixby, and Google Assistant) and data privacy models in IoT in South Africa need to be further investigated to enhance privacy standards' adherence. Analysis of Impact of POPIA on users and IOT device privacy in general needs to be studied more to aid how best technology and legislation can be used to enhance IoT privacy.

> *I think it is something I would want further investigated, with a lot more of this IoT is our data, like how does that fit in to the model of data privacy, and who then manages that data, and where ever that information is stored before it gets to me on my phone, you know, while it is swift in practice, but I am like, there are multiple touch points, how do you then govern the privacy ? (Respondent_9)*

8. References

African Union Commission. (2014). *Science, technology, and innovation strategy for Africa 2024*. African Union Commission.

Agee, J. (2009). Developing qualitative research questions: A reflective process. *International Journal of Qualitative Studies in Education*, *22*(4), 431–447. https://doi.org/10.1080/09518390902736512

Aldeer, M., Javanmard, M., & Martin, R. P. (2018). A Review of Medication Adherence Monitoring Technologies. *Applied System Innovation 2018, Vol. 1, Page 14*, *1*(2), 14. https://doi.org/10.3390/ASI1020014

Alsmirat, M. A., Jararweh, Y., Obaidat, I., & Gupta, B. B. (2017). Internet of surveillance: a cloud supported large-scale wireless surveillance system. In *The journal of supercomputing* (Vol. 73, Issue 3, pp. 973–992). Kluwer Academic Publishers. https://doi.org/10.1007/s11227-016-1857-x

American Psychological Association. (n.d.). *American Psychological Association*. Retrieved September 16, 2021, from https://www.apa.org

Anjomshoa, F., Aloqaily, M., Kantarci, B., Erol-Kantarci, M., & Schuckers, S. (2017). Social Behaviometrics for Personalized Devices in the Internet of Things Era. *IEEE Access*, *5*, 12199–12213. https://doi.org/10.1109/ACCESS.2017.2719706

Asiimwe, B. M. (2019). Assessment of Factors Associated With OTT Tax Compliance in Uganda: A Case Study of Kampala. In *Assessment of Factors Associated With OTT Tax Compliance in Uganda: A Case Study of Kampala*. Makerere University. http://hdl.handle.net/20.500.12281/7516

Atlam, H. F., & Wills, G. B. (2020). IoT Security, Privacy, Safety and Ethics. In *Internet of Things* (pp. 123–149). Springer International Publishing. https://doi.org/10.1007/978-3-030-18732-3_8

ATLAS Security Engineering and Response Team (ASERT). (2019). *Realtek SDK Exploits on the Rise from Egypt*. https://www.netscout.com/blog/asert/realtek-sdk-exploits-rise-egypt

Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: definition, potentials, and societal role of a fast-evolving paradigm. *Ad Hoc Networks*, *56*, 122–140. https://doi.org/10.1016/j.adhoc.2016.12.004

Bailey, M. W. (2015). Seduction by technology: Why consumers opt out of privacy by buying into the Internet of Things. In *Texas law review*. (Vol. 94, p. 1023). Texas Law Review Publications. https://heinonline.org/HOL/P?h=hein.journals/tlr94&i=1067

Ball, K. (2017). African Union Convention on Cyber Security and Personal Data Protection. *International Legal Materials*, *56*(1), 164–192. https://doi.org/10.1017/ilm.2016.3

BBC. (2019). *Ransomware hits Johannesburg electricity supply - BBC News*. BBC Online. https://www.bbc.com/news/technology-49125853

Benson, A., Lawler, C., & Whitworth, A. (2008). Rules, roles and tools: Activity theory and the comparative study of e-learning. *British Journal of Educational Technology*, *39*(3), 456–467. https://doi.org/10.1111/J.1467-8535.2008.00838.X

Bhattacharya, S., & Rach, T. (2021). Social Strife of South Africa in 2021 Fueled by Economic Issue than Political Instability. *International Journal of Research in Engineering, Science and Management*, *4*(8), 38–40. https://journals.resaim.com/ijresm/article/view/1148

Birhane, A. (2020). Algorithmic Colonization of Africa. *SCRIPTed: A Journal of Law, Technology and Society*, *17*, 389. https://heinonline.org/HOL/Page?handle=hein.journals/scripted17&id=389&div=21&collection=journals

Brewster, T. (2017, March 7). *Here's How The CIA Allegedly Hacked Samsung Smart TVs -- And How To Protect Yourself*. Forbes. https://www.forbes.com/sites/thomasbrewster/2017/03/07/cia-wikileaks-samsung-smart-tv-hack-security/#45fd5cef4bcd

Brill, H., & Jones, S. (2017). Little Things and Big Challenges: Information Privacy and the Internet of Things. *American University Law Review*, *66*(5), 1183–1230.

Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. *International Journal of Information Management*, *51*. https://doi.org/10.1016/j.ijinfomgt.2019.05.008

Burrell, G., & Morgan, G. (2017). Sociological Paradigms and Organisational Analysis Elements of the Sociology of Corporate Life. In *Sociological Paradigms and Organisational Analysis*. Routledge. https://doi.org/10.4324/9781315242804

Burtch, G., Carnahan, S., & Greenwood, B. N. (2018). Can you gig it? An empirical examination of the gig economy and entrepreneurial activity. *Management Science*, *64*(12), 5497–5520.

Cambridge English Dictionary. (n.d.). Retrieved September 16, 2021, from https://dictionary.cambridge.org

Carpenter, D. (2018). *Ethics, Reflexivity and Virtue In: The SAGE Handbook of Qualitative Research Ethics, Reflexivity and Virtue*. https://doi.org/10.4135/9781526435446

Carson, D., Gilmore, A., Perry, C., & Gronhaug, K. (2011). Qualitative Marketing Research. In *Qualitative Marketing Research*. SAGE Publications, Ltd. https://doi.org/10.4135/9781849209625

Chibuye, M., & Phiri, J. (2017). A Remote Sensor Network using Android Things and Cloud Computing for the Food Reserve Agency in Zambia. *IJACSA) International Journal of Advanced Computer Science and Applications*, *8*(11), 411–418.

Cho, H., Ippolito, D., & Yu, Y. (2020). Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs. *ArXiv.Org*, 7. https://arxiv.org/abs/2003.11511

Chong, I., Xiong, A., & Proctor, R. W. (2019). Human Factors in the Privacy and Security of the Internet of Things. *Ergonomics in Design*, *27*(3), 5–10. https://doi.org/10.1177/1064804617750321

Competition Commission of South Africa. (2019). *DATA SERVICES MARKET INQUIRY FINAL REPORT competition regulation for a growing and inclusive economy*.

Cousin, P., Le Gall, F., Pham, C., Malaguti, N., Danet, P.-Y., & Ziegler, S. (2018). *IoT standards for africa and sustainable development goals (SDGs)*. Institute of Electrical and Electronics Engineers Inc.

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches* (Second Edi). Sage Publications.

Dlamini, N. N. (2017). *The potential use of the Internet of Things (IoT) in South African retail businesses*. University of Cape Town.

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*, 531–537. https://researchspace.csir.co.za/dspace/bitstream/handle/10204/7438/Dlodlo2_2013.pdf

Dolley, C. (2021, November 6). Cyberattacks: South Africa, you've been hacked. *Daily Maverick*. https://www.dailymaverick.co.za/article/2021-11-06-cyberattacks-south-africa-youve-been-hacked/

Dries, G. (2018). *How the "Internet of Things" Came to Be - Read the Whole Story Here* (Vol. 2020, Issue Mar 4,). https://itelligencegroup.com/sk/global-blog/how-the-internet-of-things-came-to-be-read-the-whole-story-here/

Engeström, Y. (1987). *Learning by Expanding: An Activity Theoretical Approach To Developmental Research*.

Engeström, Y. (1999). Activity theory and individual and social transformation. In *Perspectives on Activity Theory* (pp. 19–38). Cambridge University Press.

https://doi.org/10.1017/cbo9780511812774.003

Engeström, Y. (2014). The Emergence of Learning Activity as a Historical Form of Human Learning. In *Learning by Expanding* (pp. 25–108). Cambridge University Press. https://doi.org/10.1017/cbo9781139814744.004

Engeström, Y., & Miettinen, R. (1999). Introduction. In Y. Engeström, R. Miettinen, & R.-L. Punamäki (Eds.), *Perspectives on Activity Theory* (pp. 1–16). Cambridge University Press. https://doi.org/10.1017/CBO9780511812774.002

Fathin, U. (2020). Singapore launches contact tracing mobile app to track coronavirus infections. In *Reuters*. https://www.reuters.com/article/us-health-coronavirus-singapore-technolo-idUSKBN2171ZQ

Feiler, J. (2016). Exploring the HomeKit World. In *Learn Apple HomeKit on iOS* (pp. 9–26). Springer.

Fernandes, E., Jung, J., & Prakash, A. (2016). Security analysis of emerging smart home applications. *2016 IEEE Symposium on Security and Privacy (SP)*, 636–654.

Foltz, C. B., & Foltz, L. (2020). Mobile users' information privacy concerns instrument and IoT. *Information and Computer Security*. https://doi.org/10.1108/ICS-07-2019-0090

Foltz, C. B., & Foltz, L. (2021). MUIPC and intent to change IoT privacy settings. *Journal of Computing Sciences in Colleges*, *36*(7), 27–38. http://www.ccsc.org/publications/journals/SC2021.pdf#page=27

Foot, K. (2014). *Cultural-Historical Activity Theory: Exploring a Theory to Inform Practice and Research*. http://www.tandfonline.com/toc/whum20/current#.UqlMEeKRMTA.

Fu, Y., & Wu, W. (2018). Behavioural informatics for improving water hygiene practice based on IoT environment. *Journal of Biomedical Informatics; J Biomed Inform*, *78*, 156–166. https://doi.org/10.1016/j.jbi.2017.11.006

Gartner. (2020). Market Guide for Industrial IoT Gateways. In *Gartner*. Gartner. https://www.gartner.com/document/3982835

Gul, S., Asif, M., Ahmad, S., Yasir, M., Majid, M., Malik, M. S. A., & Arshad, S. (2017). A survey on role of internet of things in education. *International Journal of Computer Science and Network Security*, *17*(5), 159–165.

Haghayegh, S., Khoshnevis, S., Smolensky, M. H., Diller, K. R., & Castriotta, R. J. (2019). Accuracy of Wristband Fitbit Models in Assessing Sleep: Systematic Review and Meta-Analysis. *Journal of Medical Internet Research*, *21*(11), e16273–e16273. https://doi.org/10.2196/16273

Hasan, H, & Kazlauskas, A. (2014). Activity theory: Who is doing what, why and how. In

Helen Hasan (Ed.), *Being Practical with Theory: A Window into Business Research* (pp. 9–14). THEORI. http://eurekaconnection.files.wordpress.com/2014/02/p-09-14-activity-theory-theori-ebook-2014.pdf

Hawthorne, R. (2018). The effects of lower mobile termination rates in South Africa. *Telecommunications Policy*, *42*(5), 374–385. https://doi.org/10.1016/j.telpol.2018.02.007

He, Q., Xu, Y., Liu, Z., He, J., Sun, Y., & Zhang, R. (2018). A privacy-preserving Internet of Things device management scheme based on blockchain. *International Journal of Distributed Sensor Networks*, *14*(11). https://doi.org/10.1177/1550147718808750

He, Y. (2019). Recommending Privacy Settings for IoT. *24th Inter-National Conference on Intelligent User Interfaces (IUI '19 Companion)*, 157–158. https://doi.org/10.1145/3308557.3308732

Hejazi, H., Rajab, H., Cinkler, T., & Lengyel, L. (2018). Survey of platforms for massive IoT. *2018 IEEE International Conference on Future IoT Technologies (Future IoT)*, 1–8. https://doi.org/10.1109/FIOT.2018.8325598

Holmes, A. (2019). *The FBI is warning people about the security of their smart TVs*. Business Insider. https://www.businessinsider.com/smart-tv-security-fbi-warning-2019-12?IR=T

IDC. (2020). *The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast* (Vol. 2020, Issue Apr 23,). https://www.idc.com/getdoc.jsp?containerId=prUS45213219

Independent Communications Authority of South Africa. (2020). *Emergency release of spectrum to meet the spike in broadband services demand due to COVID-19*. https://www.icasa.org.za/news/2020/emergency-release-of-spectrum-to-meet-the-spike-in-broadband-services-demand-due-to-covid-19

Independent Communications Authority of South Africa. (2021). *5G Annual Report - 2021*. https://www.icasa.org.za/legislation-and-regulations/5g-annual-report-2021

INTERPOL Cybercrime Directorate. (2021). *AFRICAN CYBERTHREAT ASSESSMENT REPORT*. https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf

ISO/IEC, J. T. C. 1. (2015). Internet of Things (IoT) Preliminary Report 2014. In *International Organization for Standardization*. ISO. https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf

Iyamu, T., & Shaanika, I. (2019). The use of activity theory to guide information systems

research. *Education and Information Technologies*, *24*(1), 165–180. https://doi.org/10.1007/s10639-018-9764-9

Jeanes, E. (2019). *A Dictionary of Organizational Behaviour*. Oxford University Press.

Job, A. (2020). Security, compliance, POPI and COVID-19. In *ITWEB*. https://www.itweb.co.za/content/RgeVDqPY4z3vKJN3

Jonassen, D. H., & Land, S. (Eds.). (2014). *Theoretical foundations of learning environments*. Routledge.

Jones, L., Brown, D., & Palumbo, D. (2020). Coronavirus: A visual guide to the economic impact. In *BBC News* (Business). https://www.bbc.com/news/business-51706225

Kahn, J. (2020). *Digital Contact Tracing for Pandemic Response : Ethics and Governance Guidance*. Johns Hopkins University Press. https://doi.org/10.1353/book.75831

Kandeh, A. T., Botha, R. A., & Futcher, L. A. (2018). Enforcement of the Protection of Personal Information (POPI) Act: Perspective of data management professionals. *SA Journal of Information Management*, *20*(1), 1–9. https://doi.org/10.4102/sajim.v20i1.917

Karanasios, S., & Allen, D. (2018). Activity theory in Information Systems Research. *Information Systems Journal*, *28*(3), 439–441. https://doi.org/10.1111/isj.12184

Karpf, B. A. (2017). Dead reckoning : where we stand on privacy and security controls for the Internet of Things. In *Where we stand on privacy and security controls for the IoT*. Massachusetts Institute of Technology. https://dspace.mit.edu/handle/1721.1/111231

Kasadha, J., Alli, A. A., Basuuta, A. K., & Mpoza, A. (2019). Social media taxation and its impact on Africa's economic growth. *Journal of Public Affairs*, *20*(2), n/a-n/a. https://doi.org/10.1002/pa.2004

Kelion, L. (2020). Huawei 5G kit must be removed from UK by 2027. In *BBC News* (Technology). https://www.bbc.com/news/technology-53403793

Kelly, J. T., Campbell, K. L., Gong, E., & Scuffham, P. (2020). The Internet of Things: Impact and Implications for Health Care Delivery. *Journal of Medical Internet Research*, *22*(11), e20135. https://doi.org/10.2196/20135

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. In *Computers & Security* (Vol. 64, p. 122). Elsevier. https://doi.org/10.1016/j.cose.2015.07.002

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. *Computer*, *50*(7), 80–84. https://doi.org/10.1109/MC.2017.201

Kuutti, K. (1996). Activity Theory as a Potential Framework for Human-Computer Interaction Research. In B. A. Nardi (Ed.), *Context and Consciousness: Activity Theory and Human-*

computer Interaction (p. 400). MIT Press.

Lektorsky, V. A. (1999). Activity theory in a new era. In Y. Engeström, R. Miettinen, & R.-L. Punamäki (Eds.), *Perspectives on Activity Theory* (pp. 65–69). Cambridge University Press. https://doi.org/10.1017/CBO9780511812774.006

Lin, H., & Bergmann, N. (2016). IoT Privacy and Security Challenges for Smart Home Environments. *Information*, *7*(3), 44. https://doi.org/10.3390/info7030044

Makarova, I., Shubenkova, K., Bagateeva, A., & Pashkevich, A. (2018). Digitalization of Education as a New Destination of E-Learning. *2018 International Symposium ELMAR*, 31–34. https://doi.org/10.23919/ELMAR.2018.8534662

Mishra, S. S., & Rasool, A. (2019). IoT health care monitoring and tracking: A survey. *Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019*, 1052–1057. https://doi.org/10.1109/ICOEI.2019.8862763

Mohalder, R. D., Rahman, M. A., & Saha, A. (2019). *An IoT Based Approach against Physical and Mental Assault in Educational Institution* (pp. 1–5). IEEE. https://doi.org/10.1109/ICCCNT45670.2019.8944473

Motala, I., & Padayachee, I. (2018). Readiness to adopt the internet of things at the university of KwaZulu-Natal. In E. Ivala (Ed.), *Proceedings of the International Conference on e-Learning, ICEL* (Vols. 2018-July, pp. 256–268). Academic Conferences Limited.

Mwanza, D. (2001). *Where Theory meets Practice: A Case for an Activity Theory based Methodology to guide Computer System Design*. http://kmi.open.ac.uk/publications/techreports.html[http://www.INTERACT2001.com/]

Myers, M. D. (2019). *Qualitative research in business and management*. Sage Publications Limited.

Ndubuaku, M., & Okereafor, D. (2015). State of Internet of Things deployment in Africa and its future: The Nigerian scenario. In *African journal of information and communication* (Vol. 2015, Issue 15, p. 114). "LINK Centre University of the Witwatersrand, Johannesburg."

Nelke, S. A., & Winokur, M. (2020). Introducing IoT Subjects to an Existing Curriculum. *IEEE Design & Test*, 1. https://doi.org/10.1109/MDAT.2020.3005358

Ng, I. C. L., & Wakenshaw, S. Y. L. (2017). The Internet-of-Things: Review and research directions. *International Journal of Research in Marketing*, *34*(1), 3–21. https://doi.org/10.1016/j.ijresmar.2016.11.003

Nissen, H.-E., Klein, H.-K., Hirschheim, R. A., & IFIP Working Group 8.2. (1991). *Information systems research: contemporary approaches & emergent traditions:*

proceedings of the IFIP TC8/WG 8.2 Working Conference on the Information Systems Research Arena of the 90's Challenges, Perceptions, and Alternative Approaches: Copenhagen, Denmark. North-Holland Distributors for the U.S. and Canada Elsevier Science Pub. Co.

Padyab, A., & Ståhlbröst, A. (2018). Exploring the dimensions of individual privacy concerns in relation to the Internet of Things use situations. *Digital Policy, Regulation and Governance*, *20*(6), 528–544. https://doi.org/10.1108/DPRG-05-2018-0023

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*(3), 510–527. https://doi.org/10.1109/JSAC.2016.2525418

Pepper, S., & Botes, M. (2020). *Balancing privacy with public health: how well is South Africa doing?* https://theconversation.com/balancing-privacy-with-public-health-how-well-is-south-africa-doing-140759

Pieterse, C. (2020, April 8). *Social Distancing Explained - SA Corona Virus Online Portal*. https://sacoronavirus.co.za/2020/04/08/social-distancing/

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279. https://doi.org/10.1016/J.COMNET.2012.12.018

Rutledge, R. L., Massey, A. K., & Anton, A. I. (2017). *Privacy impacts of IoT devices: A SmartTV case study* (pp. 261–270). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/REW.2016.40

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (5th ed). Pearson Education Limited.

Seddon, P. B., & Scheepers, R. (2012). Towards the improved treatment of generalization of knowledge claims in IS research: drawing general conclusions from samples. *European Journal of Information Systems*, *21*(1), 6–21. https://doi.org/10.1057/ejis.2011.9

Sen, A., Ahmed, A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving privacy in internet of things: a survey. *International Journal of Information Technology (Singapore)*, *10*(2), 189–200. https://doi.org/10.1007/S41870-018-0113-4

Shayegh, P., Jain, V., Rabinia, A., & Ghanavati, S. (2019). *Automated Approach to Improve IoT Privacy Policies*. https://arxiv.org/abs/1910.04133v1

Shepardson, D. (2020). Exclusive: U.S. finalizing federal contract ban for companies that use

Huawei, others. In *Reuters*. https://www.reuters.com/article/us-usa-china-contracting-exclusive-idUSKBN24A22F

Shuhaiber, A., Mashal, I., & Alsaryrah, O. (2019). Smart homes as an IoT application: Predicting attitudes and behaviours. *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA, 2019-Novem*. https://doi.org/10.1109/AICCSA47632.2019.9035295

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164.

Sikder, A., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, A. (2018). A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications. *ArXiv.Org*.

Singh, J., Millard, C., Reed, C., Cobbe, J., & Crowcroft, J. (2018). Accountability in the IoT: Systems, Law, and Ways Forward. In *Computer* (Vol. 51, Issue 7, pp. 54–65). https://doi.org/10.1109/MC.2018.3011052

Slevitch, L. (2011). Journal of Quality Assurance in Hospitality & Tourism Qualitative and Quantitative Methodologies Compared: Ontological and Epistemological Perspectives. *Journal of Quality Assurance in Hospitality & Tourism*, *12*(1), 73–81. https://doi.org/10.1080/1528008X.2011.541810

Soiferman, L. K. (2010). *Compare and Contrast Inductive and Deductive Research Approaches*.

Sollins, K. R. (2019). IoT big data security and privacy versus innovation. *IEEE Internet of Things Journal*, *6*(2), 1628–1635. https://doi.org/10.1109/JIOT.2019.2898113

SonicWall. (2021). *Mid-Year Update: 2021 SonicWall Cyber Threat Report*. https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2021-cyber-threat-report.pdf

South-African Government. (2013). *Protection of Personal Information Act 4 of 2013*. https://www.gov.za/documents/protection-personal-information-act?gclid=EAIaIQobChMIs9vAqOqY6wIVWOJ3Ch1bwgRDEAAYAyAAEgKdfvD_BwE

Stahl, B., Timmermans, J., & Mittelstadt, B. (2016). The Ethics of Computing: A Survey of the Computing-Oriented Literature. *ACM Computing Surveys (CSUR)*, *48*(4), 1–38. https://doi.org/10.1145/2871196

Statistics South Africa. (2019). Crime Statistics South Africa. In *http://www.statssa.gov.za/*. http://www.statssa.gov.za/?page_id=737

Subahi, A., & Theodorakopoulos, G. (2018). Ensuring Compliance of IoT Devices with Their Privacy Policy Agreement. *Proceedings - 2018 IEEE 6th International Conference on Future Internet of Things and Cloud, FiCloud 2018*, 100–107. https://doi.org/10.1109/FICLOUD.2018.00022

Subahi, A., & Theodorakopoulos, G. (2019). Detecting IoT user behavior and sensitive information in encrypted iot-app traffic. *Sensors (Switzerland)*, *19*(21). https://doi.org/10.3390/s19214777

Swaroop, K. N., Chandu, K., Gorrepotu, R., & Deb, S. (2019). A health monitoring system for vital signs using IoT. *Internet of Things*, *5*, 116–129. https://doi.org/10.1016/j.iot.2019.01.004

Taherdoost, H. (2016). Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. *International Journal of Academic Research in Management (IJARM)*, *Vol 5*, 18–27. https://doi.org/10.2139/ssrn.3205035

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. *Mdpi.Com*, *10*(12), 4102. https://doi.org/10.3390/app10124102

United Nations. (2019). *World Population Prospects 2019 Highlights*.

University of Cape Town. (2018). *Research Data Management Policy*. University of Cape Town. https://www.uct.ac.za/sites/default/files/image_tool/images/328/about/policies/TGO_Policy_Research_Data_Management_2018.pdf

Viljoen, I. M., Castelyn, C. de V., Pope, A., Botes, M., & Pepper, M. S. (2020). Contact tracing during the covid-19 pandemic: Protection of personal information in south africa. *South African Journal of Bioethics and Law*, *13*(1), 15–20. https://doi.org/10.7196/SAJBL.2020.V13I1.718

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, *15*(3), 320–330. https://doi.org/10.1057/palgrave.ejis.3000589

Weiser, M. (1991). The Computer for the 21st Century. *Scientific American*, *265*(3), 94. https://doi.org/10.1038/scientificamerican0991-94

Whetten, D. A. (1989). What Constitutes a Theoretical Contribution? *The Academy of Management Review*, *14*(4), 490. https://doi.org/10.2307/258554

Wickramasinghe, C. I., & Reinhardt, D. (2019). A Survey-based Exploration of Users' Awareness and their Willingness to Protect their Data with Smart Objects. In M. Friedewald, Ö. Melek, L. Eva, K. Stephan, & F. Samuel (Eds.), *Privacy and Identity Management* (pp. 427–446). https://doi.org/10.1007/978-3-030-42504-3_27

Williams, M., Nurse, J., & Creese, S. (2018). “Privacy is the Boring Bit”: User Perceptions and Behaviour in the Internet-of-Things. *ArXiv.Org*.

Winder, D. (2020, February 19). *Hackers Made Tesla Cars Autonomously Accelerate Up To 85 In A 35 Zone*. Forbes.Com. https://www.forbes.com/sites/daveywinder/2020/02/19/hackers-made-tesla-cars-autonomously-accelerate-up-to-85-in-a-35-zone/#357641c07245

Wolfe, E., & Ries, B. (2019, December 13). *Ring camera: A hacker accessed a family’s security camera told their 8-year-old daughter he was Santa Claus - CNN*. CNN.Com. https://edition.cnn.com/2019/12/12/tech/ring-security-camera-hacker-harassed-girl-trnd/index.html

World Economic Forum. (2018). *Why schools should teach the curriculum of the future, not the past* (Vol. 2020, Issue July 17,). https://www.weforum.org/agenda/2018/09/why-schools-should-teach-the-curriculum-of-the-future-not-the-past/

World Health Organization. (2020). *WHO Director-General’s opening remarks at the media briefing on COVID-19-11 March 2020*. https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

www.cable.co.uk. (2021). *Worldwide Mobile Data Pricing 2021 | 1GB Data Cost in 230 Countries - Cable.co.uk*. Cable.Co.Uk. https://www.cable.co.uk/mobiles/worldwide-data-pricing/

Zachariadis, M., Scott, S., & Barrett, M. (2013). Methodological implications of critical realism for mixed-methods research. *MIS Quarterly: Management Information Systems*, *37*(3), 855–880. https://doi.org/10.25300/misq/2013/37.3.09

Zeng, E., Mare, S., Roesner, F., & Allen, P. G. (2017). *End User Security and Privacy Concerns with Smart Homes*. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1–20. https://doi.org/10.1145/3274469

Appendix

A. Ethics approval letter

Faculty of Commerce

Private Bag X3, Rondebosch, 7701
2.26 Leslie Commerce Building, Upper Campus
Tel: +27 (0) 21 650 4375/ 5748 Fax: +27 (0) 21 650 4369
E-mail: jacques.rousseau@uct.ac.za
Internet: www.uct.ac.za
@Commerce UCT UCT Commerce Faculty Office

20 11 2020

Philip Bazanye

Department of Information Systems

University of Cape Town

REF: REC 2020/11/014

User adherence towards privacy standards in the usage of IoT devices in South Africa

We are pleased to inform you that your ethics application has been approved. Unless otherwise specified this ethical clearance is valid until 30-Nov-2021 .

Your clearance may be renewed upon application.

Please be aware that you need to notify the Ethics Committee immediately should any aspect of your study regarding the engagement with participants as approved in this application, change. This may include aspects such as changes to the research design, questionnaires, or choice of participants.

The ongoing ethical conduct throughout the duration of the study remains the responsibility of the principal investigator.

We wish you well for your research.

2020.11.20
09:29:17 +02'00'

Jacques Rousseau
Commerce Research Ethics Chair
University of Cape Town
Commerce Faculty Office
Room 2.26 | Leslie Commerce Building

Office Telephone: +27 (0)21 650 2695 / 4375
Office Fax: +27 (0)21 650 4369
E-mail: jacques.rousseau@uct.ac.za
Website: https://www.commerce.uct.ac.za/Pages/Ethics-in-Research

B. Research letter

Department of Information Systems

Leslie Commerce Building
Engineering Mall, Upper Campus
Private BagX3 - Rondebosch - 7701
Tel: +27 (0) 21 6502261 Fax: +27 (0) 21650 2280
http://www.commerce.uct.ac.za/informationsystems/

Good day,

As part of the requirements for completing a master's degree in information systems at the University of Cape Town, I would like to invite you to participate in my research project. By agreeing to participate in this study, you can also choose to withdraw from the research at any time for whatever reason, in accordance with the UCT Faculty of Commerce ethical research requirements.

The objective of the research is **to understand users' adherence towards privacy standards when using IoT devices in South Africa**. This is extremely important topic to understand, considering the privacy risks that exist in the use of IoT.
All the information collected will be treated in a confidential manner ensuring anonymity of your responses and used exclusively for the purposes of this study.

The questionnaire should only take approximately 30 minutes to complete and is available at the below link or by scanning the QR code. Should you be available to conduct an online interview, the zoom and Microsoft teams meeting link for direct interviews is also available at the end.

https://us02web.zoom.us/j/4609291064?pwd=ZVpPUHpJdXVPN2pXajVCUWVRYXRHUT09
Zoom ID 460 929 1064

https://forms.office.com/Pages/ResponsePage.aspx?id=NUNFkk5Wz0ywsCREW4wD91ttEubrvDNAg0y7CFF3rxxURVpSMFNHR0FFR0lEOU03TEpTUDZDTjc4SC4u

Regards

Philip Bazanye

C. Pilot questions

Department of Information Systems

Leslie Commerce Building
Engineering Mall, Upper Campus
Private BagX3 - Rondebosch - 7701
Tel: +27 (0) 21 6502261 Fax: +27 (0) 21650 2280
http://www.commerce.uct.ac.za/informationsystems/

Section 1- Introduction

Good day, I thank you for volunteering to participate in this study. This research has been approved by the Commerce Faculty Ethics in Research Committee. The aim of this research is to explore the factors that influence people to adhere to privacy settings used on internet connected devices. I will appreciate the information provided. The **fields below are optional**, you may exit this session by simply cancelling or pressing submit.

The main objectives of this session are as follows:

To understand the factors influencing users' adherence towards privacy standards in the use of IoT devices in South Africa.
To interpret how users are keeping to the prescribed IoT privacy standards.
To investigate ways by which to increase adherence to IoT device privacy standards. To come up with a conceptual framework

Date	
Duration	

Section 2 - Demographic information

Category	
Gender	
Age	
Education level (highest)	
Career /profession	
Sector/Industry	
Location	
Any IT course taken?	
Do you require a data refund for participating in this study? - if yes, cell number (Only for data refund if used WhatsApp, Zoom or Microsoft Teams)	

Section 3: Device ownership and use

Question ID	Question
Q1	How often do you use the internet?
Q2	What do you consider online privacy to be?
Q3	How many internet connected devices do you own? (List them)
Q4	How much does it cost to maintain your internet connected device(s) (e.g., Data)?
Q5	How often do you use this/these device(s)?
Q6	How often do you change the default password(s) and default username of this device using the provided app/interface?
Q7	How often do you update the provided app/interface software relating to your device?
Q8	What physical efforts do you have in place to protect/secure this/these devices? (Laptop cable, thumb drive encrypted USB, passcode, fingerprint scanner)
Q9	Do you have any form of smart home/home automation implementation? (e.g., controlling lighting, alarm systems, access control, CCTV).
Q10	What are your concerns regarding the devices in your ownership recording data? (Audio/video/Content history/location).
Q11	How often do you physically turn off this/these devices?

Section 4: Privacy

Pilot Question ID	Question
PQ1	What do you think influences your adherence to privacy?
PQ2	What privacy settings exist, and are active on your device? Do you change the default passwords?
PQ3	How often do you review these privacy settings on your device?
PQ4	How do you monitor your privacy whilst your IoT devices are switched on?
PQ5	Did you read the full terms of use policies that are addressed to your device(s) usage?
PQ6	Referring to your device specific privacy policy(ies)/Terms and conditions, what wording would you consider crucial to your adherence to the recommended standards?
PQ7	What are the known issues regarding privacy that relate to your device(s)?
PQ8	Which government regulations are you aware of regarding the internet in general?
PQ9	What information do you think is collected by these/this device(s)?
PQ10	What laws are you aware of that seek to protect your rights with the usage of your device?

D. Interview schedule

	Privacy and security	**Theme**
Q1	How would you define privacy in respect to your internet connected device?	Awareness/ knowledge/sensitised
Q2	What is your understanding of obedience/adherence?	Education/sensitised /Adherence understanding
Q3	PQ22 What are the known issues regarding privacy that relate to your device(s)?	Fear/Paranoia/Awareness
Q4	What steps are you taking to ensure your information gathered/stored by your IoT devices is safe and secure? *(Physical, Network level, Software level)*	Habits/information provided by user/Awareness
Q5	What is your comfort level regarding trusting a third-party with keeping your IoT device information and your devices safe? *(Password managers, Multifactor Authentication)*	Third-party providers
	Knowledge/Awareness/Attitudes/Habits	
Q6	PQ24 What information do you think is collected by these/this IoT device(s)? *(Bio data, browsing history, recordings)*	Awareness/Assumptions
Q7	What has the South African Legislature/Government done to protect you and your information collected from the devices you own?	Awareness/ knowledge/sensitised / Regulation/Rules
Q8	How do you feel about reading the device manufacturer accompanying documentation like terms and conditions / terms of use of the device?	Habits/Knowledge /Awareness/Attitudes
Q9	Are you willing to change habits to ensure your privacy is well secured?	Research question two (RQ2).
	Devices/Ease of use	
Q10	PQ12 How often do you update the provided app/interface software relating to your device?	Habits/Tech savviness
Q11	How is the network quality/reception in your Area/Location? Do any of your devices make use of streaming services and how secure do you think it is?	Network speeds ease the use of device(s)
Q12	PQ17 What privacy settings exist, and are active on your device? Do you change the default codes?	Habits/Knowledge/ Tech savviness
Q13	PQ14 What are your concerns regarding the devices in your ownership recording data? (Audio/video/Content history/location).	Device type and feature awareness
Q14	Please comment about your most used IoT device functionality and how safe you think it is to use.	Discussion
	Cost	
Q15	How does the cost of mobile data impact the maintenance and use your device from software update point of view?	Costs
	Any more comments/realisations regarding this interview?	Discussion

E. Respondent demographics

	Pseudo Name	Location	Profession	IT Course	Qualification	Gender	Date of interaction	Pilot Study
1	Respondent_1	Johannesburg	Developer Team Lead	Y	Honors	Male	20210628 152700	N
2	Respondent_2	Johannesburg	Travel consultant	N	Bachelors	Female	20210628 172229	N
3	Respondent_3	Rustenberg	IT Analyst	Y	Certificate	Male	20210702 111216	Y
4	Respondent_4	Pretoria	Marketing/IT	Y	Masters	Female	20210704 173201	N
5	Respondent_5	Mogwase	Client Services	N	Bachelors	Female	20210705 182424	Y
6	Respondent_6	Soweto	Software Developer	Y	Undergrad	Male	20210711 134621	Y
7	Respondent_7	Johannesburg	Psychologist	N	Honors	Female	20210711 171036	Y
8	Respondent_8	Krugersdorp	Business Analyst	Y	Masters	Male	20210717 060227	Y
9	Respondent_9	Roodepoort	IT Analyst	Y	Bachelors	Female	20210717 143327	N
10	Respondent_10	Midrand	Software Development Manager	Y	Diploma	Female	20210727 064246	N
11	Respondent_11	Cape Town	Investment Analyst	N	Undergrad	Male	20210325 213114	Y
12	Respondent_12	Johannesburg	IT Team Lead	Y	MBA	Female	20201208 094351	Y
13	Respondent_13	Johannesburg	IT Team Lead	Y	Honors	Female	20201208 104426	Y
14	Respondent_14	Cape Town	Scrum Master	Y	Honors	Male	20201209 114944	Y
15	Respondent_15	Pretoria	Medical Professional	N	Undergrad	Male	20201210 105103	Y
16	Respondent_16	Midrand	Medical Professional	N	Honors	Female	20201210 120000	Y
17	Respondent_17	Johannesburg	Business Analyst	Y	Masters	Female	20201217 182445	Y
18	Respondent_18	Tembisa	Self Employed	Y	Honors	Female	20201226 220958	Y
19	Respondent_19	Krugersdorp	Performance Engineer	Y	Bachelors	Female	20210323 130534	Y
20	Respondent_20	Krugersdorp	I.T	Y	Undergrad	Female	20210323 133822	Y
21	Respondent_21	Johannesburg	I.T Student	Y	Undergrad	Male	20210325 200815	Y
22	Respondent_22	Cape Town	Analyst	Y	Honors	Male	20210325 205909	Y
23	Respondent_23	Pretoria	Financial Services Professional	Y	Honors	Male	20210325 210155	Y
24	Respondent_24	Johannesburg	Telecommunications Professional	Y	Undergrad	Male	20210325 210320	Y
25	Respondent_25	Cape Town	Marketing Professional	Y	Bachelors	Female	20210325 210537	Y
26	Respondent_26	Johannesburg	Private Equity Professional	Y	Honors	Male	20210325 210458	Y
27	Respondent_27	Johannesburg	Will not say	N	Honors	Male	20210325 214141	Y
28	Respondent_28	Johannesburg	Asset Management Professional	N	Honors	Male	20210326 104119	Y
29	Respondent_29	Rustenburg	Public Relations Professional	Y	Undergrad	Female	20210329 15336	Y
30	Respondent_30	Johannesburg	Medical Professional (Dental)	N	Matric	Female	20210411 124745	Y
31	Respondent_31	Cape Town	Human Resources Consultant	N	Matric	Female	20210504 080053	Y

F. Thematic analysis framework

Overarching concept	Conceptual node	Dictionary Definition of concept	Core code definition	(Section ID) (New/ Existing code) (Code Text) (Code Reference hits)	Quote(s) backing concept	Summary of code in study context	Literature on concept
5.2 Tools	Devices	*"A machine, for example a phone or computer, that can be used to connect to the internet"* (*Cambridge English Dictionary*, n.d.)	*Configuration: "The particular hardware elements and their interconnection in a computer system for a particular period of operation."*	(5.2.1) (Existing) (Devices' settings) (150)	*"Uhm So the smart TV, the uhm, smart speaker, obviously my car, the Nav, then uhm, over and above, just my phone and the iPads" (Respiondent3)*	The device settings are the basic configuration of a user's IoT device(s) that influence them to be adherent or otherwise.	Research has been done in the area of recommending privacy settings for IoT device users (He, 2019). However, default settings are not a perfect fit for all user's preferences.
			A Supporting service rendered to the device owner in support of device functionality	(5.2.2) (Existing) (Related Services) (86)	*"Well, no, but I think with some of the cases, it is not like you have much of a choice, it is, sort of like a by-product of using the device!" (Respondent_9)*	These are mutually exclusive services rendered in conjunction with the IoT device to function in the activity system.	
			The cost associated to	(5.2.3) (Existing)	*"Data would run out, and I would end up buying more data.*	The multi-faceted costs of using IoT	

Overarching concept	Conceptual node	Dictionary Definition of concept	Core code definition	(Section ID) (New/ Existing code) (Code Text) (Code Reference hits)	Quote(s) backing concept		Summary of code in study context	Literature on concept
			running/maintaining the said device.	(Cost factor) (36)	*I do not want to do that" (Respondent_4)*		devices incurred by users.	
5.3 Subject	User	*"Someone who uses a product, machine, or service"* (*Cambridge English Dictionary*, n.d.) *"The various aspects of a person's character that combine to make them different from other people"* (*Cambridge English Dictionary*, n.d.)	*"Understanding of a situation or subject at the present time based on experience"* (*Cambridge English Dictionary*, n.d.)	(5.3.1) (Existing) (Awareness) (95)	Referring to POPIA *"I have heard of it, but I do not exactly know what it is!" (Respondent_2)*		The subject's perception of factors that affect their adherence to privacy standards.	Main actor in an activity system according to Hasan and Kazlauskas (2014).
			"The right to be left alone" (Butterfield et al., 2016)	(5.3.2) (Existing) (Understanding of privacy) (39)	*"…it is having my data secure so that it is not shared with anyone without my consent or approval" (Respondent_6)*		IoT Device user definition of the term "Privacy".	Kokolakis (2017) however states that attitudes vary depending on personal information in question and if the user stands to gain.
			"The collection of qualities that make up an individual's character" (Jeanes, 2019)	(5.3.3) (Existing) (Personality) (304)	(5.3.3.1) (Existing) (Attitudes) (135)	*"You know, on a certain level, I am not that important for anyone, to want to take my data" (Respondent_10)*	Attitudes are a construct of how an individual perceives something.	

Overarching concept	Conceptual node	Dictionary Definition of concept	Core code definition	(Section ID) (New/ Existing code) (Code Text) (Code Reference hits)	Quote(s) backing concept		Summary of code in study context	Literature on concept
		A habit is "something that you do often and regularly, sometimes without knowing that you are doing it" (*Cambridge English Dictionary*, n.d.)			(5.3.3.2) (Existing) (Habits) (110)	*"No, no unless if they are enforced, if I remember, but otherwise I do not explicitly adhere" (Respondent_1)*	Routine subconscious actions carried out by an individual.	
			"Anxiety is an emotion characterised by feelings of tension, worried thoughts and physical changes like increased blood pressure" (American Psychological Association, n.d.)		(5.3.3.3) (Existing) (Anxiety) (59)	*"I have generally never thought of it, hearing you say that actually makes me a bit anxious" (Respondent_5)* *"I keep thinking that the worst that could happen is people find out my name and maybe a little about my personal*	*The feeling of unease regarding use of IoT devices.*	

Overarching concept	Conceptual node	Dictionary Definition of concept	Core code definition	(Section ID) (New/ Existing code) (Code Text) (Code Reference hits)	Quote(s) backing concept	Summary of code in study context	Literature on concept
					preferences" (Respondent_7)		
			Belief that somebody/something is sincere and has no intention of harm or trickery" (Cambridge English Dictionary, n.d.)	(5.3.4) (Existing) (Trust) (51)	*"I do not check those I just kind of trust the vendor implicitly" (Respondent_1)*	The individual quality of honesty, safety and reliability related feelings accorded to third parties.	
		Fear is "an unpleasant emotion or thought that you have when you are frightened or worried by something dangerous, painful, or bad that is happening or	*"The bad feeling that you have when you are in danger or when a particular thing frightens you" (Cambridge English Dictionary, n.d.)*	(5.3.5) (Existing) (Fear) (34)	*"I think the issue that I am most uncomfortable with these devices is, some of these devices have the ability to record sound" (Respondent_7)*	Fear is the emotion brought about by freight or worry towards a situation.	

Overarching concept	Conceptual node	Dictionary Definition of concept	Core code definition	(Section ID) (New/ Existing code) (Code Text) (Code Reference hits)	Quote(s) backing concept	Summary of code in study context	Literature on concept
		might happen" (Cambridge English Dictionary, n.d.)					
5.4 Rules	Rules and regulations awareness	*Rule – "a guideline or standard that is used to guide responses or behaviour or that communicates situational norms"* (American Psychological Association, n.d.) *Regulation- "an official rule or the act of controlling something"*	*Documentation set aside for purposes of protecting user privacy.*	(5.4.2) (Existing) (Privacy policies, Terms and Conditions) (110)	*"It should be much shorter, uhm there should not be a lot of technical jargon, because that definitely puts some of us off!" (Respondent_2)* *"It is also written in jargon so even if you read the whole thing, you do not understand it" (Respondent_7)*	Rules consist of terms and conditions, legislation from the Government, privacy policies from device manufacturers and this theme analyses awareness of the "rules".	According to Williams et al. (2018), Regulations reduce perceived risk. This is agreeable to some extent.

Overarching concept	Conceptual node	Dictionary Definition of concept	Core code definition	(Section ID) (New/ Existing code) (Code Text) (Code Reference hits)	Quote(s) backing concept	Summary of code in study context	Literature on concept
		(*Cambridge English Dictionary*, n.d.)					
		"Set of laws suggested by a government" (*Cambridge English Dictionary*, n.d.)	*Knowledge of sets of laws imposed by legislators.*	(5.4.1) (Existing) (Legislation awareness) (37)	*"Yes, so I feel like there are still loopholes that need to be tied up before you can really say that your information is being utilised and only consented by you" (Respondent_10)*		According to Job (2020), awareness is essential to foster adherence.
5.5 Community	Community	*"People who are considered as a unit because of their common interests, social group, or nationality"* (*Cambridge English Dictionary*, n.d.)	*The act of being spied upon or associated paranoia or thought of being surveyed*	(5.5.1) (Existing) (Surveillance and paranoia) (33)	*"The ability to, sort of to do whatever I want, whenever I want and not to be observed or be monitored by anyone, not having my activities being tracked down" (Respondent_3)*	User day-to-day monitoring by a third-party without their consent.	Alsmirat et al. (2017)
			Influences from the surroundings of a user	(5.5.2) (Existing) (Community effect) (46)	*"So, it's more statistical if I am buying something that I know historically people have kind of complained then that will get me a reading" (Respondent_1)*	Impact the community has on a user's decision to adhere.	Atzori et al. (2017)
			"The act of forming opinions about	(5.5.3) (Existing)	*"I think, all information about us is collected, because things*	Exploration of	

Overarching concept	Conceptual node	Dictionary Definition of concept	Core code definition	(Section ID) (New/ Existing code) (Code Text) (Code Reference hits)	Quote(s) backing concept	Summary of code in study context	Literature on concept
			what has happened or what might happen without knowing all the facts" (*Cambridge English Dictionary*, n.d.)	(Speculation) (37)	*like Google, we never log out of our emails… I know that Google does not care about privacy that much" (Respondent_8)*	participants' responses that hint to speculation.	
5.6 Division of Labour	Accountability	*"The fact of being responsible for what you do and able to give a satisfactory reason for it"* (*Cambridge English Dictionary*, n.d.)	*The individuals selected by the population to represent them in the legislature*	(5.6.1) (Existing) (Government policymakers) (1)	*"If the government can do more, then that would be good, I do not know if they have the capability to do more". (Respondent_8)*	Deals with who plays what role when IoT devices are involved.	Ball (2017)
			Government or non-Government originations charged with enforcing legislative mandates	(5.6.2) (Existing) (Government policy enforcers) (2)	*"Yeah, I would, I mean right now, in some cases I do not even bother, it depends on the, the reputation of the company also helps" (Respondent_1)*	Node addressing policy enforcement themes as identified by participants.	
			Select people in the know, who instruct other people	(5.6.3) (Existing) (Educators) (56)	*"I do not want to sound ignorant, but I do not think we are taking the time to educate ourselves" (Respondent_10)*	Coding of Themes addressing instruction of oneself or others	Nelke and Winokur (2020), Chong et al. (2019).

Overarching concept	Conceptual node	Dictionary Definition of concept	Core code definition	(Section ID) (New/ Existing code) (Code Text) (Code Reference hits)	Quote(s) backing concept	Summary of code in study context	Literature on concept
						regarding privacy.	
			Makers of IoT devices and Supporting services' providers	(5.6.4) (Existing) (Service Providers/Device manufacturer) (5)	*"The right to have personal information, kept private... so, in other words for other services or companies not to retain that information when I am interacting on the internet" (Respondent_7)*	Companies involved in service provision and device manufacturing.	Subahi and Theodorakopoulos (2018).
5.7 Object	Adherence	*"The fact of someone behaving exactly according to rules, beliefs, etc.:"* (*Cambridge English Dictionary*, n.d.)	*Not compliant with set out rules*	(5.7.1) (Existing) (Non-adherence) (34)	*"Uhm, I did not do it because it is actually listening to your device every time, so I changed those settings as well." (Respondent_6)*	Code for mentions or hints of non-adherence.	Kuutti (1996), Burtch et al. (2018)
			Associated benefits of following the rules.	(5.7.2) (Existing) (Perceived benefits) (18)	*"Would you like to send anonymous reports about your usage, I say yes, I mean, if it is going to help you improve this free thing that I am getting then sure" (Respondent_1)*	Coding of participants' apparent benefits in adherence/non-adherence.	
6 Unlinked (Contradictions)	Unlinked	*The unconnected items.*		(6.3.1) (New) (Health impact) (5)	*"I kind of get sceptical on whether you know what I am about to buy this phone is there like a disclaimer on their*	Interview respondent mentions of health-	Kelly et al. (2020). Sicari et al. (2015)

Overarching concept	Conceptual node	Dictionary Definition of concept	Core code definition	(Section ID) (New/ Existing code) (Code Text) (Code Reference hits)	Quote(s) backing concept	Summary of code in study context	Literature on concept
					liability for health" (Respondent_1)	related factors.	
			"Suitable for your purposes and needs and causing the least difficulty" (*Cambridge English Dictionary*, n.d.)	(6.3.2) (New) (Conveniences and necessity) (35)	*"But typically, with the ads, I find it makes my life better, I do not really mind it, I do end up spending a bit more" (Respondent_10)*		Zheng et al. (2018)
					"If I am playing music with Apple music then suddenly, they are recommending music that other people are listening to who listen to music I listen to, I don't mind" (Respondent_1)		

G. Three-year average data costs for select Sub Sahara African countries.

Rank	Country	Plans measured	Average price of 1GB (local currency)	Currency	Conversion rate (USD) (Frozen 23/03/2021)	Average price of 1GB (USD)	Cheapest 1GB for 30 days (USD)	Most expensive 1GB (Local currency)	Average price of 1GB (USD – 2020)	Average price of 1GB (USD – 2019)
5	Sudan	33	104.00	SDG	0.00	$0.27	$0.03	350.25	$0.63	$0.68
22	Somalia	27	0.60	USD	1.00	$0.60	$0.18	6.67	$0.50	$6.19
27	Ghana	34	3.82	GHS	0.17	$0.66	$0.17	20.00	$0.94	$1.56
32	Tanzania	60	1,742.42	TZS	0.00	$0.75	$0.28	10,000.00	$0.73	$3.71
43	Nigeria	60	333.33	NGN	0.00	$0.88	$0.03	2,000.00	$1.39	$7.91
48	Cameroon	44	500.00	XAF	0.00	$0.90	$0.60	4,000.00	$2.75	$1.71
50	Senegal	35	520.00	XOF	0.00	$0.94	$0.30	3,333.33	$3.30	$3.28
62	Zambia	60	16.67	ZMW	0.07	$1.13	$0.01	100.00	$1.36	$2.25
69	Rwanda	47	1,133.33	RWF	0.00	$1.25	$0.35	21,000.00	$1.48	$3.79
71	Niger	22	709.60	XOF	0.00	$1.28	$0.47	6,666.67	$3.30	$25.52
86	Uganda	60	5,732.14	UGX	0.00	$1.56	$0.45	83,333.33	$1.62	$5.02
89	Angola	20	1,000.00	AOA	0.00	$1.61	$1.03	2,000.00	$5.29	$7.95
105	Guinea	19	20,000.00	GNF	0.00	$1.99	$0.79	50,000.00	$2.08	$4.53
109	Burundi	54	4,100.00	BIF	0.00	$2.10	$0.09	10,000.00	$2.12	$18.79
117	Eswatini	9	33.33	SZL	0.07	$2.24	$0.69	41.67	$13.31	$5.25
118	Kenya	50	247.07	KES	0.01	$2.25	$0.26	1,200.00	$1.05	$2.73
130	Côte d'Ivoire	29	1,428.43	XOF	0.00	$2.58	$1.17	10,000.00	$3.20	$6.18
131	Liberia	40	2.59	USD	1.00	$2.59	$1.55	20.00	$3.25	$3.75
135	Lesotho	27	39.33	LSL	0.07	$2.66	$1.29	133.33	$2.13	$7.19
136	**South Africa**	**60**	**39.47**	**ZAR**	**0.07**	**$2.67**	**$0.12**	**516.00**	**$4.30**	**$7.77**
140	Mozambique	19	200.00	MZN	0.01	$2.79	$0.19	500.00	$3.33	$12.82
150	Comoros	25	1,333.33	KMF	0.00	$3.21	$0.60	40,000.00	$4.38	$5.27
152	Sierra Leone	21	33,333.33	SLL	0.00	$3.26	$2.17	45,000.00	$3.69	$9.22
153	Mali	42	1,816.67	XOF	0.00	$3.28	$1.20	94,000.00	$4.12	$12.37
162	Benin	37	2,000.00	XOF	0.00	$3.61	$0.45	33,333.33	$27.22	$20.99

Rank	Country	Plans measured	Average price of 1GB (local currency)	Currency	Conversion rate (USD) (Frozen 23/03/2021)	Average price of 1GB (USD)	Cheapest 1GB for 30 days (USD)	Most expensive 1GB (Local currency)	Average price of 1GB (USD – 2020)	Average price of 1GB (USD – 2019)
167	Botswana	30	43.25	BWP	0.09	$3.92	$1.63	400.00	$13.87	$16.79
173	Guinea-Bissau	9	2,441.41	XOF	0.00	$4.41	$2.25	20,000.00	$4.12	$11.71
177	Burkina Faso	31	2,500.00	XOF	0.00	$4.52	$2.35	10,000.00	$2.47	$10.26
179	Togo	18	2,596.15	XOF	0.00	$4.69	$2.03	22,500.00	$4.50	$15.12
181	Cape Verde	24	445.00	CVE	0.01	$4.78	$1.07	4,500.00	$4.81	$4.25
183	Gabon	52	2,666.67	XOF	0.00	$4.82	$1.06	10,000.00	$4.89	$3.39
184	Madagascar	36	19,500.00	MGA	0.00	$5.14	$0.66	190,000.00	$8.81	$7.24
192	Gambia	31	300.00	GMD	0.02	$5.86	$2.37	5,000.00	$5.10	$6.89
212	Seychelles	21	182.86	SCR	0.05	$8.64	$2.36	480.00	$11.43	$19.55
214	Central African Republic	13	5,000.00	XOF	0.00	$9.03	$3.01	33,333.33	$8.25	$6.03
224	Namibia	33	330.56	NAD	0.07	$22.37	$1.20	1,065.00	$4.78	$11.02
225	Chad	15	2,500.00	XAF	0.00	$23.33	$2.21	25,000.00	$23.33	$23.33
226	Malawi	5	20,000.00	MWK	0.00	$25.46	$20.37	20,000.00	$27.41	$3.59
227	São Tomé and Príncipe	16	70.00	STN	0.44	$30.97	$13.27	275.00	$28.26	$5.33

Note. Adapted from https://www.cable.co.uk/mobiles/worldwide-data-pricing/2021/mobile_data_price_comparison_data.xlsx by www.cable.co.uk