

https://dspace.org/

Individual intentions to share personal information online: an extension of the protection motivation theory model

Arthur, Kojo

2020
https://hdl.handle.net/10539/31449

Downloaded from a DSpace repository. https://dspace.org/



Individual Intentions to Share Personal Information Online:

An Extension of the Protection Motivation Theory Model

Submitted by:
Kojo Arthur
0609564k

Proposed Supervisor:
Professor Jason Cohen

Date: 19 August 2020

PLAGIARISM DECLARATION

I declare that this is my own unaided work and is, to the best of my knowledge and belief, original, except as acknowledged in the text.

I have read and understood the Senate policy on plagiarism and am aware that plagiarism is the intentional or unintentional "failure to acknowledge the ideas or writing of another" or "presentation of the ideas or writing of another as one's own". In this context "others" means any other person including a student, academic, professional, published author or other resource such as the internet. Failing to acknowledge the use of ideas of others constitutes an important breach of the values and conventions of the academic enterprise.

I am aware that plagiarism offences will be dealt with in terms of the Senate policy and may be subject to disciplinary action (which can result in dismissal from the course).

I have appended a reference list of citations used in this essay/assignment.

Signed:



Date: 19 August 2020

ABSTRACT

The internet has become part of modern everyday life. People are increasingly using the internet for business, social and other aspects of their lives. Use of the Internet in the modern context, however, requires sharing of some personal information (PI) online. To enjoy the benefits of online use, some individuals may be willing to share their PI regardless of the risks. Others, however, may be reluctant to share their PI online due to the threats and potential harm that may be caused by improper handling and use of PI. Information systems (IS) researchers have thus been interested in exploring the factors that influence individual intentions to share PI online.

This paper's contribution to IS privacy research is in the form of an enhanced Protection Motivation Theory (PMT) model by adopting and extending Rogers' (1975) Protection Motivation Theory (PMT) model to include elements of trust and risk, and by addressing the research question "*What Factors Affect Individual Intentions to Share PI Online*?". By answering the research question, this report has resulted in an increased understanding of factors that relate to individuals' information privacy concerns and their intended behaviours when considering the use of online services. The study also contributed to IS privacy research by adding to the literature on the privacy concept and information privacy concerns in South Africa. This study has provided empirical evidence to support practitioners by helping them acknowledge that as their services become more personalised, individual intentions to share their PI online is linked to their concerns for privacy and ultimately their intentions to use such services.

This study was informed by the positivist paradigm as it proceeded deductively to develop and test the relationships that make up the conceptual framework of the study. Considering that this study was based on advances in technology used for commercial and governmental services as well as social interactions that are driven by personalisation, this study used a self-administered online survey questionnaire to gather data to measure the proposed conceptual model's variables. The questionnaire was developed in eSurveyCreator and distributed to the study's research sample population through emails and Facebook and WhatsApp social media platforms. The useable sample consisted of 152 South African Internet users with access to email, Facebook or WhatsApp. The study contributed by showing the efficiency of online survey questionnaire distribution techniques through social media platforms to reach sample populations.

Limitations to internal validity and generalizability were acknowledged, and these arise from the studies context, the research population and the idea that factors such as social awareness and internet literacy found to be mediating factors for concerns for privacy by other research was not considered in the scope of this study. This meant that the lack of temporal precedence in the data collected could lead to causal inferences, and any causal assumptions that readers wanted to make should be concerning relevant literature and theory.

Results of the study's demographic analysis highlighted that the respondents were predominantly employed males between the ages of 25 to 35 living in the Gauteng region of South Africa. Furthermore, principal component analysis of the study's measurement instruments confirmed the validity and the reliability of the study's construct items. Correlation and regression analysis to test and show the strength, as well as direction of relationships between the conceptual model constructs, was also performed. The results revealed that seven out of eight of the paper's hypothesis were supported (H1 and H3 to H8) and one was rejected (H2).

The study closed off by highlighting its contributions. With the most significant factors affecting privacy concerns being those related to threat appraisal processes: that is, perceived vulnerability and perceived severity. Another factor, not PMT related that was found to be a significant antecedent to privacy concerns was perceived online risk. The study concluded by giving some suggestions for future research. In general, it was suggested that while PMT is an established theory that has been adopted

to study privacy concerns, there might be an opportunity to extend PMT by looking at other behavioural models, especially those that include fear or concern related factors such as risk and trust.

Key Words and Phrases: Concern for Privacy, Information Privacy, Protection Motivation Theory.

DEDICATION

This thesis is dedicated to my wife Tshegofatso who has been a constant source of support and encouragement during this undertaking. This work is also dedicated to my daughter who inspires me to work hard for the things I want to achieve.

ACKNOWLEDGEMENT

I am grateful to God for the good health and wellbeing that was needed to complete this work. I would like to thank my parents for their love and support throughout my life. They have given me the strength to aspire for more. My brothers, Kweku and Nana, deserve my wholehearted thanks as well for their advice during the challenges of completing this work. I would also like to express my sincere gratitude to my supervisor Prof. Jason Cohen at Wits for his continuous support, guidance, patience and motivation.

Contents

PLAGIARISM DECLARATION I

ABSTRACT II

DEDICATION IV

ACKNOWLEDGEMENT IV

LIST OF TABLES VII

LIST OF FIGURES VIII

1. INTRODUCTION 1

1.1. BACKGROUND 1
1.2. PROBLEM STATEMENT 2
1.3. PURPOSE OF THE STUDY 3
1.4. INTENDED CONTRIBUTION OF THE STUDY 4
1.5. DELIMITATIONS OF THE STUDY 5
1.6. CONCLUSION 5

2. LITERATURE REVIEW 7

2.1. THE PRIVACY CONCEPT 7
2.2. REVIEW OF INFORMATION PRIVACY LITERATURE 13
2.3. CONCLUSION 23

3. THEORETICAL BACKGROUND AND RESEARCH MODEL 24

3.1. PROTECTION MOTIVATION THEORY 24
3.2. CONCEPTUAL MODEL 27
3.3. CONCLUSION 31

4. RESEARCH METHODOLOGY 32

4.1. RESEARCH PARADIGM 32
4.2. SURVEY DESIGN AND SAMPLING 33
4.3. OPERATIONALISATION 34
4.4. PRE- AND PILOT TESTING 38

4.5. **Data Analysis Methods** 38
4.6. **Ethical Considerations** 39
4.7. **Internal and External Validity** 40
4.8. **Conclusion** 41

5. DATA HANDLING AND CLEANING 42

5.1. **Analysis** 42
5.2. **Conclusion** 43

6. RESULTS 44

6.1. **Demographic Analysis** 44
6.2. **Analysis of the Measurement Instrument** 46
6.3. **Hypothesis Testing and Analysis of the Research Model** 55
6.4. **Conclusion** 67

7. DISCUSSION 68

8. CONCLUSION 72

8.1. **Overview of Results** 72
8.2. **Contributions** 73
8.3. **Limitations of Study** 73
8.4. **Suggestions for Future Research** 74
8.5. **Conclusion** 74

APPENDIX A 92

APPENDIX B 101

APPENDIX C 102

LIST OF TABLES

Table 1: Comparison of POPIA and FIPS Principles 9

Table 2: Concern for Privacy Publications Since 2010 15

Table 3: Summary Key Concepts Identified by IS Research on Privacy 19

Table 4: Summary Conceptual Model Factors and Example Measurements 36

Table 5: Survey Response and Completion 42

Table 6: Respondent Demography 44

Table 7: Respondent Demography Types of Online Accounts 45

Table 8: KMO and Bartlett's Test Results 46

Table 9: Second PCA Run Results 46

Table 10: PCA Communalities 47

Table 11: PCA Total Variance Explained 49

Table 12: PCA Rotated Correlation Matrix 50

Table 13: Summary of Measurement Items following PCA and Construct Reliability Tests 52

Table 14: Descriptive Statistics of Composite Scores for Variables 54

Table 15: Moderator Model Summary 62

Table 16: Moderator Model Coefficients 63

Table 17: Correlation Strength of Relationships Between H3, H5, H6 and H7 on Concern for Privacy 65

Table 18: Coefficient Strength of Relationships Between H3, H5, H6 and H7 on Concern for Privacy 66

Table 19: Summary of Hypothesis Results 67

LIST OF FIGURES

Figure 1: National Comprehensive Data Protection or Privacy Laws and Bills in 2019 10

Figure 2: POPIA Compared to Privacy Laws in 14 African Countries 11

Figure 3: POPIA Compared to Privacy Laws in Selected non-African Countries 12

Figure 4: Graph Depicting Countries Where Most Privacy Concern Publications Originate 14

Figure 5: Graph Showing Concern for Privacy Publications Since 2010 16

Figure 6: Illustration of the PMT Model 25

Figure 7: Application of the PMT Model in Information Security Research 26

Figure 8: PMT Illustration of Trust as Moderator Between Privacy Concern and Self-Disclosure 26

Figure 9: The Study's Proposed Conceptual Model 27

Figure 10: Scatterplot Graph for Privacy and Intention to Share PI Online 56

Figure 11: Scatterplot Graph for Perceived Online Risk and Concern for Privacy 57

Figure 12: Scatterplot Graph for Perceived Online Risk and Online Trust 58

Figure 13: Scatterplot Graph for Perceived Vulnerability and Concern for Privacy 59

Figure 14: Scatterplot Graph for Perceived Severity and Concern for Privacy 60

Figure 15: Scatterplot Graph for Self-Efficacy and Concern for Privacy 61

Figure 16: Summary of Conceptual Model 63

1. Introduction

This chapter will outline the context of this research paper and study through an overview of the concept of privacy as well as give a summary of the generally accepted information privacy principles. The chapter will highlight some of the reasons why information privacy has become topical and a subject of research lately. The study's problem statement, as well as purpose, will also be explained. The chapter will also highlight the study's intended contributions to information privacy research and practitioners in general, and close with an outline of the boundaries within which this study will be performed.

1.1. Background

The concept of information privacy referred to as privacy in this paper, is defined by researchers as any interest that people have in controlling any personal information (PI) about themselves (Clarke, 1999). The definition for PI according to South Africa's Protection of Personal Information Act No.4 of 2013 (POPIA), includes personally identifiable information relating to specific individuals, such as personal details (i.e. name, surname, marital status, etc.), biometric information, location information, unique identifiers, correspondence or opinions about the individual. Advances in information technology along with the growing use of the Internet for most aspects of modern life necessitates the need that individuals share their PI online (Bélanger & Crossler, 2011; Youn, 2009; Zhang & McDowell, 2009). Governments and businesses have taken advantage of such advances in information technology to personalise and improve the services they offer, and in some cases to build competitive advantage. As such, recently individuals' PI has been considered as a driving force and critical asset for service delivery in the case of governments and customer service in the case of businesses (Alashoor et al., 2017; Dinev & Hart, 2005, 2006). Researchers are beginning to state that this has the effect of governments and businesses exercising significant influence over the behaviour of individuals (Bélanger & Crossler, 2011), and societies have been worried about the indiscriminate collection of voluminous amounts of their PI. Governments and businesses in a matter of seconds can collect large amounts of PI such as location, name, email, preferences, movements, etc., about their customers online either automatically through computer programs called cookies or manually through online forms (H. Chen et al., 2016).

Research shows that this has resulted in increased privacy concerns amongst online users (Bélanger & Crossler, 2011; Youn, 2009; Zhang & McDowell, 2009). Organisations in today's data-driven economy can build profiles of individuals through PI that is provided by these individuals manually or automatically (Alashoor *et al.*, 2017; Chen *et al.*, 2016; Gao, Li & Luo, 2015; Warkentin, Goel & Menard, 2017). PI may be collected manually through online forms and automatically through programs and other mechanisms such as website visits, shares, likes, etc. Often these profiles can be looked up by other individuals, and other organisations such as credit bureaus, banks, insurance companies and marketers (Alashoor *et al.*, 2017; Gao *et al.*, 2015). Similarly, when such PI leaks into the hands of unauthorised third-parties, including criminals or those with malicious intent, then individuals can suffer from crimes related to identity theft such as fraud, physical harm from stalkers or robbers, embarrassment and/or other threats (Alashoor *et al.*, 2017; Chen *et al.*, 2016; Clarke, 1999). Studies reveal that few privacy-related regulations and organisation policies sufficiently protect individuals from harms resulting from the breach of PI (Alashoor *et al.*, 2017; Chen *et al.*, 2016; Gao *et al.*, 2015; Warkentin *et al.*, 2017). Therefore, one can understand why privacy concerns are on the rise. For example, in 2017 South Africa experienced a privacy breach where approximately 60 million citizens' personal information such as identification numbers, addresses and salary information were exposed to the internet through an insecure real estate company server, leaving affected individuals at risk of identity theft (Fihlani, 2017; Van Niekerk, 2017; Van Zyl, 2017). Other relevant examples include the 17 March 2017 decision by the South African Constitutional Court in the case of Black Sash Trust versus Minister of Social Development and Others (Tlakula, 2017). In that case, the South African Information Regulator was

cited as a respondent in an urgent application brought to the court by a not-for-profit organisation called Black Sash Trust that looked for the court's support to rectify the notion that the PI of grant beneficiaries, mostly indigents, belongs to the South African Social Security Agency (SASSA). The court decided in favour of the regulator and declared that the PI of grant beneficiaries is the property of those beneficiaries and could never belong to someone else (Tlakula, 2017). Another recent case that is related privacy concerns and that is still developing is the 04 to 12 August 2019 case at the Pretoria High Court of South Africa where the Information Regulator was granted an opportunity to intervene as a friend of the court (Grootes, 2019; Maughan, 2019). The case was between the President of South Africa and the country's Public Protector. In the case the regulator deemed it necessary to intervene as she believed that Public Protector triggered some privacy and data protection concerns when the Public Protector relied on the President's PI: that is, private emails and bank statements of various entities, that were used by his 2017 presidential campaign team in a report that was produced by the Public Protector. The report found that the President misled the South African Parliament by not declaring donations made to his 2017 presidential campaign. In this case, the PI concerns found by the South African Information Regulator related to the constitutional implication of the President's PI having been possibly unlawfully obtained by the Public Protector. Regulator felt that it was important to get involved as a friend of the court to make a recommendation and to help the court with decisions that will impact privacy law and its application in future (Grootes, 2019; Maughan, 2019). Also, studies show that privacy concerns have an impact on the adoption of online technology and services (Bélanger & Crossler, 2011; Youn, 2009). Organisations are beginning to realise this and therefore updating their online services with mechanisms such as privacy notices that speak to how customer/individual's data is treated and increased privacy features that allow individuals to pursue protective behaviours such as assessing the risks of sharing PI online before doing so (Alashoor *et al.*, 2017). For example, some companies (mainly those head-quartered in the European Union-EU) sent emails to individuals during May 2018 about updates to their privacy policies as a result of the EU General Data Protection Regulations (GDPR) that came into effect on 25 May 2018 (Griffen, 2018; Sommerlad, 2018). It is therefore not surprising that privacy has recently been a topic of research in the IS literature.

A review of IS literature and research on privacy concerns reveals that studies have generally been based on individual's privacy concerns during their online transactions or compliance with information security policies (LaRose et al., 2008; Lee & Larsen, 2009; Mou et al., 2017). The method of research for these studies has predominantly been survey-based where the demographics have generally covered students from the USA (Mohamed & Ahmad, 2012). This suggests that there remain understudied contexts in which online privacy concerns are important to study. The predominant theory used in past research is the Protection Motivation Theory (PMT). PMT is mainly focused on the following constructs, intention to transact, concern for privacy threat appraisal processes and coping appraisal processes (Mou *et al.*, 2017). One of the reasons for the extensive use of PMT for privacy research is that the concept of privacy includes individual psychological factors such as trust and fear, which can be accommodated in PMT research, and these behaviours mediate individual intentions within an environment, for example, s, the Internet (Conner, Norman, Boer & Seydel, 2005; Anderson & Agarwal, 2010; Bélanger & Crossler, 2011; Dinev & Hart, 2005; Johnston & Warkentin, 2010; Johnston, Warkentin & Siponen, 2015; Pavlou, 2011). PMT is a promising theory from which to continue to explore online privacy-related behaviours.

1.2. Problem Statement

Research reveals that organisations are increasingly using the Internet to provide their services online. As such, this also requires individuals to share some PI and that recently PI has become a critical business enabler. Researchers posit that advances in technology have enabled the pervasiveness of information technologies and systems including the ease at which large amounts of data, including personal information, can be collected has raised awareness about privacy matters (Armstrong, 2014;

Clarke, 2016; Kaisler et al., 2013; Kemp, 2014). Furthermore, the occurrence of the recent concept of "the information economy" through which organisations have benefited from having individuals' PI has raised concerns around privacy (Anic et al., 2016). In some cases, PI is collected, aggregated and matched from various data sources to create insights so that organisation can provide their customers personalised offerings, targeted marketing campaigns and realised efficiencies in business operations (Anagnostopoulos et al., 2015; Greengard, 2014; Hussain et al., 2015; Pasluosta et al., 2015). Research shows that understanding privacy issues nowadays as well as the privacy concerns people have. Also, privacy is associated with individual's liberty and the right to pursue their way of life and views within the boundaries of the law (Clarke, 2016; Nussbaum, 2001; Prothro & Grigg, 1960). Privacy is also associated with individual's rights to govern themselves, their mental health, the right to control one's PI from errors that can lead to incorrect profiling or bias as well as how an individual is portrayed in public (Albarghouthi et al., 2016; Boyd & Crawford, 2011; *Cathy O'Neil*, 2016; Katal et al., 2013; O'Neil, 2017). Some researchers argue that there are situations where the access and processing of individuals' PI could be used as a form of social control. Furthermore, there are examples of such situations when politicians have been found to employ targeted campaigns by using individuals' PI to increase their chances of being voted for by manipulating voters' behaviour (Grassegger and Krogerus, 2017; McLeod, 2016). Recent studies have shown that these techniques have been used successfully by a London based company called Cambridge Analytica to help Donald Trump's online campaign as part of the 2016 US presidential elections and for the UK Brexit campaign (Grassegger and Krogerus, 2017; McLeod, 2016). In some cases, privacy issues have been classified as concerns that deal with consumer protection (Anic et al., 2016). Research suggests that individuals' privacy concerns impact on their intentions to share PI online, and that individuals may be more willing to share their PI with online services that they trust and where risk perceptions are lowest (Anderson & Agarwal, 2010; Conner *et al.*, 2005; Dinev & Hart, 2005; Johnston & Warkentin, 2010; Johnston, *et al.*, 2015; Pavlou, 2011).

Considering the context outlined previously, researchers and practitioners must understand privacy concerns to manage the harmful or unintended effects of its improper collection, processing and use. Within the context of the "information economy" as well as the risks around the collection and use of PI, practitioners especially should be interested in what factors that affect individuals' privacy concerns and how this impacts their intentions to share their PI online as this may affect their ability to be competitive, their reputation in the markets and industries that they operate, the trust that consumers, governments and regulators may have in them and their offerings, they may get fines from regulators as well as lose out on the opportunity to improve their organisational practices by complying with relevant privacy laws and standards (Botha et al., 2017). This proposed research study, therefore, aims to answer the question, "*what factors affect individual intentions to share PI online?"*

1.3. Purpose of the Study

This paper attempts to evaluate the factors that affect individuals' privacy concerns and how these impact individuals' intentions to share PI online. These factors are mainly those involved in the threat appraisal and coping appraisal process variables from PMT.

The context of this study is in South Africa where approximately 59% of households have not less than one member who can access the Internet (STATSSA, 2016). Market researchers also estimate that approximately 16 million South Africans use Facebook, this number represents possible a quarter of South Arica's entire population (Staff Writer, 2017; STATSSA, 2016).

This study was conducted in the positivist paradigm as it is ideally suited for testing and explaining the relationships that make up the proposed conceptual framework for this study. Furthermore, the study used a self-administered online survey questionnaire to gather data to measure the proposed conceptual model's variables. The questionnaire was developed in eSurvey Creator and distributed to

the study's research sample population through emails and Facebook and WhatsApp social media platforms to individuals based in South Africa.

1.4. Intended Contribution of the Study

The contribution of this paper will enable IS privacy research by exploring the phenomenon of individuals' privacy concerns and its associated factors. More specifically, this study's contribution is in the form of an enhanced PMT model and subsequently the increased understanding of factors that relate to information privacy concerns of individuals and their intended behaviours when intending to use online services that require them to share their PI.

This paper makes a further theoretical contribution to IS privacy research by understanding the relationship between factors that affect information privacy concerns. It does so by considering the threat and coping appraisal processes that make up the PMT model. Also, this study considers in one conceptual model, the factors that influence concern for privacy, and the elements of trust and risk, where risk is mediated by trust and the relationship between concern for privacy and intention to transact is moderated by trust.

From a practical perspective, the study results will assist those in practice: that is, businesses and government agencies that provide personalised goods and services online, to understand that use of online services and technologies is influenced by individual's concerns about how their PI will be handled as individuals are becoming aware of the negative impacts of improper use of their PI. If organisations that develop online services (social, not-for-profit and for-profit) can better understand the factors that contribute towards earning the confidence and trust of their users, especially where sharing of PI is essential, they can improve adoption of their services.

This study will offer empirical evidence to help practitioners understand that as they offer more personalised services online it is important to acknowledge that individuals' intentions to share their PI online may be a factor that is influenced by their concerns for privacy and subsequently influencing their use of those online services. Also, the study will contribute to the increasing discourse around information privacy concerns, especially in the South African context, which is characterised by increasing connectivity and use of personal information. This paper will contribute to the information privacy research area by clarifying the privacy concept, its elements, and some of the reasons for individual's information privacy concerns, which may be relevant in South Africa and globally. The study will also contribute to information privacy research by showing that it is possible to use recent survey questionnaire distribution techniques, such as online surveys through social media platforms, to reach sample populations. The online survey distribution approach via social media platforms shows that as Internet connectivity increases, the approach makes it convenient for survey participants to take part in relevant studies and collect data effectively for analysis.

Lastly, businesses and governments will benefit from this study by understanding through supporting evidence that they may need to consider tailoring some of their online services to address individuals' concerns for privacy, as this impacts individuals' intentions to use such services. Such tailoring of online services that address privacy concerns may result in improved company performance and sustainability, especially in the digital era and data-driven economy. For example, through empirical evidence organisations may consider the most effective privacy related mechanisms to deploy for their specific type of online service. Such mechanisms may include developing privacy and security guides, tailored privacy notices that speak to how they handle individuals PI, developing secure websites and deploying trust certificates, to name a few.

1.5. Delimitations of the Study

Study of the literature reveals that various models have been used to understand individual intentions to transact or share PI online and that these models have been inspired and mostly based on PMT. These models are generally used to explore and understand individuals' behaviour online and they include Technology Threat Avoidance Theory (TTAT), Fear-Appeals Model (FAM) and Health Belief Model (HBM) (Bélanger & Crossler, 2011; Boss *et al.*, 2015; Cohen, 2017; Conner *et al.*, 2005; Dinev & Hart, 2005; Johnston *et al.*, 2015; Junglas, Johnson & Spitzmüller, 2008; Youn, 2009; Zhang & McDowell, 2009). For this study, only PMT and its relevant constructs will be adopted and extended to give answers to the research question. The scope of this study is limited to a review and synthesis of IS privacy research related to individual privacy concerns and how these can be explained by adopting some PMT concepts such as the intention to transact, concern for privacy, threat appraisal and coping appraisal.

Therefore, factors such as response cost and response efficacy that are frequently used in information security research will not be considered as they are generally relevant for information security and related studies that aim to understand the relationship between response cost, response efficacy and compliance behavioural intentions based on a recommended action (Zhang & McDowell, 2009). Response efficacy relates to individuals' beliefs that recommended actions will have the desired effect, response cost, on the other hand, relates to the amount of effort, time or money an individual believes it will take to carry out a recommended action (Zhang & McDowell, 2009).

The social awareness factor from TTAT theory was not considered for this study. This study considered the FAM variables and concepts relevant to privacy rather than IS security more broadly (Y. Chen & Zahedi, 2016; Herath & Rao, 2009; Kolkowska et al., 2017; Yazdanmehr & Wang, 2016; Yoon et al., 2012). This will include perceived threat severity, perceived self-efficacy and behavioural intention.

Also, this study will focus on individuals' intentions to share PI in cases where they are aware that the sharing of PI must make use of an online platform. The PI referred to could be any form of personally identifiable information whether it is collected manually through website forms or tracking technologies such as website cookies.

The limitations, threats to internal validity and generalisability issues faced by the results of the proposed study are explained in chapter four and five of this paper. This includes limitations arising from the context in which the study was performed and the research population.

1.6. Conclusion

This chapter gave a background on privacy concepts and compared their definitions of privacy in literature and law such as contained in South Africa's POPIA. Privacy was defined as any interest that an individual has in controlling or at least significantly influencing any PI about themselves. PI examples such as personal details, biometric information, location information, unique identifiers, correspondence or opinions about the individual were highlighted. The chapter also explained that technology innovations and growing use of the Internet makes it necessary for individuals to share their PI on the Internet resulting in increased privacy concerns. Recent cases of interference in political systems and increases in Internet crimes such as identity theft and fraud were cited as some examples that gave rise to privacy concerns. Based on the above, the study's problem statement was developed to bring to the fore the importance of understanding privacy concerns to manage the harmful or unintended effects of its improper collection, processing and use of individuals' PI. Therefore, this chapter explained that the study will evaluate the factors that affect individuals' privacy concerns and how they affect individuals' intentions to share PI online. The intended contribution of this study to IS literature and practitioners was highlighted as the exploration of factors that affect privacy concerns through the development of an enhanced PMT model. The next chapter will provide a detailed explanation of the

history of the information privacy concept as well as its principles and reviews the available literature on the topic.

2. Literature Review

This chapter explains the concept of privacy in detail, including its history, relevant laws from inception in the United States of America (U.S.A) and those in the South African context, standards as well as the various principles that make up the privacy concept. The chapter also explains how advances in information technology: that is, pervasive and invasive technology, enabled development of the theory of information privacy. The impacts, risks and issues of information privacy are highlighted and explained in this chapter. Findings, themes and outcomes of earlier information privacy literature, including past conceptual models and theories used in privacy literature are presented.

2.1. The Privacy Concept

Advances in technologies such as database management systems (DBMS) has made it easier to collect, aggregate, store and process individuals' PI (Bélanger & Crossler, 2011). During its early days, these DBMS capabilities elevated general awareness about the negative consequences of the extensive collection, aggregation, storage and processing of PI, and so laws and related guidelines were put in place to protect individuals from abuse, crimes and other harm related to improper handling of PI (Bélanger & Crossler, 2011; Smith, Dinev & Xu, 2011; Smith, Milberg & Burke, 1996). Some of these laws include the 1974 U.S.A Privacy Law and the Organisation for Economic Corporation and Development's (OECD) Fair Information Privacy Principles (Smith *et al.*, 2011; Smith *et al.*, 1996).

Early understanding of privacy was based on the idea that privacy is a right that applies to all individuals, and that this right to privacy ultimately has an influence on the physical and/or psychological well-being of individuals (Warren & Brandeis, 1890). Over the years further research covering the concept of privacy resulted in the development of the following four generally accepted categories of privacy. They are the physical privacy of an individual, privacy related to personal behaviour, communication as well as personal information privacy (Bélanger & Crossler, 2011; Smith *et al.*, 2011; Smith *et al.*, 1996). Out of these four generally accepted categories of privacy, this study will focus on communication privacy and personal data privacy as this study is based on exploring "*factors that influence individuals' intentions to share PI online*". To do so this study will combine and use communication and personal data privacy as these are the categories most affected by the sharing of PI online in the modern context (Bélanger & Crossler, 2011; Smith *et al.*, 2011; Smith *et al.*, 1996). For this study, the above-mentioned two categories will be combined and discussed as **information privacy** or used a reference for the concept of privacy in keeping with the practice adopted by most IS privacy researchers for similar studies (Bélanger & Crossler, 2011; Smith *et al.*, 2011; Smith *et al.*, 1996).

Privacy principles are generally based on similar elements, namely, collection, unauthorised secondary use, improper access and information quality (Clarke, 1999; Junglas, Johnson & Spitzmuller, 2008). These privacy elements are largely derived from the 1980 OECD eight fair information principles (FIPS) (Smith *et al.*, 2011; Smith *et al.*, 1996).

OECD FIPS principles have formed the basis for several modern privacy laws worldwide, including, South Africa's Protection of Personal Information (POPIA) Act No.4 of 2013. POPIA defines PI personally identifiable information, such as personal details: that is, name, surname, marital status, etc., biometric information, location information, unique identifiers, correspondence or opinions about the individual (Botha, Grobler, Hahn & Eloff, 2017; Republic of South Africa the Presidency, 2013). Following on from that, privacy is defined by researchers as the individual's interests in their ability to control or at least significantly influence how their PI is treated by others (Bélanger & Crossler, 2011; Youn, 2009).

The Protection of Personal Information Act, 4 of 2013 (POPIA) is an Act of the South African Parliament (Protection of Personal Information Act No. 4 of 2013 (POPIA), 2013). It was passed in 2013 and currently, the entire Act is not effective (Commencement of Section 1, Part A of Chapter 5 and Sections

112 And 113 of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013), 2014). Only section 1, Part A of chapter 5 and sections 112 and 113 are effective, and these sections deal with the establishment of an information regulator and the regulator's powers (Commencement of Section 1, Part A of Chapter 5 and Sections 112 And 113 of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013), 2014). Parts of the Act that are enforced allow for the instalment of an Information Regulator and their office.

Two key legislations in South Africa enable POPIA, they are the South African Constitution and the Promotion of Access to Information Act, 2 of 2000 (PAIA) (Botha et al., 2017; Constitution of The Republic of South Africa No. 108 of 1996, 1996; Promotion of Access to Information Act 2 Of 2000, 2000; Protection of Personal Information Act No. 4 of 2013 (POPIA), 2013; Reddy, 2012). Section 14 and 32 of the Bill of Rights in the Constitution speaks to the rights to privacy and access of information, respectively (Botha et al., 2017; Fichet, 2015; Promotion of Access to Information Act 2 Of 2000, 2000; Reddy, 2012). POPIA deals with the privacy rights whilst PAIA deals with information access and establishes rules on how PI can be accessed and collected, how much of it can be collected, the accuracy of collected PI, how it can be used and shared, where it can be shared, how it should be protected and how it should be destroyed or changed (Botha et al., 2017; Fichet, 2015; Reddy, 2012; Protection of Personal Information Act No. 4 of 2013 (POPIA), 2013). Other laws that apply to privacy and should be read in conjunction with are the Electronic Communications and Transactions Act, 25 of 2002 (ECTA), which is South African legislation that has provisions: that is, sections 50 and 51, related to the protection of personal information obtained through electronic means. The second applicable legislation is the European Union General Data Protection Regulation (GDPR). This piece of legislation is like POPIA and came into force on 25 May 2018. GDPR binds all entities handling the PI of people living in the EU, regardless of which country the entities run from (Botha et al., 2017; Lund, 2019).

POPIA has also stated some key definitions that essential for the application of the Act, these are **Processing**, which means the collection, use, storage, modification, destruction, aggregation, and distribution of PI; **Data Subject**, which means an individual whom a specific PI relates to; **Responsible Party**, means an individual or entity that processes PI; **Operator**, an individual or entity contracted to process PI on for a Responsible Party; **Public Record**, a record that is in the public domain or is being kept or controlled by a public entity; and **Unique Identifier** means an identifier that is issued by a Responsible Party and assigned to a Data Subject for the privacy purposes of the Responsible Party's operations (Protection of Personal Information Act No. 4 of 2013 (POPIA), 2013).

Under the current enforceable POPIA laws the Information Regulator will have powers to investigate responsible parties, settle complaints, make request for people to give evidence in court, request individuals to give evidence or provide information that would be necessary for investigations in the same way that a South African High Court would, perform premises searches and do interviews (Botha et al., 2017; Protection of Personal Information Act No. 4 of 2013 (POPIA), 2013). The information regulator will also have powers to confiscate equipment and other tools that are used to process PI, and require that responsible parties should provide information about how they process PI (Botha et al., 2017; Protection of Personal Information Act No. 4 of 2013 (POPIA), 2013).

POPIA's principles are highlighted below (Botha et al., 2017; Smith et al., 1996, 2011). As they are based on the OECD's FIPS principles, **Table 1** below highlights the similarities between the POPIA the OECD's eight privacy principles:

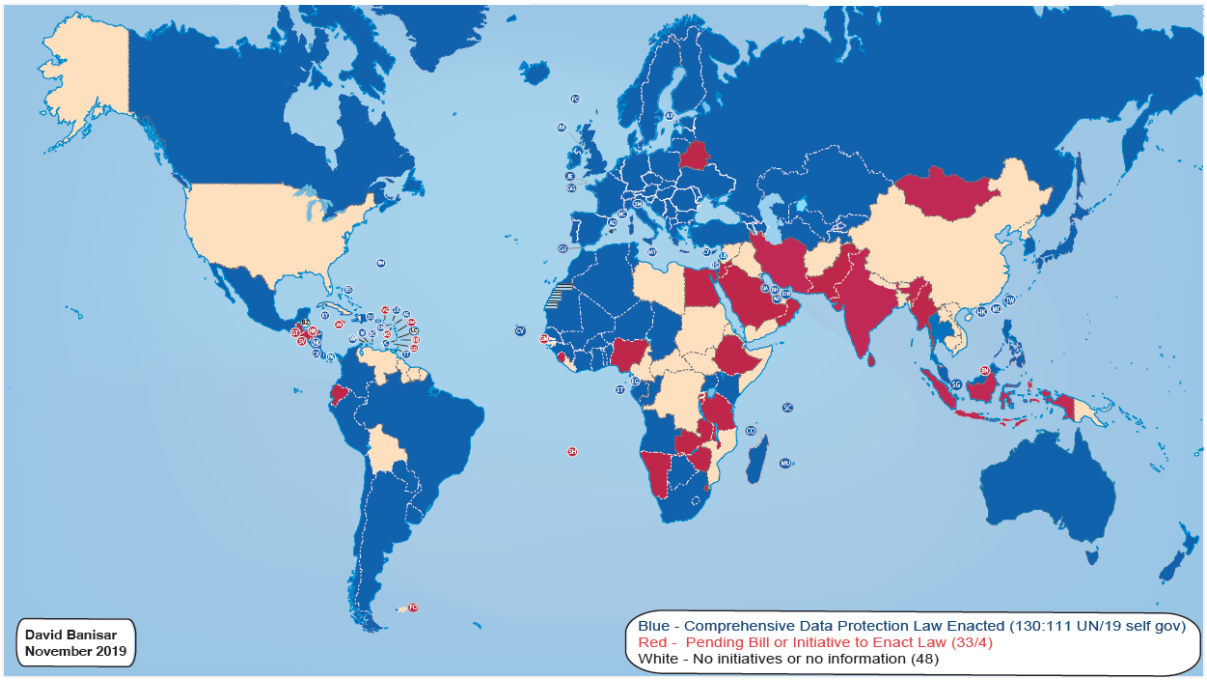
Table 1: Comparison of POPIA and FIPS Principles

OECD FIPS Principles	POPIA Principles	Requirement Description
Accountability	**Accountability**	Entities that collect or use individuals PI are accountable for following any laws related to the protection of PI.
Collection Limitation	**Processing Limitation**	PI should only be collected and used where consent has been obtained from individuals and where collection or use is lawful.
Purpose Specification	**Purpose Specification**	Use of individuals' PI should be in line with the purposes for which it was initially collected.
Use Limitation	**Further Processing Limitation**	Consent needs to be obtained from individuals for further use of the use of their PI than what it was initially collected for.
Data Quality	**Information Quality**	Collection of PI from individuals should be for a specific purpose and that the PI collected and used should be correct, updated and complete.
Openness	**Openness**	Organisations should be open about how individuals' PI will be treated.
Security Safeguards	**Security Safeguards**	PI should be kept safe by generally accepted security standards.
Individual Participation	**Data Subject Participation**	Individuals should be able to access data about themselves and make changes where needed.

There are other key requirements highlighted by POPIA in addition to its eight key principles. POPIA has additional rules for cross-border transfer of PI: that is, PI can only be transferred cross-border in cases where there is consent from individual owners of the PI and where privacy laws are similar to that of South Africa or better, direct marketing, combining separate sets of PI: that is, data-matching and aggregation, the use of biometrics, automated decision-making and some administrative requirements (Botha et al., 2017; Fichet, 2015). Essentially, POPIA's goals are to promote the protection of PI in public and private organisations, define key requirements to process PI, provide for an Information Regulator, the publishing of codes of conduct around unwelcomed electronic communications and decisions that are made via automated means as well as manage the sending of personal information to other countries outside South Africa (Botha et al., 2017; Fichet, 2015).

A high-level comparison of POPIA against other privacy legislation worldwide was performed by Botha et al (2017). The study discovered that internationally there are over 100 countries as well as autonomous sovereignties and territories that have adopted extensive information privacy or data protection laws to protect individuals' PI help by those states and other organisations (Banisar, 2016). **Figure 1** maps out all regions that have adopted privacy laws and those that are currently focusing on the need: regions highlighted in blue have issued privacy laws and those in red are doing so. For the regions highlighted in white, there are either no pursuits to adopt and privacy laws or there is no information available to verify this.

Figure 1: National Comprehensive Data Protection or Privacy Laws and Bills in 2019



Source: Banisar (2019)

Botha et al (2017) state that 16 African countries have adopted comprehensive information privacy laws. With the adoption of the African Union (AU) Convention on Cyber Security and Personal Data Protection in June 2014 more African countries have been progressing with initiatives to enable privacy laws (Botha et al., 2017; Fichet, 2015). A comparison of POPIA to some African privacy laws highlighted that all the laws included retention requirements in line with the purposes the PI was obtained but, in some cases, retention periods were not defined. Security obligations and the rights of individuals to their PI were enforced, this includes the rights to access, correct and oppose any PI held about them. South Africa was found to have defined accountability as one of its privacy principles which the other African countries had not done (Botha et al., 2017; Fichet, 2015).

For the comparison of the POPIA to non-African privacy laws by Botha et al (2017), countries were selected based on their influence globally and the maturity of their privacy laws. As mentioned in earlier sections the OECD's FIPS is the basis for most privacy laws (Botha et al., 2017; Reddy, 2012). The EU's Data Protection Directive (DPD) was revised to form the GDPR. Like POPIA, the GDPR makes specific provision for child protection whilst the UK has a Data Protection Act (DPA) that has strong protections for more sensitive information such as ethnic background, political opinions, religious beliefs, health, sexual orientation and criminal records (Botha et al., 2017; Reddy, 2012). Canada, the USA and Australia have a mix of privacy laws that cover government departments, private entities and different states but most POPIA principles are covered (Botha et al., 2017; Reddy, 2012).

See **Figure 2 and 3** below for the comparisons of POPIA to selected African and non-African privacy laws

Figure 2: POPIA Compared to Privacy Laws in 14 African Countries

Country	Act	PoPI Principles								Other Areas					
		Accountability	Processing Limitation	Purpose Specification	Further Processing Limitation	Information Quality	Openness	Security Safeguards	Data Subject Participation	DPO Required	Breach Notification	Cross-border Data Transfer Limitations	Electronic Marketing	Online Privacy	Enacted Year
South Africa	PoPI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		2013
Angola	PDL		✓	✓		✓		✓	✓			✓		✓	2011
Benin	PPD		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓		2009
Burkina Faso	PPD		✓	✓		✓		✓	✓			✓			2004
Cape Verde	PPD		✓	✓		✓		✓	✓			✓	✓	✓	2013
Gabon	PPD		✓	✓		✓		✓	✓			✓			2011
Ghana	DPA		✓	✓	✓	✓	✓	✓	✓		✓				2012
Ivory Coast	PPD		✓	✓		✓		✓	✓	✓		✓			2013
Madagascar	PPD		✓	✓		✓		✓	✓	✓		✓			2015
Mali	PPD		✓	✓		✓		✓	✓			✓			2013
Mauritius	DPA		✓	✓	✓	✓	✓	✓	✓			✓			2004
Morocco	PIRP PD		✓	✓		✓		✓	✓			✓	✓		2009
Senegal	PPD		✓	✓		✓		✓	✓			✓			2008
Seychelles	DPA		✓	✓	✓	✓	✓	✓	✓			✓			2003
Tunisia	DPA		✓	✓	✓	✓	✓	✓	✓	✓		✓			2004

Source: Botha et al. (2017)

Figure 3: POPIA Compared to Privacy Laws in Selected non-African Countries

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

* This row was not populated with a single act as the USA has a variety of privacy legislation.

Source: Botha et al. (2017)

Botha et al (2017) posit that the protection and management of data as well as PI have become an important part of conducting business in recent times. Information privacy has also become a serious consideration for regulators, legislators and consumers across the world. The South African government's objective for POPIA was manage privacy in line with similar international laws as well as stimulate business and manage the cross-border transfer of PI (Botha et al., 2017; Reddy, 2012). Privacy laws and requirements help to protect citizen's constitutional right to privacy by giving them better control over their PI, it also forces organisations to safeguard individual's which in helps protect individuals from various types of crime such as identity theft that can lead to fraud, robberies, kidnapping, murder, etc. According to the 2019 Symantec Internet Security Threat Report (ISTR), South Africa ranked as the top 10 attack victims globally for cybercrimes such as email phishing and ransomware, surpassed by countries such as Saudi Arabia, Norway, Netherlands, Japan, China and the USA (O'Gorman et al., 2019). Looking at the statistics for cybercrime the high rates for reported cybercrimes call for enforcement of information privacy laws as well as ensuring compliance and awareness (Botha et al., 2017).

However, cybercrime and other types of crime should not be the only reason for enacting privacy laws to protect individuals PI. Compliance to POPIA has significant consequences for organisations that do not responsibly conduct themselves when it comes to the proper handling of individuals PI in terms of the law (Botha et al., 2017; Reddy, 2012; Protection of Personal Information Act No. 4 of 2013 (POPIA), 2013). POPIA dictates some organisational changes such as the installation of an Information Officer and generally accepted security practices if these are not in place already. For organisations not compliant with POPIA enforcement notices could prevent the processing of personal information (Botha et al., 2017; Reddy, 2012; Protection of Personal Information Act No. 4 of 2013 (POPIA), 2013). Privacy incidents may cause system shutdowns due to forensic investigations and these incidents may generate negative publicity and damage brands (Botha et al., 2017; Reddy, 2012). Fines up to ZAR 10 million, contractual penalties, lawsuits and even jail time of up to 10 years for an organisations Chief Executive Officer, operational losses, losing customers, loss of future earnings and the inability or reduced ability to compete especially through loss of trust (Botha et al., 2017; Reddy, 2012; Protection of Personal Information Act No. 4 of 2013 (POPIA), 2013). For example, having internationally accepted privacy laws in South Africa helps it do business easier with other countries that have similar laws. Similarly,

organisations can also be fined, have civil lawsuits, criminal lawsuits or have investigations by regulatory agencies which may affect their operations (Botha et al., 2017; Reddy, 2012; Protection of Personal Information Act No. 4 of 2013 (POPIA), 2013).

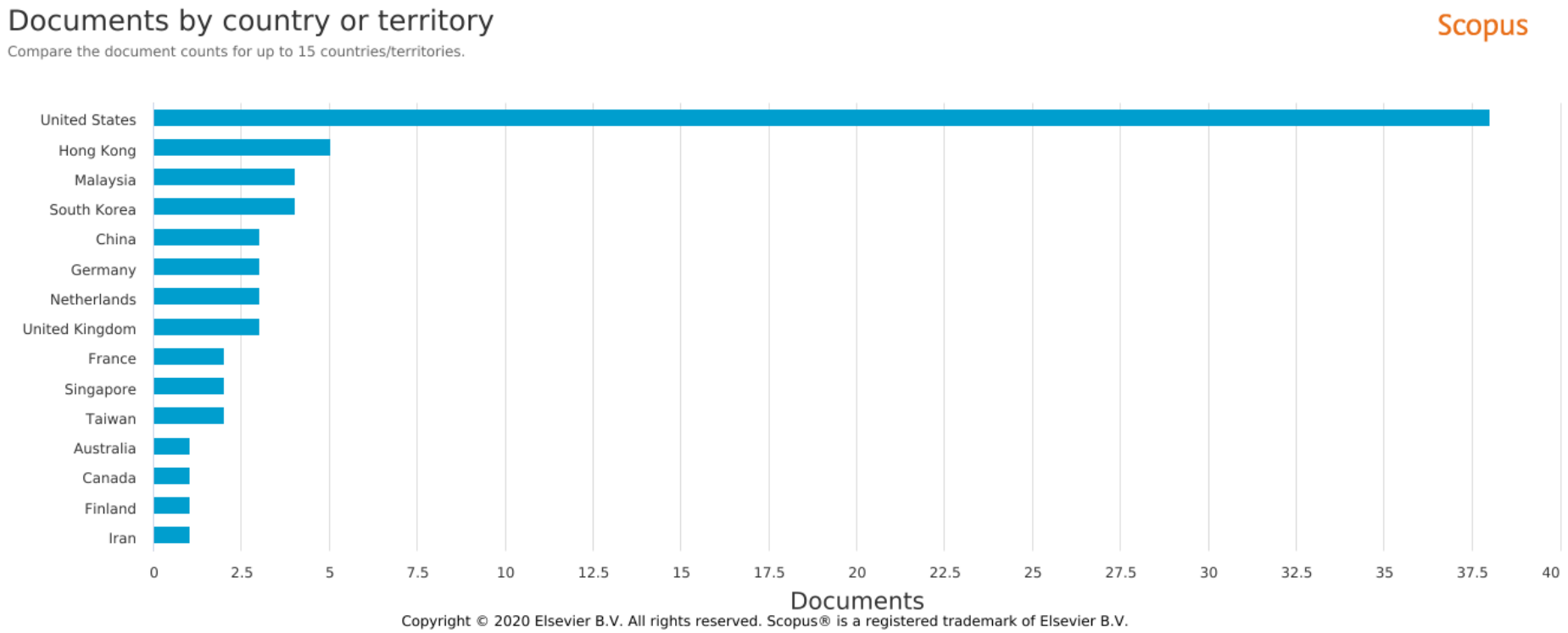
The above discussion has highlighted the way personal data or information and how it should be protected is being considered across countries and through legislative and regulatory instruments. Despite the protection of personal information being regulated, individuals nonetheless experience significant concerns over their personal information, and this has become more prevalent due to Internet penetration. The next section reviews the literature on individual information privacy concerns.

2.2. Review of Information Privacy Literature

A review of information privacy literature was performed to better understand the predominant concepts, factors, contexts, research methods, populations, demographics, variables used and findings of studies on individual privacy concerns.

Searches on well-known research databases such as Scopus, Web of Science, ScienceDirect, ProQuest were performed on IS journals such as the Journal of Management Information Systems (MIS), Communications of the Association for Computing Machinery (ACM) as well as the European Journal of Information Systems. The search query considered peer reviewed IS articles and journals published from 2010 to January 2020. Based on some criteria such as the looking at only journals that have been peer-reviewed and based on the topics or search string “concern” and “privacy”, approximately 57 journals were returned out of which 32 were based on information privacy research that was focused on the concern for privacy construct in the context of the requirement for individuals to share their details online. Gill and Bhattacherjee (2009) state that technology trends are normally attributed to commercial and academic material, and sometimes in areas where the trends have become topics of interest. The focus for commercial publications is normally on profits whilst recognised authors and academics develop academic publications. Baskerville and Myers (2009) also explains that media, consultants and specialists are normally the first one to drive technology trends. As such, the results of the literature search for “privacy” and “concern” as the results returned it would seem that academics from the USA, Hong Kong, Malaysia, South Korea and some EU countries like Germany, Netherlands and France are the main supporters of discussions and publications related to concern for privacy. Figure 4 has been supplied below to explain the phenomenon:

Figure 4: Graph Depicting Countries Where Most Privacy Concern Publications Originate

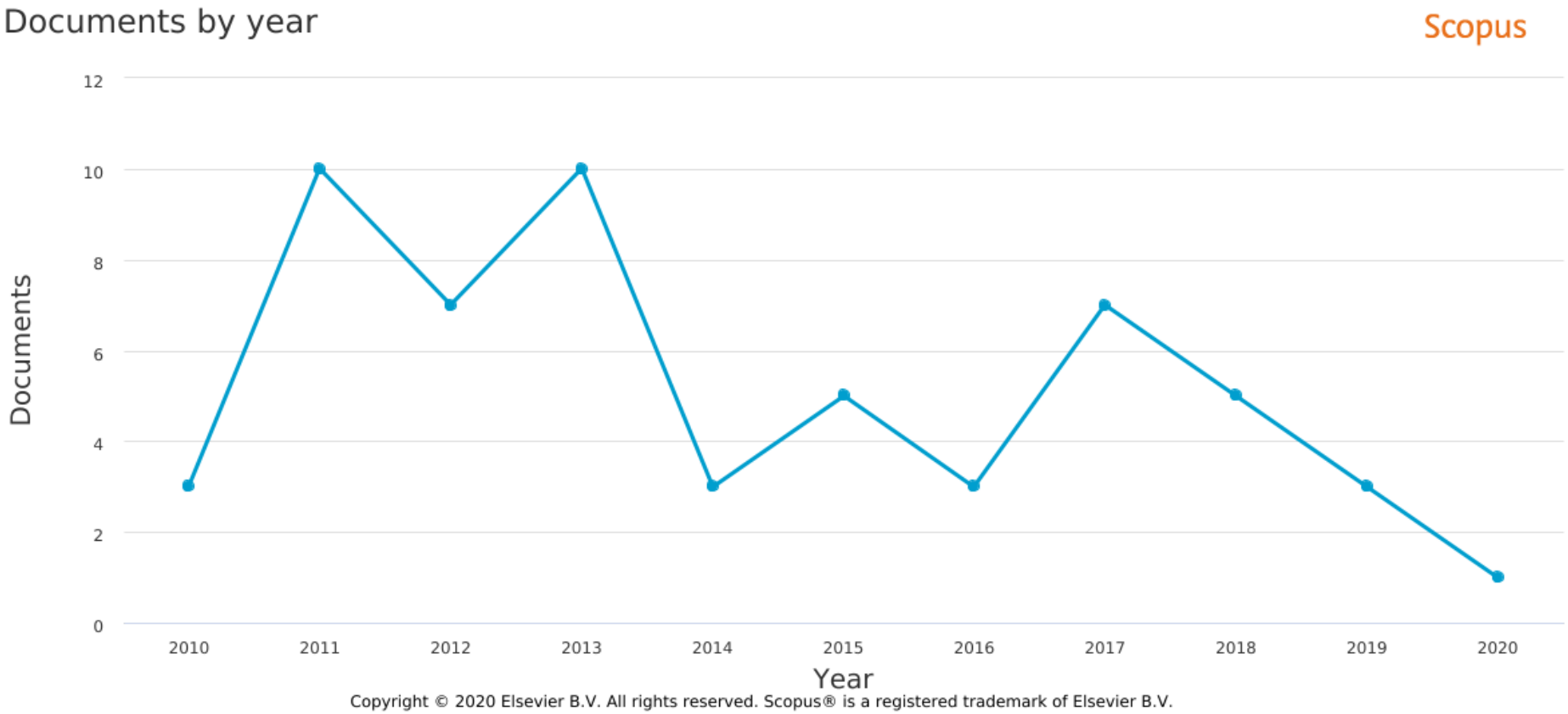


Some evidence that privacy concern is an IS trend that is in its infancy as suggested by Smith et al., (2011) is the low number of publications on concern for privacy dating as far back as 2010. The number of privacy concern publications reached their highest in 2011 and 2013. The trend dwindled from 2014 onwards but picked up again in 2017 to seven articles, which is about 12% of the total articles published since 2010. At the time of writing this report: that is, on 07 February 2020, three are only three articles were published in 2019 but after only two months into 2020 one article was published. This can be seen in **Table 2 and Figure 5** below based on information that was returned through queries that were performed on Scopus (www.scopus.com) for publications relating to concern for privacy.

Table 2: Concern for Privacy Publications Since 2010

Year	Number of Publications	Percentage of Total
2020	1	2%
2019	3	5%
2018	5	9%
2017	7	12%
2016	3	5%
2015	5	9%
2014	3	5%
2013	10	18%
2012	7	12%
2011	10	18%
2010	3	5%

Figure 5: Graph Showing Concern for Privacy Publications Since 2010



The analysis of information privacy literature revealed that over the past years privacy research has mainly been focused on online transactions such as online banking and shopping as well as the payment of bills for municipal services online, personalised technologies that include the Internet of Things (IoT) enabled devices such as smartwatches, fitness trackers and other location-based devices. Publications around how an organisation can enable information privacy and security policy compliance to protect their customers and their organisation for some of the privacy and security-relevant services they provide, sometimes mostly online (Alashoor et al., 2017; Mou et al., 2017; Pennsylvania State University et al., 2011; Smith et al., 2011). Furthermore, protection motivation theory it's the predominant theoretical model used to explore the concept of privacy and factors affecting information privacy concerns (Conner et al., 2005, p. 81; Dinev & Hart, 2005; Mou et al., 2017; Pennsylvania State University et al., 2011). Other theories used to explain privacy concerns include the communication privacy management theory that posits that disclosure is the process by which people announce or receive personal information (Michigan, 1960), technology threat avoidance theory, which explores the behaviour of information technology users to avoid the threat of harmful information technologies (Liang & Xue, 2009), fear-appeals model, which deals with persuasive messages that are designed and used, normally in drug-prevention campaigns to frighten people into taking a specific course of action (Witte, 1992), and lastly the health belief model, which explains that to prevent illness, individuals will take some action if they see themselves as vulnerable (Jones et al., 2015). However, these will not be used for this research as explained in chapter 1.

Studies reveal that Internet literacy, individual intentions to use the internet, social awareness and privacy concerns are inter-related factors. This means that these factors will always influence each other is in the same direction (Dinev & Hart, 2005). Researchers also found that privacy concern is influenced by perceived benefits once a measure of protection behaviour is adopted, and self-efficacy does not influence privacy concern (Conner *et al.*, 2005). Rather self-efficacy influences privacy protection behaviour and that perceived vulnerability significantly influence privacy concerns (Conner *et al.*, 2005; Mou *et al.*, 2017). Furthermore, research reveals that online privacy concerns are affected by threat appraisal factors such as perceived control, perceived severity and perceived vulnerability (Conner *et al.*, 2005; Junglas, *et al.*, 2008; Zhang & McDowell, 2009).

Research posits that concern for privacy and the intention to share PI online is moderated by trust and that trust, in turn, is mediated by risk. Researchers also believe that information privacy is a multi-level concept but is seldom studied as such (Alashoor *et al.*, 2017; Chen, *et al.*, 2016; Mou *et al.*, 2017; Warkentin *et al.*, 2017).

The study's literature review highlighted that information privacy research is characterised by scant papers that consider in one conceptual model the factors that influence concern for privacy, and the elements of trust and risk, where risk is mediated by trust and the relationship between concern for privacy, and intention to transact is moderated by trust (Alashoor *et al.*, 2017; Bélanger & Crossler, 2011; Boss, Galletta, Lowry, Moody & Polak, 2015; Chen, *et al.*, 2016; Dinev & Hart, 2005; Gao, *et al.*, 2015; Johnston & Warkentin, 2010; Johnston, *et al.*, 2015; Junglas, *et al.*, 2008; Mou *et al.*, 2017; Warkentin *et al.*, 2017; Warkentin, Johnston, Shropshire & Barnett, 2016; Youn, 2009; Zhang & McDowell, 2009).

A summary of the review of privacy literature has been provided in **Table 3** to illustrate the predominant dominant concepts, factors, contexts, research methods, populations, demographics and variables used in the information privacy research papers that were considered. To summarise the information in, review of literature revealed that privacy research has primarily been focused predominantly on two themes, namely, explanation of the concept of privacy, and use or adoption of online services and personalised technologies such as smart devices. Of the two themes, there is more literature on the use or adoption of online services and personalised technologies. Such studies have primarily explored PMT constructs like coping and threat appraisal, privacy concerns, perceived vulnerability, self-efficacy and behavioural intention. Other notable variables are being familiar with big data, trust, self-disclosure accuracy and concerns, social influence, performance expectancy, perceived privacy risk, third-party access, personality traits, attitudes on privacy, social awareness and Internet literacy. The research

methods and demographics used for privacy studies have mostly been through surveys with university students.

Table 3: Summary Key Concepts Identified by IS Research on Privacy

Reference	Context	Methods Used and Demographics	PMT Constructs	Other Variables
Alashoor *et al.* (2017)	Self-disclosure accuracy in social networking websites	Survey Northeast USA students	Privacy concerns Perceived vulnerability Self-efficacy	Familiarity with big data Awareness of big data Awareness of big data implications Trust Self-disclosure accuracy Self-disclosure concerns
Bélanger and Crossler (2011)	Information privacy	Literature review	Privacy concerns.	Impacts of electronic business and privacy Attitudes regarding privacy Privacy practices
Boss *et al.* (2015)	Protection Motivation Theory	Literature review	Coping appraisal Threat appraisal	
Chen, *et al.* (2016)	Online information disclosure	Survey USA adults over 18 years of age	Online privacy concerns Awareness of online information disclosure	Information stolen Relational conflicts Privacy setting Access setting Contact management

Reference	Context	Methods Used and Demographics	PMT Constructs	Other Variables
				Identity masking
Dinev and Hart (2005)	Online transactions	Survey Southern USA respondents within technology, finance, retail, education and government industries	Intention to transact Privacy concerns.	Internet literacy Social awareness
Gao, *et al.* (2015)	Wearable technology acceptance in healthcare	Survey MBA students	Self-efficacy Perceived vulnerability Perceived severity Intention to adopt healthcare wearable devices	Performance expectancy Hedonic motivation Effort expectancy Functional congruence Social influence Perceived privacy risk Product type
Johnston *et al.* (2015)	Information security policies and procedures compliance.	Hypothetical scenario, Government employees	Perceived threat severity Perceived threat susceptibility Perceived self-efficacy Perceived response efficacy	Compliance intention Formal sanction certainty Formal sanction severity Informal sanction certainty Informal sanction severity Sanction celerity
Junglas *et al.* (2008)	Personalised technology	Survey	Privacy concerns.	Personality traits.

Reference	Context	Methods Used and Demographics	PMT Constructs	Other Variables
		University students		
Mou *et al.* (2017)	Protection Motivation Theory in Information Security Literature	Literature review	Perceived severity Perceived vulnerability Fear Self-efficacy Response cost Behavioural intention Perceived threat	
Warkentin *et al.* (2017)	Smart meter technology adoption	Survey USA home owners	Internet users' information privacy concerns Behavioural intention	Social influence Trusting beliefs Risk beliefs Psychological ownership Meter invasiveness Program discount Third party access
Youn (2009)	Online privacy concerns	Survey Middle school students	Online privacy concerns Privacy protection behaviours	Intrapersonal sources Cognitive appraisals
Zhang and McDowell (2009)	Online users	Survey Southern USA students	Perceived severity Perceived vulnerability	

Reference	Context	Methods Used and Demographics	PMT Constructs	Other Variables
			Fear Response Efficacy Response cost Intention to share PI	

Moreover, information privacy literature reveals that data collected for such research has focused mostly on student respondents based in the USA (Bélanger & Crossler, 2011; Boss *et al.*, 2015; Dinev & Hart, 2005; Junglas, *et al.*, 2008; Johnston, *et al.*, 2015; Youn, 2009; Zhang & McDowell, 2009). Therefore, there is a gap concerning similar research and publications that consider information privacy and privacy concerns outside the USA and Asia. Instead, there is a need to consider the concept and phenomenon in developing regions or environment such as South Africa where privacy concerns are starting to peak (Privacy International, 2019).

2.3. Conclusion

Technological advances have made it easier to collect data. More so, individuals' PI can be considered a driving force for the modern data-driven economy, and threats related to this new ability to collect large amounts of individuals' data has come to the fore. Consequently, individuals are beginning to be aware of these threats and are starting to show concerns for privacy especially in situations where they must share their PI online. Privacy or information privacy as explained, an individuals' right to exert as a certain amount of control over the extent of use of their PI. The eight conditions, as developed by the OECD, for proper processing of PI were explained as well.

Initial privacy researchers predominantly explored the concept of privacy and the use or adoption of online services and personalised technologies instead of the factors affecting individuals' information privacy concerns. Also, the protection motivation theory and its associated variables have predominantly been used to explore the concept of privacy and factors affecting information privacy concerns. Prior research on information privacy has been able to contribute to the field through their explanations of what is privacy, the impacts of privacy issues as well as some of the relationships between variables that influence individuals behaviours when adopting online services or adopting personalised technologies. By using and exploring PMT constructs prior research has been able to explain the relationships between privacy concerns, the perceived benefits of adopting protection behaviour online, and threat appraisal factors such as perceived control, perceived severity and perceived vulnerability that can influence individual's intention to use online services or adopt privacy relevant technologies. The next chapter will present the theoretical background and research model of this study.

3. Theoretical Background and Research Model

This chapter of the study provides an explanation of protection motivation theory (PMT), which will be adopted and used to develop this study's conceptual model to answer the research problem. PMT was developed as a basis for understanding and predicting the protective behaviours individuals adopt when they are faced with potentially fearful or threatening situations. Therefore, this chapter explains why the proposed conceptual model is suited to understand the study's problem. This chapter also explains the variables used as part of the study's proposed conceptual model and the model's eight hypotheses are developed.

3.1. Protection Motivation Theory

The PMT model was developed as a basis for understanding and predicting the protective behaviours that individuals adopt when they are faced with potentially fearful or threatening situations, and that that fear and trust are often motivational drivers for some individuals' behaviours (Conner *et al.*, 2005; Maddux & Rogers, 1983; Zhang & McDowell, 2009).

PMT as a theory was developed from Expectancy-Value Theory (EVT) (Mou et al., 2017). EVT states that choices related to achievement are driven by a combination of individuals' expectations for success and their views about the value of tasks in certain areas (Studer & Knecht, 2016). For example, people will follow a passion if they find value in pursuing the interest and expect to be successful at it (Mou et al., 2017; Studer & Knecht, 2016). PMT adapted EVT to explain the behaviours adopted by individuals to avoid threats and it includes two analytical processes that are key in describing protection motivation, such as, threat appraisal processes and coping appraisal processes (Maddux & Rogers, 1983; Milne et al., 2000; Mou et al., 2017). According to PMT, threat appraisal processes are evaluated by individuals when they pursue their interests or activities (Milne et al., 2000; Mou et al., 2017). Coping appraisal processes, on the other hand, are based on the use of intellectual, emotional and behavioural strategies to manage the psychological demands of circumstances when they are assessed (Ellsworth & Scherer, 2003; Milne et al., 2000; Mou et al., 2017). Typically the demands are assessed as stressful or beyond one's capabilities to reduce the negative psychological effects caused by stress (Ellsworth & Scherer, 2003; Milne et al., 2000; Mou et al., 2017). Threat appraisal processes are explained by variables known as perceived severity, perceived vulnerability and fear. Coping appraisal processes are explained by variables known as perceived self-efficacy, perceived response efficacy and perceived response cost (Britton et al., 2011; Ellsworth & Scherer, 2003; Maddux & Rogers, 1983; Milne et al., 2000).

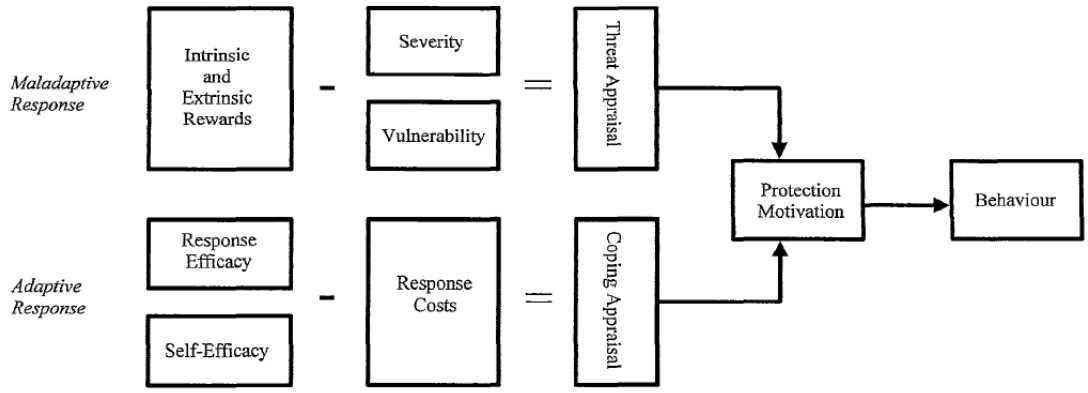
Research shows that when individuals transact online it involves elements and factors involved in threat and coping appraisal processes, especially, in situations where individuals are expected to share their PI (Bélanger & Crossler, 2011; Conner et al., 2005, p. 81; Cromer, 2010). Based on this, the PMT model is considered a suitable theoretical model to be adopted to understand individuals' concerns for privacy and how the factors therein influence individuals' intentions to share PI online as presented in Conner et al. (2005). See **Figure 6, 7 and 8** for an illustration and examples of the adaptation of Maddux and Rogers' (1983) revised PMT model. The **Figure 6** model illustrates that threat appraisals are based on maladaptive responses that are characterised as intrinsic and extrinsic rewards (Conner et al., 2005). These translate into the severity and vulnerability of individuals to situations. Also, coping appraisals are based on adaptive responses characterised as response efficacy and self-efficacy. These translate into response costs to individuals in situations. This means that the protection motivation that an individual may decide to take is mediated by the two appraisal processes mentioned, and individuals' behaviour is dependent on the strategy taken for protection motivation.

The **Figure 7** model presents an adaptation of PMT that looks to understand individuals' behavioural intentions regarding compliance with information security policies, standards or requirements

(Warkentin et al., 2016). The model illustrates that individuals' continuance compliance intentions with security standards are affected by their beliefs about how serious a threat is, their chances of encountering the threat, their views about whether they have an effective response to the threat and their belief that they can carry out the response to the threat.

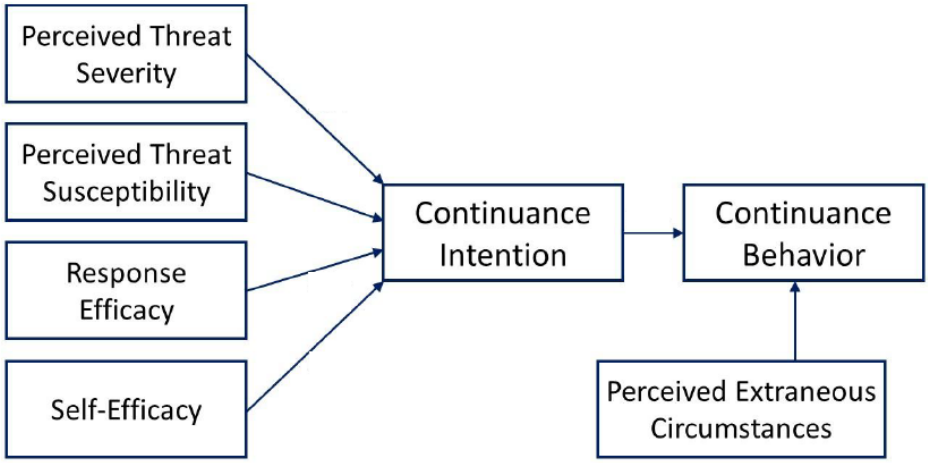
The **Figure 8** model depicts a model of individuals' actual information protective practices through eight hypotheses where trust moderates the relationship between privacy concerns and the accuracy of the information disclosed on social networks(Alashoor et al., 2017; Belanger & Crossler, 2019). Earlier studies suggest that the need to model information protection behaviours regarding concepts like trust which are not part of the PMT but can be situated alongside PMT constructs such as concern and self-efficacy (Boss et al., 2015; Oladimeji, 2017). Research shows that people's attitudes towards information sharing refer to the evaluation by individuals of their preparedness to share information through their mobile devices or on social media (Alashoor et al., 2017; Belanger & Crossler, 2019). Belanger and Crossler (2019) explain further that mobile privacy protection self-efficacy is people's views about how they can manage their privacy on their mobile devices.

Figure 6: Illustration of the PMT Model



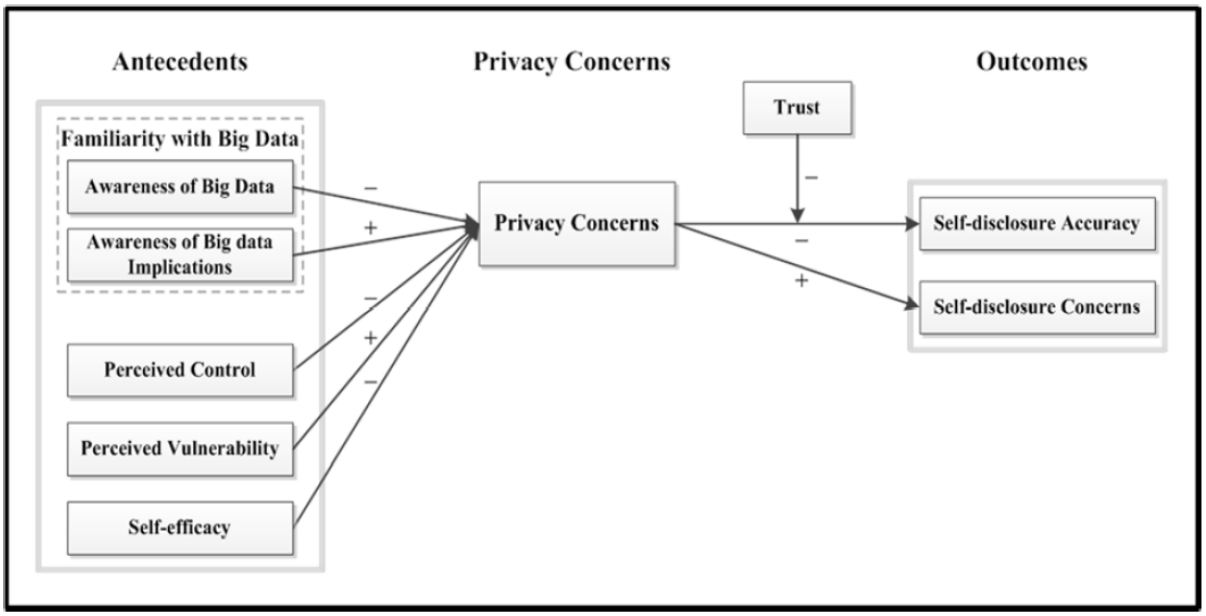
Source: Conner *et al.* (2005)

Figure 7: Application of the PMT Model in Information Security Research



Source: Warkentin *et al.* (2016)

Figure 8: PMT Illustration of Trust as Moderator Between Privacy Concern and Self-Disclosure



Source: Alashoor et al., (2017)

Salleh et al., (2013) posits that trust is critical only in uncertain circumstances has and it has become critical for daily transactions, communications and interactions online. Trust is also understood as an important predictor of perceived risk and in situations where there is no risk and actions can be carried out with absolute certainty then no trust would be required (Alashoor et al., 2017; Belanger et al., 2002; Belanger & Crossler, 2019; Salleh et al., 2013). Such studies have proven that perceived risk is reduced when trust occurs (Alashoor et al., 2017; Belanger et al., 2002; Belanger & Crossler, 2019; Salleh et al., 2013). As such, trust and perceived risk are important for online business such as online shopping, payment of municipal bills online and internet banking (Alashoor et al., 2017; Belanger et al., 2002; Belanger & Crossler, 2019; Salleh et al., 2013).

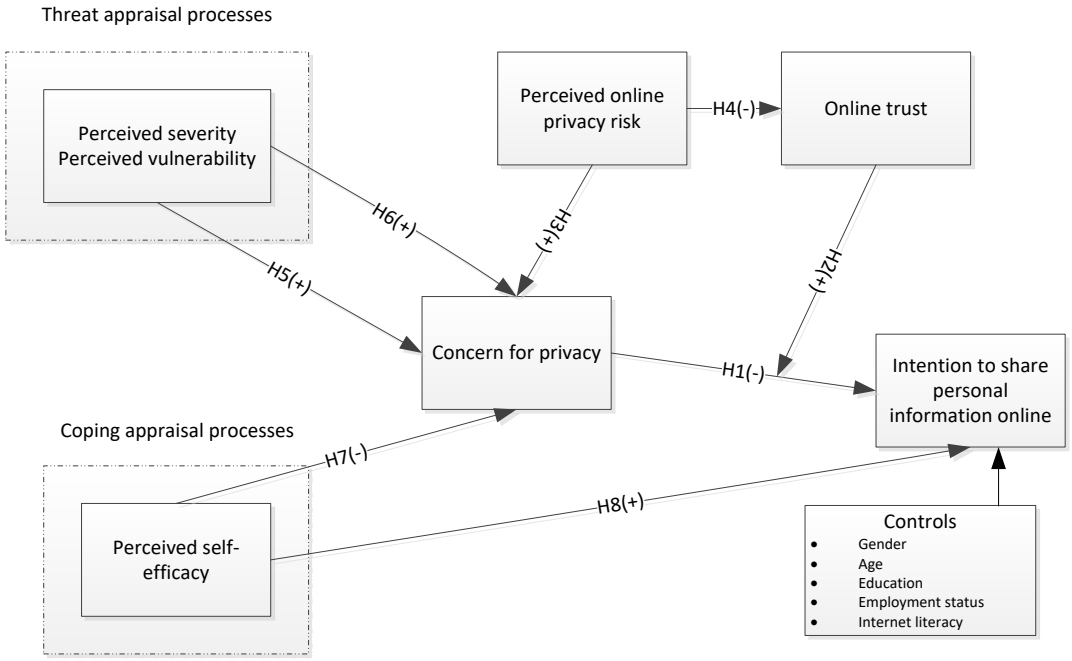
3.2. Conceptual Model

Review of past IS privacy literature reveals that PMT is the predominant model used to understand information privacy concepts, such literature is normally focused on how intended behaviour is affected by the threat and coping appraisals (Dinev & Hart, 2005; Junglas, *et al.*, 2008; Zhang & McDowell, 2009). However, many of these studies exclude other potentially important factors. Some of the excluded factors that this study explored are the factors of risk and trust, and how they might influence the relationship between concerns for privacy and intention to transact or share PI online (Alashoor *et al.*, 2017; Dinev & Hart, 2006; Gao, *et al.*, 2015; Warkentin *et al.*, 2017).

Although some information privacy literature considers trust and risk factors as well as their impact on individuals' online behaviour, such prior research is few (Alashoor *et al.*, 2017; Dinev & Hart, 2006; Gao, *et al.*, 2015; Warkentin *et al.*, 2017).

This study proposes an extension to the PMT to understand the factors and relationships amongst the factors that affect individuals' concerns for privacy and their intentions to share PI online. This will be done by exploring how threat and coping appraisal factors influence concerns for privacy, and how factors of risk and trust can influence concerns for privacy and the relationship between concern for privacy and intention to share PI online, respectively. See **Figure 7** below for an illustration of this study's expended PMT model:

Figure 9: The Study's Proposed Conceptual Model



3.2.1. Intention to Share Personal Information Online

The model's dependent variable is the intention to share personal information online, which is known as people's planned behaviour or the amount of effort an individual is willing to endure to carry out an actual behaviour online (Ajzen, 1991; Alashoor *et al.*, 2017). This is normally based on the protection motivational factors, such as concerns for privacy that lead to such behaviour (Ajzen, 1991; Alashoor *et al.*, 2017). Example of such behaviour includes a willingness to share PI when shopping online, paying bills or performing online banking(Belanger et al., 2002; Belanger & Crossler, 2019; Hussain et al., 2015; Salleh et al., 2013).

3.2.2. Concern for Privacy

Services such as online shopping, online driver's license applications, online banking, social media often require individuals to share their PI such as names, surnames, credit card details, contacts details and even physical address on the internet. This way of collection and use of PI poses potential threats to individual privacy, which could affect the adoption of online services (Gao *et al.*, 2015; Warkentin *et al.*, 2017). Research shows that privacy is often quoted as the reason individuals have stopped or delayed to use the internet for performing everyday activities like online shopping, banking, social interactions and bill payments as they worry that this may result in them losing control over their PI (Clarke, 1999; Gao, *et al.*, 2015; Warkentin *et al.*, 2017). This phenomenon could be attributed to the lack of sufficient information about the privacy practices of some organisations' online services and subsequently possible low levels of trust in such organisations' privacy practices (Dinev & Hart, 2005; Alashoor *et al.*, 2017; Chen, *et al.*, 2016; Gao, *et al.*, 2015). As such, some researchers have characterised concern for privacy as a cognitive response to individuals' low levels of trust in such organisations' privacy practices (Bélanger & Crossler, 2011; Youn, 2009). For example, some of the questions the study's research questionnaire asked respondents was whether they were generally worried about sharing their PI online because of many things others can do with it or that they were often worried about that their PI being stolen easily if they shared it online. .

IS theories around concerns for privacy were generally developed around the same time as advances in IS, and these theories continue to evolve as technology continues to advance in becoming more pervasive and personalised. As such, researchers believe that this is likely to cause concerns for privacy is to increase (Junglas, *et al.*, 2008). Furthermore, researchers believe that the basis for privacy concerns are two-fold, namely, individual interactions with technology, specifically the internet, and the social process of interacting with entities that individuals often know very little about (Dinev & Hart, 2005). In response to the growing concern for privacy, IS researchers have begun to explore information privacy issues such as how individuals respond and try to address their concerns for privacy (Bélanger & Crossler, 2011).

Based on the considerations outlined above, this model and hypothesis below consider the negative relationship between concern for privacy and the behavioural intention to share PI online:

Hypothesis 1 (H1): The greater the concern for privacy, the less likely an individual's intention to share their PI online.

3.2.3. Online Trust and Perceived Online Privacy Risk

Online trust can be defined as how much a person thinks that online services and platforms will handle their PI safely and securely: that is, the belief that the online organisation is reliable in the way they handle their PI (Alashoor *et al.*, 2017). Consequently, the relationship between concerns for privacy and the intention to share PI online may be stronger or weaker depending on trust (Alashoor *et al.*, 2017). This leads to the hypothesis:

Hypothesis 2 (H2): Online trust moderates the relationship between concerns for privacy and intentions to share PI online.

Perceived online privacy risk refers to how much a person thinks that that if they share their PI online then there is potential for misuse, unauthorised access or harm (Cromer, 2010; Dinev & Hart, 2006; Milne *et al.*, 2000; Warkentin *et al.*, 2017). Also, when individuals are faced with situations where they are required to share their PI online they tend to be generally concerned about what happens to the PI that they disclose (Cromer, 2010; Dinev & Hart, 2006; Milne *et al.*, 2000; Warkentin *et al.*, 2017). This includes concerns that their PI may be available to an unknown group of information seekers without them knowing (Cromer, 2010; Dinev & Hart, 2006; Milne *et al.*, 2000; Warkentin *et al.*, 2017). This leads to the hypothesis:

Hypothesis 3 (H3): The greater the perceived online privacy risk, the more likely an individual will have concern for privacy.

Researchers have observed that individuals' concern for privacy tends to be either greater or less depending on their level of trust in an online service as well as their level of perceived online privacy risks before using such services (Cromer, 2010; Dinev & Hart, 2006; Milne *et al.*, 2000; Warkentin *et al.*, 2017). This points to the idea that individuals could trust online platforms more if they believe that the online risks to using such platforms were relatively low (Cromer, 2010; Dinev & Hart, 2006; Milne *et al.*, 2000; Warkentin *et al.*, 2017). This leads to the hypothesis:

Hypothesis 4 (H4): The greater the perceived online privacy risk, the more likely an individual will have less online trust.

3.2.4. Threat Appraisal Process

As explained, threat appraisal processes are the intellectual and emotional strategies used by individuals to assess the likelihood and level of threat of an event (Britton et al., 2011; Conner et al., 2005, p. 81; Milne et al., 2000; Mou et al., 2017; Zhang & McDowell, 2009). The two core constructs are Perceived Vulnerability and Perceived Severity. Perceived Vulnerability is the level to which an individual is inclined to believe that they are exposed to a given threat. Perceived Severity refers to how serious an individual believes that they would be affected should a possible threat occur, i.e. the extent to which the consequences of an information privacy breach will be serious.

3.2.4.1. Perceived Vulnerability

Perceived vulnerability is defined as the level to which an individual tends to believe that they are exposed to a threat (Milne *et al.*, 2000; Mou *et al.*, 2017). Research shows that some individuals believe that they are less likely to be affected by a threat than others. Therefore, in an online context individuals who claim that they are more vulnerable than others will have a higher concern for privacy when they need to share their PI online because of the potential psychological stress (Britton et al., 2011; Milne et al., 2000; Zhang & McDowell, 2009). This leads to the hypothesis:

Hypothesis 5 (H5): The greater the perceived vulnerability about online privacy, the more likely an individual will have concern for privacy.

3.2.4.2. Perceived Severity

Perceived severity deals with the belief that an individual has of the consequences for themselves should they be affected by a possible threat (Milne *et al.*, 2000; Mou *et al.*, 2017). Also, research shows that the more convinced an individual is about the severity of consequences of a threat, then they will be concerned about online privacy (Cromer, 2010; Milne *et al.*, 2000; Mou *et al.*, 2017; Zhang & McDowell, 2009). In this context, a person may believe that they may be severely affected by identity theft or financial crime (Belanger & Crossler, 2019; Britton et al., 2011). This leads to the hypothesis:

Hypothesis 6 (H6): The greater the perceived severity about online privacy, the more likely an individual will have concern for privacy.

3.2.5. Coping Appraisal Process

Coping appraisal processes are adopted by individuals to evaluate possible strategies for dealing with supposed threats (Cromer, 2010; Milne *et al.*, 2000; Mou *et al.*, 2017; Zhang & McDowell, 2009). While past PMT studies name three core constructs: perceived response efficacy, response cost and self-efficacy. This study only includes perceived self-efficacy in the model. This is because this study is focused on privacy research around privacy concerns, and how it can be understood by adopting PMT. Therefore, the relevant PMT construct involving coping appraisal processes is self-efficacy and only self-efficacy was considered for this study. The other coping appraisal process factors such as response cost and response efficacy are normally used in information security research and they are generally relevant for information security and related studies that aim to understand the relationship between response cost, response efficacy and compliance behavioural intentions based on a recommended action (Zhang & McDowell, 2009).

3.2.6. Perceived Self-Efficacy

Studies show that claims that individuals have about their self-efficacy have proven to be important factors in mediating their protection motivation and behavioural intentions (Cromer, 2010; Maddux & Rogers, 1983; Youn, 2009). These are typically manifested in situations where protective behaviours and actions require specialised knowledge, such as the ability to use technologies that can safeguard one's privacy online (Cromer, 2010; Maddux & Rogers, 1983; Youn, 2009).

Research reveals that individuals who are confident about how to protect themselves online tend to understand better the harmful effects of improper access of their PI (Junglas, *et al.*, 2008; LaRose, *et al.*, 2008; Youn, 2009). This means that individuals who claim that they are confident that they can protect their privacy online are less likely to have a concern for privacy. This leads to the hypotheses:

Hypothesis 7 (H7): The greater the perceived self-efficacy to protect their online privacy, the less likely an individual will have concern for privacy.

Individuals who view themselves as knowledgeable and competent Internet users are more likely to use online services and ultimately share their PI online because they feel confident about their ability to deal with any potential threats to their privacy online (Dinev & Hart, 2005; Cromer, 2010; Milne *et al.*, 2000). This means that individuals who are confident in their skills to safely transact online are more likely to share their PI online (Dinev & Hart, 2005; Cromer, 2010; Milne *et al.*, 2000). Some examples include awareness and understanding of how to use protection features such as passwords, trackers and location settings on mobile devices or websites (Belanger & Crossler, 2019; Oladimeji, 2017). This leads to the hypotheses:

Hypothesis 8 (H8): The greater the perceived self-efficacy to protect their online privacy, the more likely an individual's intentions to share their PI online.

3.2.7. Controls

The following variables were added as controls:

Internet literacy which is defined as the ability that an individual has to use a computer system to achieve certain outcomes (Dinev & Hart, 2005). For this study internet literacy, particularly familiarity with the use of various types of online accounts was added as a control because research reveals that the greater the level of Internet literacy, the greater an individual's intentions to share PI online (Dinev & Hart, 2005).

Age, gender, education and employment status were included as controls in the study as researchers have discovered that these factors are important in describing the population of individuals that typically use online services (Kurfalı et al., 2017).

3.3. Conclusion

This chapter of the study explained the theoretical model that was adopted for this study. The chapter explained that PMT was developed as a basis for understanding and predicting the protective behaviours individuals adopt when they are faced with potentially fearful or threatening situations. Drawing on an extended PMT model, eight hypotheses were developed. These are summarised as:

1. H1: The greater the concern for privacy, the less likely an individual's intention to share their PI online.
2. H2: Online trust moderates the relationship between concerns for privacy and intentions to share PI online.
3. H3: The greater the perceived online privacy risk, the more likely an individual will have concern for privacy.
4. H4: The greater the perceived online privacy risk, the more likely an individual will have less online trust.
5. H5: The greater the perceived vulnerability about online privacy, the more likely an individual will have concern for privacy.
6. H6: The greater the perceived severity about online privacy, the more likely an individual will have concern for privacy.
7. H7: The greater the perceived self-efficacy to protect their online privacy, the less likely an individual will have concern for privacy.
8. H8: The greater the perceived self-efficacy to protect their online privacy, the more likely an individual's intentions to share their PI online.

The next chapter will explain the approach taken to test the above hypotheses and answer the research question. The chapter will explain the research design along with methods for data collection and analysis.

4. Research Methodology

This chapter explains the research paradigm and approach. The chapter details the process used to develop the study's survey questionnaire, which consisted primarily of 7-point Likert-type scales used to assess the model's variables. The chapter also discusses pre- and pilot testing as well as online distribution of the questionnaire. The method of survey distribution was chosen to reach a favourable number of respondents for the study sample. The various data analysis methods used are introduced, including, the statistical methods used to test the hypotheses. The chapter closes with a view of the steps taken to manage potential ethical issues that could arise while conducting this study.

4.1. Research Paradigm

Paradigms form how individuals view the world. IS research is mainly informed by two research paradigms, namely, positivist and interpretivist (Bhattacherjee, 2012; Oates, 2006). These paradigms differ in how research is conducted, as well as the basis for exploring research questions and the way they are answered.

This study is informed by the positivist paradigm. Positivist research studies are based on the assumption that events within the world and our environment are consistent, and that this level of consistency is a result of independent laws and patterns in which the world works (Bhattacherjee, 2012; Oates, 2006). Therefore, these events within our environments and the world can be objectively studied or understood by relying on these consistent and independent laws, regardless of how anyone may perceive these laws to work (Bhattacherjee, 2012; Oates, 2006; Saunders et al., 2009).

The positivist research mindset is to explore these independent and consistent laws by building up an iterative research cycle where a research theory that is developed about a phenomenon is studied through investigations that aim to confirm or deny the theory. Therefore, results for positivist research are often understood by continuous review of the cause and effect of the outcomes (Bhattacherjee, 2012; Oates, 2006). The positivist research paradigm is thus reflected in how this study will test and explain the relationships hypothesised between PMT factors, concern for privacy and individual intentions to share PI online. Also, the relational research approach was used by this study to analyse and interpret research results as this was best suited to understand the type of relationships between the variables for the proposed conceptual model (Bhattacherjee, 2012; Coleman, 05 March 2017a, 17 August 2017b; Oates, 2006). This approach was used as the relationships between the variables for this study’s proposed conceptual model were presumed to be casual and the aim for this paper was to determine whether the claims were true (Bhattacherjee, 2012; Coleman, 05 March 2017a, 17 August 2017b; Oates, 2006). The credibility of the claims in terms of the relationships between the variables for this study’s conceptual model was assessed by performing correlational statistical analysis (Bhattacherjee, 2012).

The study is quantitative. Quantitative research explains phenomena and concepts through the collection of numerical data that is analysed using statistical methods (Muijs, 2004).’

A comparison can be made between the positivist research paradigm and interpretivist research in which researchers explore individuals’ perceptions of the world by trying to understand the meanings and values that assign to a phenomenon that is studying a specific context (Bhattacherjee, 2012). The interpretivist approach to research does not worry about proving or denying research hypotheses but rather attempts to identify, explore and explain how various elements within a context are related or interrelated (Bhattacherjee, 2012; Coleman, 05 March 2017a, 17 August 2017b; Oates, 2006). Furthermore, interpretivist research is typically based on examining individuals in their normal social settings through qualitative analysis methods such as interviews, observations, questionnaires and case studies (Coleman, 05 March 2017a, 17 August 2017b). As such, it was determined that the interpretivist research approach was not suitable for this study as this paper attempts to understand the

factors that influence individuals' intention to share PI through the acceptance or rejection of various hypotheses. The interpretivist research approach was also not desirable as it is often influenced by the researcher's assumptions, beliefs, values and actions which has an influence on the research process and study (Bhattacherjee, 2012; Coleman, 05 March 2017a, 17 August 2017b; Oates, 2006).

4.2. Survey Design and Sampling

A survey instrument was used for data gathering to perform statistical analysis on the factors influencing individual concern for privacy and ultimately their intention to share PI online. The use of survey questionnaires is best suited for this type of study as they are useful for exploring unobservable data such as individuals' preferences, traits, attitudes or behaviours (Bhattacherjee, 2012). Also, this approach was chosen as it is in line with what other researchers have used for this type of study (Bélanger & Crossler, 2011; Boss *et al.*, 2015; Dinev & Hart, 2005; Johnston & Warkentin, 2010; Junglas, *et al.*, 2008; Warkentin *et al.*, 2016; Youn, 2009; Zhang & McDowell, 2009).

Careful attention was paid to the content, sequencing and wording of the questions asked in the questionnaire survey. Typical survey questionnaire issues such as ambiguity, generalisations, too much detail and being presumptuous to name a few were avoided by pre-testing the questionnaire with five IS researchers who have extensive experience in conducting similar studies. Pre and Pilot testing results will be explained in this chapter (Bhattacherjee, 2012).

Given the idea that this study is based on advances in technology used for commercial and governmental services as well as social interactions that are driven by personalisation, it was decided that it would be reasonable to collect data through a self-administered online survey questionnaire. Studies show that (Duffy et al., 2005; Saunders et al., 2009; Shih & Xitao Fan, 2008) some of the known advantages of adopting an online survey methodology is that:

- they are not restricted to location and cost less than traditional survey methods.
- if Internet access is relevant for a study the online surveys allow researchers to reach certain populations especially those who have Internet access.
- online survey respondents are less affected by social desirability bias because of the presence of an interviewer.
- with the increasing use of the internet, respondents may be more comfortable with online surveys, and online surveys have been found to produce higher response rates than traditional survey methods.
- response rates can be increased through added features like reminders, which are synonymous with online surveys.

The online survey questionnaire was developed using eSurvey Creator and distributed to the study's research sample population through online social media channels such as Facebook, WhatsApp and emails. The sample population had the opportunity to click on the link of the study questionnaire to respond. To ensure the anonymity of the study's survey respondents, the collection of PI was not done be gathered through the study's survey questionnaire. Other ethical considerations will be explained in this chapter.

As the research data was collected via an online survey questionnaire, the two types of sampling techniques were evaluated to determine the method to adopt. Probability and non-probability sampling are two methods of sampling that can be used (Bhattacherjee, 2012). Probability sampling is used when a sample is selected from a larger population, and participants considered randomly selected. Non-probability sampling, on the other hand, is a sampling technique that relies on subjective judgement and the probability of a participant being selected for the sample cannot be calculated: that is, participants are not randomly selected (Bhattacherjee, 2012). Non-probability sampling was considered as the study dealt with a large population of online Internet users for which a sampling frame does not

readily exist (Bhattacherjee, 2012; Cameron, 2016; Duffy et al., 2005; Kayam & Hirsch, 2012; Saunders et al., 2009; Shih & Xitao Fan, 2008). he sampling approach adopted for this study was non-probabilistic sampling (Bhattacherjee, 2012). Specifically, the snowball sampling technique was used, which is typical of studies that involve non-deterministic samples (Saunders, Lewis & Thornhill, 2009). Distributing the study's survey questionnaire initially online through Facebook, WhatsApp and email and thereafter requesting that respondents share the online survey questionnaire link with other potential respondents, per the adopted snowball sampling approach, allowing a sufficient portion of research population to be sampled (Bhattacherjee, 2012; Cameron, 2016; Kayam & Hirsch, 2012; Saunders et al., 2009). Market researchers estimate that approximately 16 million South Africans use social media, more especially, Facebook (Staff Writer, 2017). Furthermore, the use of online survey questionnaires on social media such as Facebook is being used to perform research studies (Bhattacherjee, 2012; Kayam & Hirsch, 2012; Saunders *et al*, 2009).

This approach made it convenient for research participants to take part in the study and allowed the study to reach as many samples in the population as possible by making the survey questionnaire more easily accessible on platforms that many South Africans use (Kayam & Hirsch, 2012; Staff Writer, 2017; STATSSA, 2016). Online surveys have also been proven successful for data collection as they are automated and the tools are easy to understand and use (Kayam & Hirsch, 2012).

Previous studies posit that statistical power analysis is the ability to identify a significant effect or true association for a study's sample, whilst considering random error (Dorjee, 2017). Furthermore, the study's sample size should be large enough to be able to generalise results or observations back to the sample population and confirm that conclusions are not based on statistical variations. Generally statistical power can be calculated for specific studies but researchers can also determine statistically significant sample sizes for their work through informed decisions or judgements based on related theories or similar studies (Dorjee, 2017; Lakens, 2017). By using the judgmental approach, this research aimed to collect up to 250 responses from individuals to test the research model. The sample of 250 was selected as similar research focused on information privacy concerns sampled approximately 200 or less people (Alashoor et al., 2017; Henriques, 2018; Oladimeji, 2017). Also, previous statistics-based research has established that studies with a minimum sample size of 30 generally result in a mean for sample distribution close to a normal distribution (Saunders et al., 2009). A survey link was sent directly to a total of approximately 300 potential respondents via Facebook, WhatsApp and email. The respondents were encouraged to share the online survey with their contacts when they were done. Reminders were also sent to the initial respondents every month to complete the online survey or assist by sharing it with their contacts or by remaindering their contacts to complete it. The total responses received for the study was 163, which is approximately 65% of the expected responses. Review of similar studies shows that this number sufficient to ensure a representative sample as it is within the accepted margin of error of 5% at a 95% confidence level for the sample population of 250 (Oladimeji, 2017). Information on the analysis of the data received from the 163 online survey questionnaire responses is available in chapter six.

4.3. Operationalisation

Studies show that dependent, independent, mediation and moderation variables fall within the set of operationalised variables in a nomological network that shows the set of relationships between constructs (Bhattacherjee, 2012; Cohen, 2017; Oates, 2006; Saunders *et al.*, 2009). Dependent variables are influenced and explained by other variables typically mediating and independent variables. Dependent variables are often the subject or basis for a certain research study. Independent variables, on the other hand, are often described as the factors involved in explaining mediating variables as well as dependent variables (Bhattacherjee, 2012). Independent variables often can exist on their own and normally form the starting point for the explanation of most conceptual models.

Mediating variables are often used to explain the relationship between independent and dependent variables. Moderating variables, on the other hand, are variables that influence the strength of the relationship between independent and dependent variables (Bhattacherjee, 2012; Oates, 2006; Saunders *et al.*, 2009).

Referring to this study's conceptual model **Figure 6**, intentions to share PI online can be described as the dependent variable of the study while the factors involved in the threat and coping appraisal processes are seen as the independent variables. Concerns for privacy and perceived online risk are mediating variables because they explain how independent and dependent variables relate. Whilst trust can be described as the moderating variable in the conceptual model as it is used to explain the strength of the relationship between the mediating variable, concerns for privacy, and the dependent variable intentions to share PI online.

Closed-ended questions were used to measure the conceptual model's variables, and Likert-type scales were also used (Zhang & McDowell, 2009). The above-mentioned variables were assessed on two types of 7-point Likert-type scales ranging from 1 (totally disagree) to 7 (totally agree) and from 1 (not serious at all) to 7 (very serious).

The coping appraisal process variable was measured by using a scenario-based question where respondents were required to answer "Yes" or "No" to a question about whether they feel anxious about being asked to share their PI. Thereafter respondents were given four scenarios under which they will rate their confidence level when sharing their PI online by indicating on a 7-point Likert-type scale, whereby 1 would mean "totally disagree" and 7 indicates "totally agree" for their confidence levels per scenario provided. Similar scales of measurement have been used in previous studies to understand coping appraisal process variables such as self-efficacy (Agarwal & Karahanna, 2000a). Lastly, the dependent variable: that is, intention to share PI online, was evaluated by using a 7-point Likert-type scale from 1 (not willing at all) to 7 (very willing).

Measurements for items relating to privacy concerns, online trust and perceived online privacy risk were adopted and modified from (Alashoor et al., 2017; Dinev & Hart, 2005; Warkentin et al., 2017). Respondents had to show how much agreed with the assertion made about online trust and risk as well as privacy concerns by indicating on a 7-point Likert-type scale, where 1 indicates "totally disagree" and 7 indicates "totally agree." **Table 4** illustrates the research variables and measures, number of items per measure and the variable sources for the research survey questionnaire. The full research survey questionnaire used, and the associated measurement scales can be found in **Appendix A**.

The survey also contained demographic questions and responses for these were captured using dichotomous responses for data items like gender, nominal responses for data items such as employment status, ordinal responses for data items such as education and continuous responses for data items such as age. The survey also included questions asking the types of accounts or profiles respondents have and remaining questions captured responses for the proposed conceptual model's variables.

Table 4: Summary Conceptual Model Factors and Example Measurements

Variable	Conceptual Definition	Number of items	Example Items	Measurement Scale	Literature Support
Intention to Share PI Online	Individual's planned behaviour or the amount of effort an individual is willing to endure to carry out an actual behaviour online.	10	How willing are you to share your PI online to…register your PI online so that you can search and apply for jobs online.	1 (not willing at all) to 7 (very willing)	(Dinev & Hart, 2005)
Perceived Severity	How serious an individual believes that they can be affected by a possible threat.	4	I am concerned that online service providers do not take enough time and effort to prevent unauthorised access to my online accounts.	1 (totally disagree) to 7 (totally agree)	(Boss, Galletta, Lowry, Moody, & Polak, 2015) (Y. Chen & Zahedi, 2016) (Gao et al., 2015) (Herath & Rao, 2009) (Johnston et al., 2015) (Lee & Larsen, 2009) (Mohamed & Ahmad, 2012) (Yoon et al., 2012) (Zhang & McDowell, 2009)
		1	The consequences of Internet security attacks for me are…	1 (not serious at all) to 7 (very serious)	
Perceived Vulnerability	The level to which an individual is inclined to believe that they are exposed to a given threat.	3	I feel that I am vulnerable to hacking.	1 (totally disagree) to 7 (totally agree)	(Alashoor et al., 2017) (Boss et al., 2015) (Y. Chen & Zahedi, 2016) (Gao et al., 2015) (Herath & Rao, 2009)

					(Johnston et al., 2015) (Lee & Larsen, 2009) (Mohamed & Ahmad, 2012) (Yoon et al., 2012) (Youn, 2009) (Zhang & McDowell, 2009)
Perceived Self Efficacy	Manifested in situations when protective behaviours and actions require specialised knowledge, such as the ability to use technologies that can safeguard privacy on the internet.	1	Are you generally anxious about sharing your PI in order to use online services.	"Yes" or "No"	(Agarwal & Karahanna, 2000b)
		4	I am confident to share my PI online because I am familiar with the security measures for online services.	1 (totally disagree) to 7 (totally agree)	
Concern for Privacy	A cognitive response representing individuals' low levels of trust in such organisations' privacy practices.	3	I am often worried that my personal information can be easily stolen if I share it online.	1 (totally disagree) to 7 (totally agree)	(Dinev & Hart, 2005)
Perceived Online Risk	An individual's beliefs that if they share their PI online then there is potential for misuse, unauthorised access or harm.	3	It is risky to share my personal information online.	1 (totally disagree) to 7 (totally agree)	(Dinev & Hart, 2005)
Online Trust	The amount of belief that an individual has that online services and platforms will handle their PI safely and securely.	3	Systems provided by online service providers are safe environments to share my personal information.	1 (totally disagree) to 7 (totally agree)	(Alashoor et al., 2017)

4.4. Pre- and Pilot Testing

The purpose of pre- and pilot testing exercises is to make sure that the research questionnaire addresses the relevant issues that this study intends to explore, that it is easy to go through and comprehend and that it is developed within acceptable standards (Agarwal & Karahanna, 2000; Brown *et al.*, 2003; Culnan & Armstrong, 1999; Dinev & Hart, 2005; Junglas, *et al.*, 2008; Kurfalı *et al.*, 2017).

For pre-testing, the questionnaire was provided in electronic format to four senior IS researchers from the University of Witwatersrand, Johannesburg as well as two industry experts in information security and privacy from the Council of Scientific and Industrial Research (CSIR), Pretoria that has extensive experience in performing similar studies. They were asked to review and assess whether the research questionnaire items are sensible and plausible. Their responses and suggestions for improvement were reviewed and thematically summarised as the need for: clearer survey questionnaire instructions, shorter and more concise survey questions, more inclusive demographic questions and rating scales should be reviewed to avoid potential issues with reverse scoring. The suggestions helped to establish the content validity of the items over-and-above the use of literature sources as the basis for questionnaire development. Once feedback was received on the questionnaire from the IS researchers and industry experts, revisions were made based on their suggestions and the questionnaire was pilot tested through online survey platform eSurvey Creator to a convenience sample of 60 potential respondents. These were master's students at the University of the Witwatersrand as well as CSIR staff. Of those invited, 19 took part in the pilot and their responses were evaluated to improve the questionnaire before final administration. Improvements that were made included rephrasing of the wording of some measurement items, revising Likert-type scales from five to seven scales and the labelling of a midpoint, rearrangement of response choices to address potential issues with reverse scoring the inclusion of upfront demographics to capture the types of online accounts respondents use, removal of mandatory features for questions to allow respondents to voluntarily complete the survey questionnaire, the inclusion of a progress bar to help respondents see how far they were with completing the survey questionnaire as well as the removal of a measurement on information security incident management that was not relevant to the study's proposed conceptual model. Cronbach Alpha values for the variables were also calculated from the pilot survey data. This helped corroborate the reliability of the questionnaire (Brown et al., 2003; Kurfalı et al., 2017).

4.5. Data Analysis Methods

4.5.1. Validity and Reliability

The responses to the main survey were statistically tested using principal components analysis (PCA) as well as correlation and regression analysis through IBMS's SPSS statistics package as the primary software tool for analysis (Cohen, 2019; Statistics Solutions, 2019). PCA was chosen as it helps to assure that both convergent and discriminant validity exists for respondent data through analysis of the observed pattern of item loadings (Cohen, 2019). Also, PCA communalities were used to estimate the variance in each variable as this proves that the variance in each variable or proposed construct is accounted for by all relevant items or measures (Cohen, 2019; Knowledge Center, 2014). The total variance explained for the sample data was in three parts, namely, the Initial Eigenvalues (IEs), the Extraction Sums of Squared Loadings (ESSL) and the Rotation Sums of Squared Loadings (RSSL).

Thereafter, correlation analysis was employed to assess internal consistency reliability to prove that the various items performed measures as intended. Also, internal consistency reliability was assessed via analysis of the measures Cronbach Alpha and any Cronbach Alpha values of 0.7 and above were accepted (Cohen, 2019). As part of the reliability analysis, the Cronbach Alpha values for proposed constructs were evaluated using the standardised scores of the response data, and Cronbach Alpha values for all the proposed constructs that were considered either good ($0.8 \leq \alpha < 0.9$) or excellent(0.9

≤ α) based their relevant alpha values. Any items that did not meet this criterion were dropped and not included in further analysis performed. Overall, 10 out of 32 construct items were dropped before hypotheses testing and analysis of the research model was performed.

4.5.2. Hypothesis Testing

Following the validity and reliability tests, the constructs were reduced to their composite scores to allow for correlation and regression analysis. Composite scores were calculated because correlation and multiple regression analysis cannot be performed on multiple items (Agarwal & Karahanna, 2000b; Brown et al., 2003; Cohen, 2019; Culnan & Armstrong, 1999; Dinev & Hart, 2005; Junglas et al., 2008; Knowledge Center, 2014; Kurfalı et al., 2017). The arithmetic average of the final set of measurement items weighted equally to product the composite scores that were used for analysis and standardized scores were used.

Correlation and regression analysis were used to test the strength of how the constructs related: that is, dependent, independent, moderator and mediating variables. The specific tests that were used to test the strength of the relationships between the study's variables were bivariate correlation coefficient analysis. For bivariate correlation coefficient analysis Pearson's parametric test was performed (Agarwal & Karahanna, 2000b; Brown et al., 2003; Cohen, 2019; Culnan & Armstrong, 1999; Dinev & Hart, 2005; Junglas et al., 2008; Knowledge Center, 2014; Kurfalı et al., 2017). Pearson's test was used for this study as the data collected for this study was mainly interval (Likert-type scales) and the PCA results showed that the data to be used for further analysis was approximately normally distributed (Cohen, 2019).

4.6. Ethical Considerations

The five ethical principles to consider when conducting research are informed consent, participation based on freewill where there is no chance of harm to any participants, ensuring that all relevant information is disclosed, information is confidentially kept as well as the reporting of analysis work performed. (Bhattacherjee, 2012). Voluntary participation and harmlessness mean that the study's research subjects should know that they are not forced to take part in the study: that is, voluntary participation, and that they will not be harmed in any way by participating in the study (Bhattacherjee, 2012). Informed consent means that participants must be in the position to provide explicit consent before taking part in the research. Anonymity and confidentiality mean that to protect this study's research subject interests any information that will be provided by them cannot be available to others who are not part of the research.

Considering the sensitivity and severity of issues around the topic of privacy and in more recent times online privacy. Confidentiality and security of the data that was provided as well as the anonymity of individual participants were also key in terms of this study's ethical considerations. If this was not thought through carefully then this study could have faced some serious ethical issues (Bhattacherjee, 2012; Saunders *et al.*, 2009). The researcher addressed this concern by giving clear assurance to research subjects that the confidentiality and security of their responses were guaranteed, especially where responses to some research questions could be used to draw inferences about some sensitive problems like as respondents' online privacy and security practices and behaviours. Steps were taken to ensure that the research did not subject participants to embarrassment, harm or any other material disadvantage (Bhattacherjee, 2012; Oates, 2006; Saunders *et al.*, 2009).

The University of Witwatersrand's (WITS) ethical requirements, as well as the relevant authorisation, was adhered to (Ethics Clearance Certificate, Faculty of Commerce, Law and Management, University

of the Witwatersrand, Johannesburg, 2018). Formal Research Ethics Committee approval was obtained, refer to **Appendix B**.

4.7. Internal and External Validity

This chapter explains how issues that could affect internal, external validity as well as generalisability for the chosen method for this study's data collection were avoided.

4.7.1. Limitations and Threats to Internal and External Validity

The study's method for collecting data was done online through a survey questionnaire. Potential issues related non-response bias and situations where generalisability and validity of the research results could be questioned was carefully considered by developing the survey questionnaire in a respondent-friendly manner (Bhattacherjee, 2012; Saunders et al., 2009). Clear notices were given to respondents before initiating the survey ensure that they understood the content (Bhattacherjee, 2012; Saunders *et al.*, 2009). Follow-up requests were also performed for the online surveys to make sure that sample data was based on completed surveys. Respondents were also informed about the researcher's obligations towards them in terms of the confidentiality and privacy of their responses to manage risk related to internal and external validity (Bhattacherjee, 2012; Saunders *et al.*, 2009). Also, this review's data collection was performed online, issues such as sampling bias were addressed by using another sampling method that did not exclude those who may not have had the time or immediate access to a computer complete an online survey (Bhattacherjee, 2012; Saunders *et al.*, 2009). This was done by including an anonymous identifier that would allow respondents to continue any incomplete surveys, there were no expiry dates for surveys that were initiated and the survey was distributed via a mobile-friendly format that would allow respondents to access it easily and clearly on different types of mobile devices and computers (Bhattacherjee, 2012; Saunders *et al.*, 2009). As the review is focused on exploring the factors affecting people's online privacy behaviours, issues such as social desirability and common method bias that could have affected research results were closely looked at during analysis of response data (Bhattacherjee, 2012; Saunders *et al.*, 2009). Common method bias may have an impact on the results of the analysed sample data (Bhattacherjee, 2012; Saunders *et al.*, 2009).

Also, to properly assess the external validity and generalisability of the study the researcher considered both the context that it will be administered in: that is, to South African online users that access the Internet predominantly via their mobile phones, as well as administering the online survey to respondents via popular social media platforms in South Africa such as WhatsApp and Facebook. However, as the sampling method adopted for the study is non-probabilistic, this reduces the generalizability of the study's findings such that the similar results in the population cannot be implied from the findings within the sample (Agarwal & Karahanna, 2000b; Brown et al., 2003; Culnan & Armstrong, 1999; Dinev & Hart, 2005; Junglas et al., 2008; Kurfalı et al., 2017; Staff Writer, 2017; Writer, 2014).

Lastly, to avoid potential issues related to external validity and generalisability as the survey's questions were limited to online platforms. The respondent data was also collected at the same time the study's research survey questionnaire was distributed to potential respondents. Furthermore, the online survey instrument distributed to the respondent was the only one developed and used to collect potential respondent data. Therefore, there is no temporal precedence in the data collected that limits causal inferences, and any causal assumptions can only be made with reference to literature and theory. The questionnaire gave examples of the online platforms that were applicable to allow respondents to think

about newer technologies that require PI such a location-based services or sensors that inadvertently share PI online such as smart devices (Junglas, *et al.*, 2008).

4.8. Conclusion

This chapter explained how the research was conducted in terms of the gathering of respondent data as well as how the collected data was analysed. The collection of sample data for studies that involve non-probability sampling of online users are normally done using online questionnaires, so this study adopted the same. A structured questionnaire was used. Ethical considerations were outlined along with limitations of the methods.

5. Data Handling and Cleaning

This chapter outlines the data handling and cleaning steps. This chapter also includes information on the data handling and cleaning processes in preparation for the data analysis as well as the rationale for excluding some responses in further analysis.

5.1. Analysis

The survey questionnaire responses were exported from the eSurvey online tool in an Excel (.XLS) file format to perform the initial data cleaning and analysis. The online survey questionnaire consisted of 38 questions. Responses were codified to be used to gather data to measure the proposed conceptual model's variables. The online survey questionnaire had a total number of 163 respondents. The online eSurvey questionnaire system also indicated that out of the 163 respondents, 16 did not complete all the 38 survey questions: that is, a response is considered incomplete if a respondent had opted to participate in the study by initiating the online survey questionnaire and abandoned the survey after completing some questions. On the other hand, completed survey questionnaires were initiated and all questions were answered until the end of the survey. Analysis of the survey questionnaire responses revealed that 90.2% (147 out of 163) responses were completed and 9.8% (16 out of 163) responses were not completed as illustrated in **Table 5** below:

Table 5: Survey Response and Completion

Responses	**Count of Participation**	**Percentage of Total Participation**
Participated and completed	147	90,2%
Participated but not yet completed	16	9,8%
Grand Total	**163**	**100%**

Of the 16 responses missing data, 11 were missing more than 50% of the questionnaire and were eliminated. The remaining 5 responses had enough data and it was decided to use a mean replacement strategy to impute the missing data. As a result, a total of 147+5=152 responses were considered complete and sufficient for analysis. **Appendix C** presents a detailed explanation of missing data analysis.

Although a sample of 152 seems low, using the judgmental approach as said in chapter 4.2, this study considered that 152 responses from individuals was sufficient to test the research model. This was close to samples sizes for similar studies, and previous statistics-based research indicates that studies with a minimum sample size of 30 generally result in a mean for sample distribution close to a normal distribution that allows researchers to draw significant conclusions on the population they are studying (Alashoor et al., 2017; Henriques, 2018; Oladimeji, 2017; Saunders et al., 2009).

The mean replacement strategy for the five incomplete online survey questionnaires, related to four questions for the study's online survey questionnaire. The variables were Concern for Privacy, Online Trust, Perceived Online Risk and Intention to Share Personal Information, and mean replaced numbers were rounded off to the nearest whole number to fit properly with the answers provided by respondents to study's survey questionnaire, which was measured using Likert-type scales. No questionnaire items were phrased in the negative and therefore no reverse scoring was required., the next consideration

for data cleaning was the potential outliers: that is, any data with extreme values and do not belong to the sample population (Bhattacherjee, 2012; Saunders et al., 2009).

5.2. Conclusion

This chapter discussed the methods used to prepare the respondent data for analysis, including the process of data extraction from the online survey tool that was used to collect responses. The chapter gave a summary of the number of responses completed and those not completed, and this was used as the basis for excluding some responses in further analysis. The next chapter will discuss the results of the statistical analysis performed on the cleaned respondent data.

6. Results

This chapter will explain the data analysis results that were obtained from the online survey questionnaire. The sample demographics are presented and thereafter a discussion of the validity and reliability of the measurement instruments. Factor analysis, as well as PCA, was used to establish the validity and reliability of the study's measurement items. Lastly, the study's hypotheses were tested using bivariate correlation and regression analysis through Pearson's parametric test to show the relationships between the constructs that make up the study's proposed conceptual model.

6.1. Demographic Analysis

As explained at the beginning of this chapter, a total of 163 survey questionnaire responses were received. Some responses were incomplete and not considered for statistical analysis. The useable sample consisted of 152 responses that were used for analysis. Respondents that took part in the survey were based in South African with access to email, Facebook or WhatsApp that were over the age of 18. Respondents were asked their gender, age, level of education, employment status and their province of residence. Respondents were also asked to specify the types of online profiles they used, this included, emails, online shopping accounts, online customer-to-customer marketplace accounts such as online auctions, online municipal bill payment accounts, an online account to ticketing accounts, online gaming accounts, and any other online accounts they wanted to specify. Information obtained from the demographic responses are presented in **Table 6** and **Table 7** below:

Table 6: Respondent Demography

Demography	Category	Frequency	Percentage (percent)
Gender	Female	69	45,4
	Male	83	54,6
Age	18-24 years old	19	12,5
	25-34 years old	67	44,1
	35-44 years old	56	36,8
	45-54 years old	5	3,3
	55-64 years old	3	2
	65-74 years old	1	0,7
	Prefer not to disclose	1	0,7
Education	Completed high school (Matric)	10	6,6
	Post high school certificate/diploma	20	13,2
	Bachelor's degree or equivalent	40	26,3
	Honour's degree or equivalent	33	21,7
	Master's degree	39	25,7
	Doctorate	9	5,9
	Prefer not to disclose	1	0,7
Employment	Employed	111	73
	Not employed	6	3,9
	Prefer not to disclose	2	1,3
	Self-employed	11	7,2
	Student	22	14,5
Province	Eastern Cape	6	3,9
	Gauteng	115	75,7
	KwaZulu-Natal	11	7,2
	Limpopo	1	0,7

Demography	Category	Frequency	Percentage (percent)
	Mpumalanga	1	0,7
	North West	10	6,6
	Northern Cape	1	0,7
	Prefer not to disclose	2	1,3
	Western Cape	5	3,3

Table 7: Respondent Demography Types of Online Accounts

Type of online account	Frequency	Percentage (percent)
Email	147	96,7
Online Banking	129	84,9
Online Shopping	96	63,2
Online Billing	36	23,7
Online Ticketing	34	22,4
Online Gaming	17	11,2
Online Customer-to-Customer Market Place	10	6,6
Other Online Accounts (mostly social media accounts)	8	5,3

Out of the 152 responses the majority were shown as male: that is, 83 (54.6%). However, there was good representation in the sample across gender. Also, most respondents were between the ages of 24-34 years: that is 67 (44.1%), which is in line with the results of sample populations for previous studies similar to this one (Alashoor et al., 2017). Furthermore, majority of the respondents were employed: that is, 111 (73%), and based in the Gauteng province of South Africa: that is, 115 (75.7%), which is in line with the statistics reported about Internet access, connectivity and usage in South Africa (Kayam & Hirsch, 2012; Staff Writer, 2017; STATSSA, 2016; Writer, 2014). Other interesting demographics show that the top three online accounts owned by respondents in descending order are emails: that is, 147 (96.7%), online banking: that is, 129 (84.9%), and online shopping accounts: that is, 96 (63.2%). As the study's research sample population tracks the general South African demographic with access to the internet, the results of the demographic analysis shows that the sample population used to test the relationships as part of the study's proposed conceptual model are statistically representative of the population it is intending to measure (Agarwal & Karahanna, 2000b; Brown et al., 2003; Brown & Buys, 2005; Cameron, 2016; Kurfalı et al., 2017; Oladimeji, 2017; STATSSA, 2016). A few respondents indicated they also had social media accounts. It was not determined in the initial pilot testing that social media accounts were relevant, but it is expected that most respondents would have social media accounts given that penetration is estimated at a total of 63% for widely used tools for social media like Facebook (30%), Twitter (15%), LinkedIn (11%) and Instagram (7%)with South Africa by (Staff Writer, 2017).

As the respondent data was collected at the same time the study's research survey questionnaire was distributed to potential respondents, this short period of evaluation can limit a study's ability to assess changes in constructs and relationships amongst constructs over time, and any causal assumptions can only be made with reference to previous literature and theory (Herrmann & Hirschi, 2013; Neighbors et al., 2006). Considering that the study's survey questionnaire was distributed online some issues regarding generalisability involving response rates as well the completion of the survey questionnaire might have been present (Bhattacherjee, 2012; Cohen, 2017; Duffy et al., 2005; Saunders et al., 2009; Shih & Xitao Fan, 2008). The survey responses also show that the sample population was biased towards educated, economically active males living in the Gauteng region of South Africa who have

access to the Internet. Therefore, claims cannot be made that the research sample population is representative of the South African demography (STATSSA, 2016).

6.2. Analysis of the Measurement Instrument

This study is informed by the positivist paradigm as it tries to understand the relationship involved in the study's proposed conceptual framework through relational and correlational statistical measures. Inherent in this approach of research is the need to assess the reliability and the validity of variable measures.

6.2.1. Convergent and Discriminant Validity

Before performing discriminant and convergent validity analysis, the Kaiser-Meyer-Olkin (KMO) assessments of the appropriateness of sampling was performed to determine if the study's data is suitable for Factor Analysis (Cohen, 2019; Henriques, 2018). Also, Bartlett's test of sphericity was performed to verify that variances were equal for sampled data, and according to this, a sample is said to be significant when the p-value is < 0.001 (Cohen, 2019; Dyer & Keating, 1980). The results in Table 11 show that Bartlett's test of sphericity is significant and the KMO measure is above 0.5. This shows that the use of PCA is appropriate.

Table 8: KMO and Bartlett's Test Results

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0,751
Bartlett's Test of Sphericity	Approx. Chi-Square	2663,215
	df	496
	Sig.	0

Convergent validity is the degree to which measures or items of the same construct relate to each other and converge to the construct which they are supposed to measure (Bhattacherjee, 2012; Gefen, 2002; Oladimeji, 2017; Saunders et al., 2009). On the other hand, discriminant validity is the degree to which the measures or items of a construct diverge from other constructs that should not be the same (Bhattacherjee, 2012; Gefen, 2002; Oladimeji, 2017; Saunders et al., 2009). PCA analysis helps to assure as to both convergent and discriminant validity through the observed pattern of item loadings.

The first, initial PCA was performed on all 32 variable items. Results revealed that five items loaded highly on multiple components (constructs) or loaded less than 0.6 on any component. These were:

- Questions two and five of the Perceived Severity construct.
- Question one of the Self-Efficacy construct.
- Questions four and six of the Intention to Share Personal Information Online construct.

The above items were removed before performing further analysis.

In the next PCA run, there were five items relating to two components that were dropped because of issues with their loading. Table 9 below gives more detail about the relevant items:

Table 9: Second PCA Run Results

Item Number	Item Description	Description of Unstable Observation
Question 1	Perceived Severity	Showed a communality lower than 0.40, and it was not significant as loading to any component was below 0.60.
Question 7	Intention to Share Personal Information Online	Not significant as loading to any component was below 0.60.
Question 8	Intention to Share Personal Information Online	Loaded on a component that it was not intended to measure.
Question 9	Intention to Share Personal Information Online	Not significant as loading to any component was below 0.60.
Question 10	Intention to Share Personal Information Online	Loaded on a component that it was not intended to measure.

Finally, a stable solution emerged. The final PCA results of this stable solution are shown in tables 10, 11 and 12 below.

Table 10: PCA Communalities

	Initial	Extraction
Zscore: SMEAN(ThrtAppPercSev3)	1	0,875
Zscore: SMEAN(ThrtAppPercSev4)	1	0,899
Zscore(ThrtAppPercVul1)	1	0,718
Zscore(ThrtAppPercVul2)	1	0,824
Zscore(ThrtAppPercVul3)	1	0,81
Zscore: SMEAN(CopAppSelfEff1)	1	0,583
Zscore(CopAppSelfEff2)	1	0,769
Zscore: SMEAN(CopAppSelfEff3)	1	0,708
Zscore(CopAppSelfEff4)	1	0,725
Zscore: SMEAN(ConcForPriv1)	1	0,808
Zscore: SMEAN(ConcForPriv2)	1	0,902
Zscore: SMEAN(ConcForPriv3)	1	0,829
Zscore: SMEAN(OnlineTrst1)	1	0,764
Zscore: SMEAN(OnlineTrst2)	1	0,829
Zscore: SMEAN(OnlineTrst3)	1	0,731
Zscore: SMEAN(PercOnlineRsk1)	1	0,751
Zscore: SMEAN(PercOnlineRsk2)	1	0,818
Zscore: SMEAN(PercOnlineRsk3)	1	0,724
Zscore: SMEAN(IntToSharPersInfo1)	1	0,779
Zscore: SMEAN(IntToSharPersInfo2)	1	0,841
Zscore: SMEAN(IntToSharPersInfo3)	1	0,785
Zscore: SMEAN(IntToSharPersInfo5)	1	0,496

Communalities are estimates of the variance in each variable and they show that the variance in each variable is accounted for by all items or measures (Cohen, 2019; Knowledge Center, 2014). For PCA initial communalities always equal to 1.0, and extraction communalities are explained as estimates of the variance in each construct that is accounted for by their items or measures (Cohen, 2019; Knowledge Center, 2014). The communalities in this table are all above 0.3 or preferably above 0.4, which shows that the extracted measures represent the constructs well (Cohen, 2019; Knowledge Center, 2014).

Table 11: PCA Total Variance Explained

Total Variance Explained									
Component	**Initial Eigenvalues (IE)**			**Extraction Sums of Squared Loadings (ESSL)**			**Rotation Sums of Squared Loadings (RSSL)**		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	6,076	27,62	27,62	6,076	27,62	27,62	2,905	13,205	13,205
2	3,127	14,215	41,835	3,127	14,215	41,835	2,647	12,032	25,236
3	2,107	9,579	51,414	2,107	9,579	51,414	2,641	12,006	37,243
4	1,742	7,916	59,33	1,742	7,916	59,33	2,32	10,547	47,79
5	1,492	6,783	66,112	1,492	6,783	66,112	2,308	10,491	58,281
6	1,24	5,634	71,746	1,24	5,634	71,746	2,3	10,455	68,735
7	1,181	5,368	77,114	1,181	5,368	77,114	1,843	8,379	77,114
8	0,818	3,72	80,834						
9	0,675	3,069	83,903						
10	0,51	2,319	86,223						
11	0,448	2,038	88,26						
12	0,392	1,78	90,04						
13	0,348	1,584	91,624						
14	0,324	1,471	93,094						
15	0,288	1,311	94,406						
16	0,263	1,193	95,599						
17	0,241	1,096	96,694						
18	0,202	0,917	97,611						
19	0,174	0,789	98,4						
20	0,143	0,651	99,051						
21	0,12	0,548	99,599						
22	0,088	0,401	100						

The total variance explained for the sample data is in three parts: that is, the Initial Eigenvalues (IEs), the Extraction Sums of Squared Loadings (ESSL) and the Rotation Sums of Squared Loadings (RSSL). There are 22 items in the analysis, and they have a total IE value that sums up to 22, and they account for 100% of the variance explained in the sample data. However, according to the table's IE and ESSL, only seven items have an IE that is greater than one and a cumulative variance value of approximately 77%, which was considered acceptable for further analysis (Cohen, 2019; Knowledge Center, 2014). This also means that the seven items explain most of the variability in the sample data before rotation. The table's RSSL shows the variance explained by the extracted items after rotation (Cohen, 2019; Knowledge Center, 2014).

Table 12: PCA Rotated Correlation Matrix

Rotated Component Matrix							
	Component						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Zscore: SMEAN(ThrtAppPercSev3)							0,913
Zscore: SMEAN(ThrtAppPercSev4)							0,927
Zscore(ThrtAppPercVul1)						0,817	
Zscore(ThrtAppPercVul2)						0,859	
Zscore(ThrtAppPercVul3)						0,812	
Zscore: SMEAN(CopAppSelfEff1)		0,681					
Zscore(CopAppSelfEff2)		0,836					
Zscore: SMEAN(CopAppSelfEff3)		0,77					
Zscore(CopAppSelfEff4)		0,769					
Zscore: SMEAN(ConcForPriv1)			0,786				
Zscore: SMEAN(ConcForPriv2)			0,888				
Zscore: SMEAN(ConcForPriv3)			0,841				
Zscore: SMEAN(OnlineTrst1)					0,822		
Zscore: SMEAN(OnlineTrst2)					0,853		
Zscore: SMEAN(OnlineTrst3)					0,76		
Zscore: SMEAN(PercOnlineRsk1)				0,762			
Zscore: SMEAN(PercOnlineRsk2)				0,882			
Zscore: SMEAN(PercOnlineRsk3)				0,777			
Zscore: SMEAN(IntToSharPersInfo1)	0,848						
Zscore: SMEAN(IntToSharPersInfo2)	0,876						
Zscore: SMEAN(IntToSharPersInfo3)	0,877						
Zscore: SMEAN(IntToSharPersInfo5)	0,65						

Following the emergence of the above stable PCA solution that demonstrates good convergent validity (item measures load highly on their respective constructs) and good discriminant validity (item measures do not load highly on constructs that they are not intended to measure), the study could proceed to the next stage to evaluate the internal consistency reliability of the measures.

6.2.2. Internal Consistency Reliability

Bhattacherjee (2012) posits that internal-consistency reliability is a measure of consistency between different items of the same construct. Internal consistency reliability measures the correlations between various items in a sample test, and the results show that the various items that are meant to measure the same construct produce similar results (Bhattacherjee, 2012; Saunders et al., 2009). Normally internal consistency and reliability are assessed via item Cronbach Alphas and values of 0.7 and above are acceptable (Bhattacherjee, 2012; Cohen, 2019). This shows that the items used to measure a given

construct are consistent and dependable (Cohen, 2019; Knowledge Center, 2014). The study's Cronbach Alpha values for the proposed constructs were calculated using the standardised scores of the response data.

For scale reliability analyses, any corrected item-total correlation values that were lower than 0.4 were removed (Cohen, 2019; Knowledge Center, 2014). It was found that no items had a low-item to total correlation and needed to be eliminated. Thereafter, it was found that the Cronbach Alpha values for all the proposed constructs were shown as either good ($0.8 \leq \alpha < 0.9$) or excellent ($0.9 \leq \alpha$). Construct items that were dropped as part of the PCA analysis were not included in further analysis performed. Overall, the constructs were found to show strong evidence of reliability, and this is illustrated in **Table 13** below.

Table 13: Summary of Measurement Items following PCA and Construct Reliability Tests

Variable/Construct	Original number of measurement items	Number of items removed during PCA	Number of Items Removed after Reliability tests	Final Number of Items Measured	Cronbach Alpha	Reliability Conclusion
Perceived Severity	5	3 (items 1, 2 and 5)	0	2	0.890	Good
Perceived Vulnerability	3	0	0	3	0.835	Good
Self-Efficacy	5	1 (item 1)	0	4	0.814	Good
Privacy Concern	3	0	0	3	0.908	Excellent
Online Trust	3	0	0	3	0.842	Good
Perceived Online Risk	3	0	None0	3	0.840	Good
Intention to Share Personal Information Online	10	6 (items 4, 6, 7, 8, 9 and 10)	0	4	0.852	Good

Following the reliability tests, it was then possible to proceed to calculate composite scores for each of the constructs. As it is impossible for multiple items for being used in correlation and multiple regression analysis, each of the constructs or variables were reduced to their composite scores to allow for correlation and regression analysis (Cohen, 2019). To calculate composite scores only final surviving measurement items were included. The study's composite scores were calculated by taking the arithmetic average of the final set of measurement items weighted equally. Table 14 below illustrates composite scores calculated for the study's variables.

Table 14: Descriptive Statistics of Composite Scores for Variables

Variable/Construct	Final Number of Items Measured	Mean of composite score (unstandardized)	Standard deviation of composite score	Skewness	Kurtosis
Perceived Severity	2	6.401	0.94918	-2.959	9.699
Perceived Vulnerability	3	4.781	0.86720	-0.403	-0.553
Self-Efficacy	4	3.416	0.80128	-0.03	-0.968
Privacy Concern	3	5.453	0.91926	-0.751	-0.372
Online Trust	3	3.771	0.87154	-0.489	-0.081
Perceived Online Risk	3	5.473	0.87012	-0.590	-0.282
Intention to Share Personal Information Online	4	4.055	0.83239	-0.479	-0.213

6.3. Hypothesis Testing and Analysis of the Research Model

The strength of the relationships between the constructs: that is, dependent, independent, moderator and mediating variables, which make up the study's proposed conceptual model was tested using correlation and regression analysis. The specific tests that were used to test the strength of the relationships between the study's variables were bivariate correlation coefficient analysis. For the bivariate correlation coefficient analysis, Pearson's (parametric test) or Spearman's (non-parametric test) can be used. Pearson's test was used for this study as the data collected for this study was mainly interval (Likert-type scales) and the PCA results showed that the data to be used for further analysis was approximately normally distributed. Thereafter, any relationships that were shown to be statistically significant were said to support relevant hypotheses.

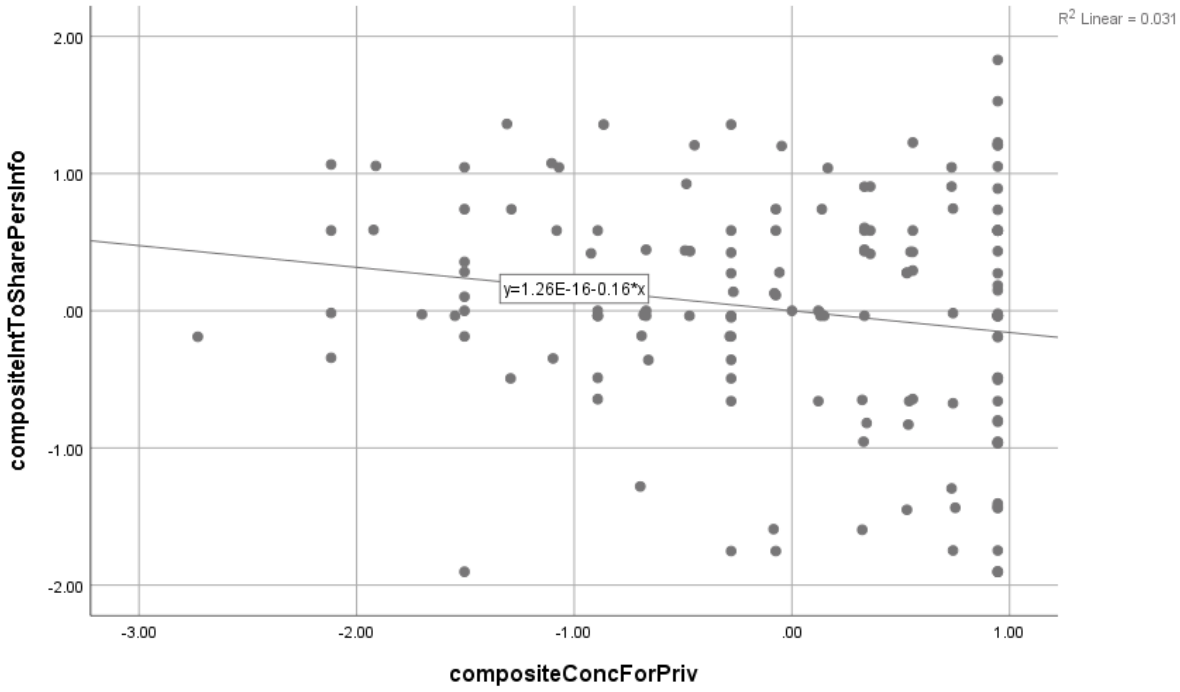
6.3.1. Correlation and Regression Analysis

Correlation, as well as regression analyses, were performed, and this was based on standardized scores before performing the correlation analysis. The first two analysis was with Perceived Severity and Vulnerability as the independent variables and Concern for Privacy as the dependent variable. The remaining three were Self-Efficacy, Concern for Privacy and Perceived Online Risk as the independent variables. Concern for Privacy was also used as the dependent variable for Self-Efficacy and Perceived Online Risk, Online Trust was used as the dependent variable for Perceived Online Risk, and Intention to Share PI Online was used as the dependent variable for Self-Efficacy and Concern for Privacy. The results are shown below.

6.3.1.1. Concern for Privacy and Intention to Share PI Online

Correlation analysis results showed that the relationship between the two variables was statistically significant. The correlation coefficient was found to be -0.175 with a p-value of 0.031. As this p-value was found to be less than the 0.05 level, the results were confirmed as statistically significant. This showed that the relationship between the two variables was strong and confirmed as negatively skewed. Figure 10 below shows the skewness of the relationship. The results suggest that concern for privacy is an independent variable for the intention to share personal information online. Therefore, an individual is less likely to share their PI online if they have a strong concern for privacy and hypothesis one (H1) is supported.

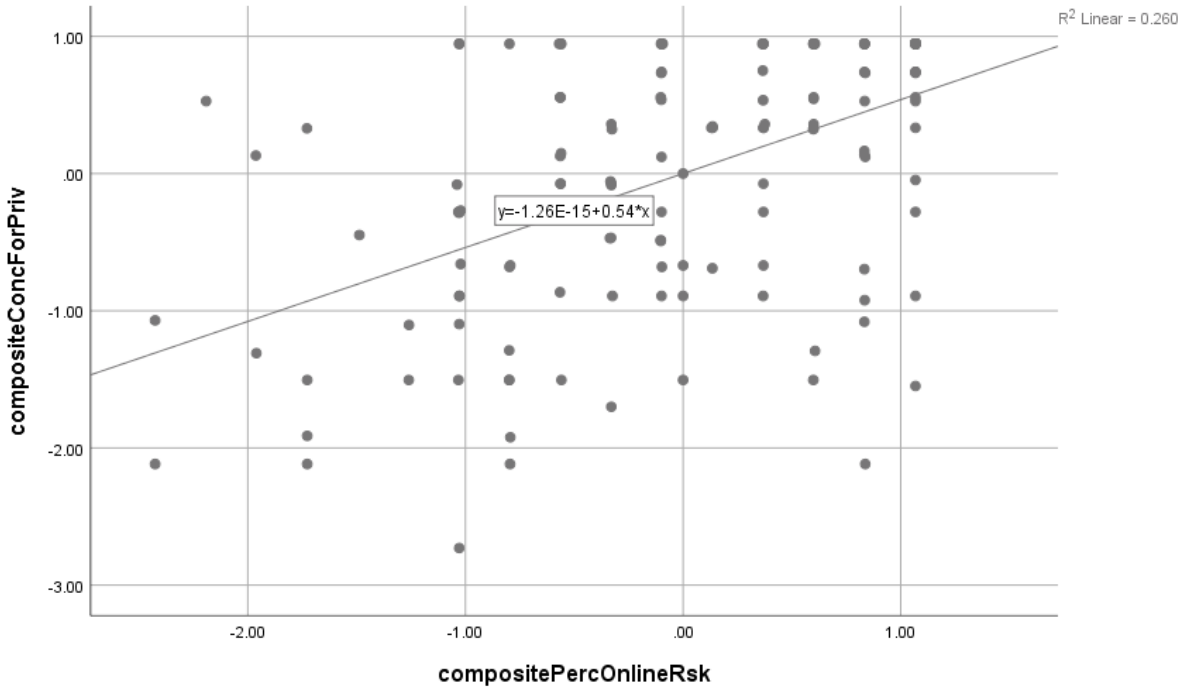
Figure 10: Scatterplot Graph for Privacy and Intention to Share PI Online



6.3.1.2. Perceived Online Risk and Concern for Privacy

Correlation analysis results showed that the relationship between the two variables was statistically significant. The correlation coefficient was found to be 0.510 with a p-value of 0.00. As this p-value was found to be less than the 0.01 level, the results were confirmed as statistically significant. This showed that the relationship between the two variables was strong and confirmed as positively skewed. Figure 11 below shows the skewness of the relationship. The results suggest that online risk is an independent variable for concern for privacy. Therefore, an individual is more likely to be concerned about their privacy if they believe that online platforms pose a risk to their privacy, and hypothesis three (H3) is supported.

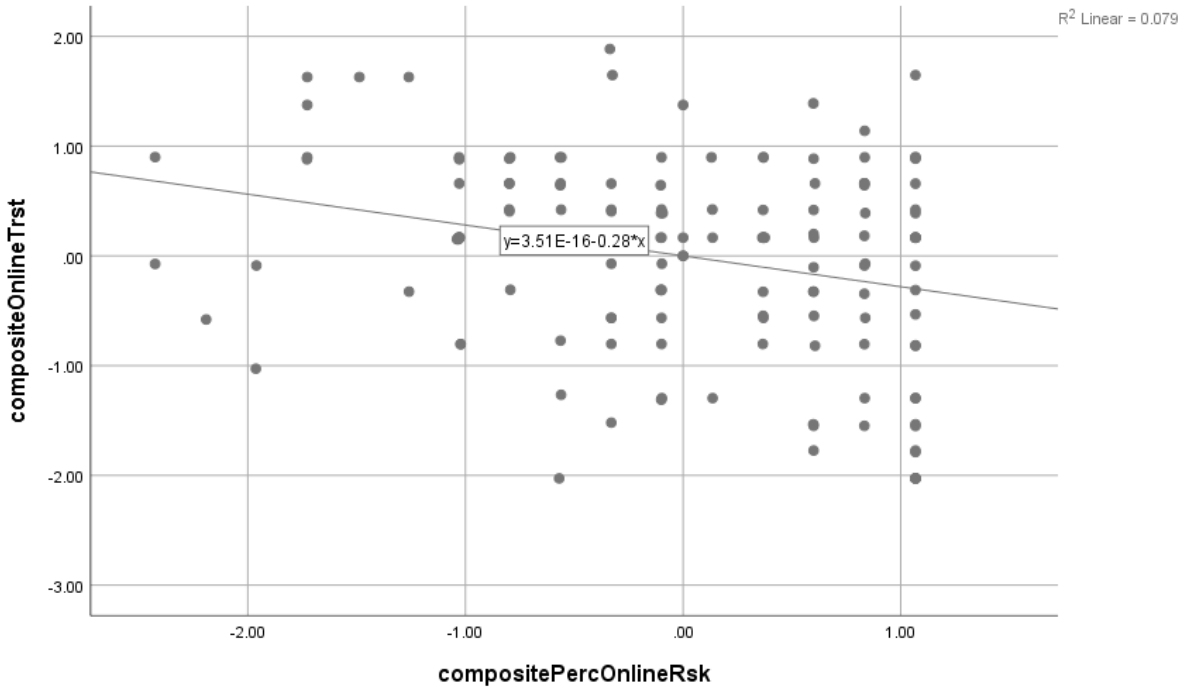
Figure 11: Scatterplot Graph for Perceived Online Risk and Concern for Privacy



6.3.1.3. Perceived Online Risk and Online Trust

Correlation analysis results showed that the relationship between the two variables was statistically significant. The correlation coefficient was found to be -0.280 with a p-value of 0.00. As this p-value was found to be less than the 0.01 level, and the results were confirmed as statistically significant. This showed that the relationship between the two variables was strong and confirmed as negatively skewed. Figure 12 below shows the skewness of the relationship. The results suggest that online risk is an independent variable for online trust. Therefore, an individual is less likely to trust an online platform if they believe that online platforms pose a risk to their privacy, and hypothesis four (H4) is supported.

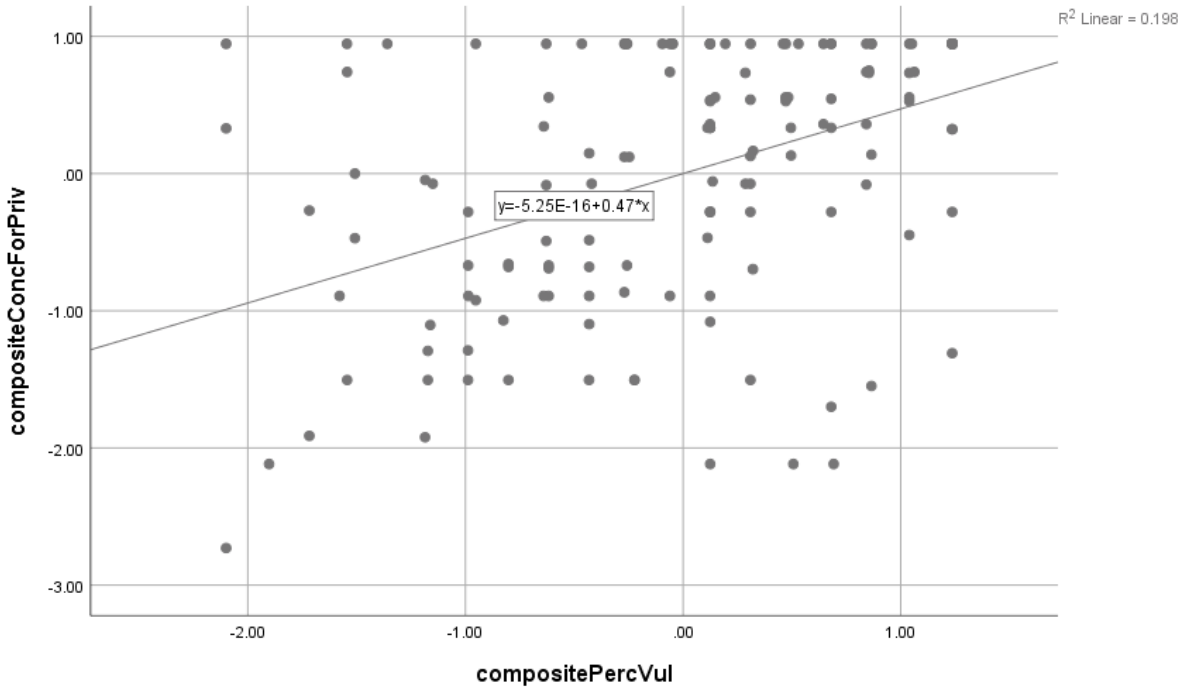
Figure 12: Scatterplot Graph for Perceived Online Risk and Online Trust



6.3.1.4. Perceived Vulnerability and Concern for Privacy

Correlation analysis results showed that the relationship between the two variables was statistically significant. The correlation coefficient was found to be 0.445 with a p-value of 0.000. As this p-value was found to be less than the 0.01 level, the results were confirmed as statistically significant. This showed that the relationship between the two variables was strong and positively skewed. Figure 13 below shows the skewness of the relationship. The results suggest that perceived vulnerability is an independent variable for concern for privacy. Therefore, an individual is more likely to have concern for privacy if they believe that they could be vulnerable to online privacy breaches and hypothesis five (H5) is supported.

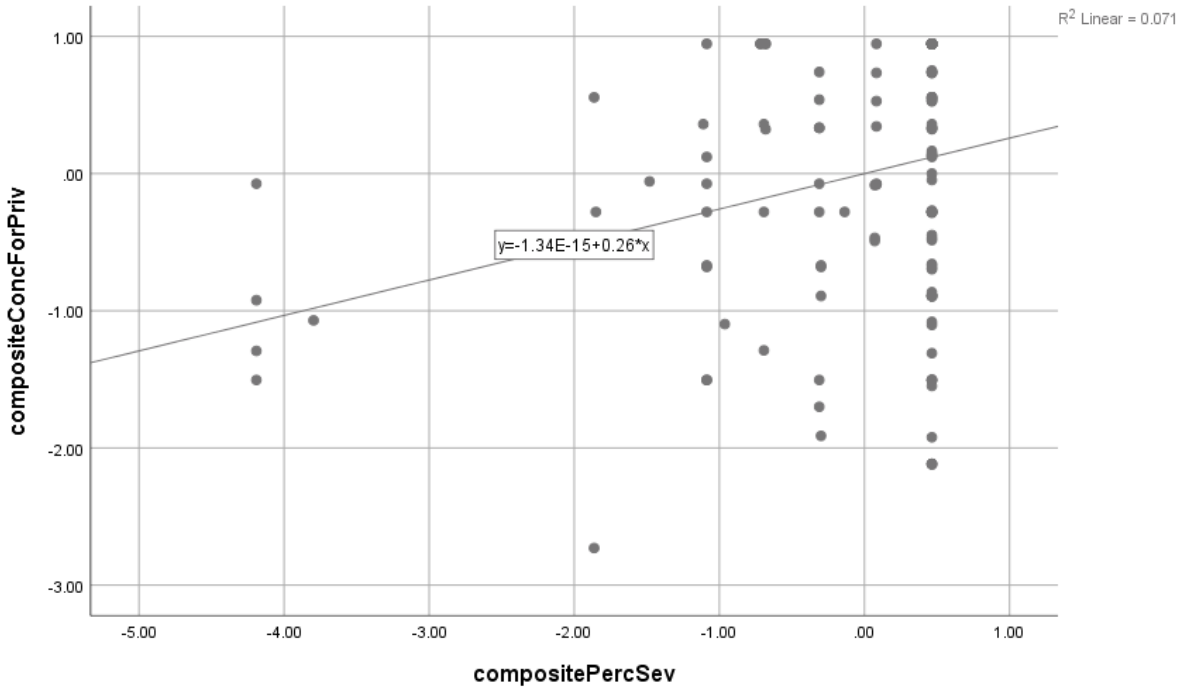
Figure 13: Scatterplot Graph for Perceived Vulnerability and Concern for Privacy



6.3.1.5. Perceived Severity and Concern for Privacy

Correlation analysis results showed that the relationship between the two variables was statistically significant. The correlation coefficient was found to be 0.267 with a p-value of 0.001. As this p-value was found to be less than the 0.01 level, the results were confirmed as statistically significant. The strength of the relationship between the two variables was confirmed as positively skewed. Figure 14 below shows the skewness of the relationship. The results suggest that perceived severity is an independent variable for concern for privacy. Therefore, an individual is more likely to have concern for privacy if they believe that the effect of any breaches to their online privacy could be severe and hypothesis six (H6) is supported.

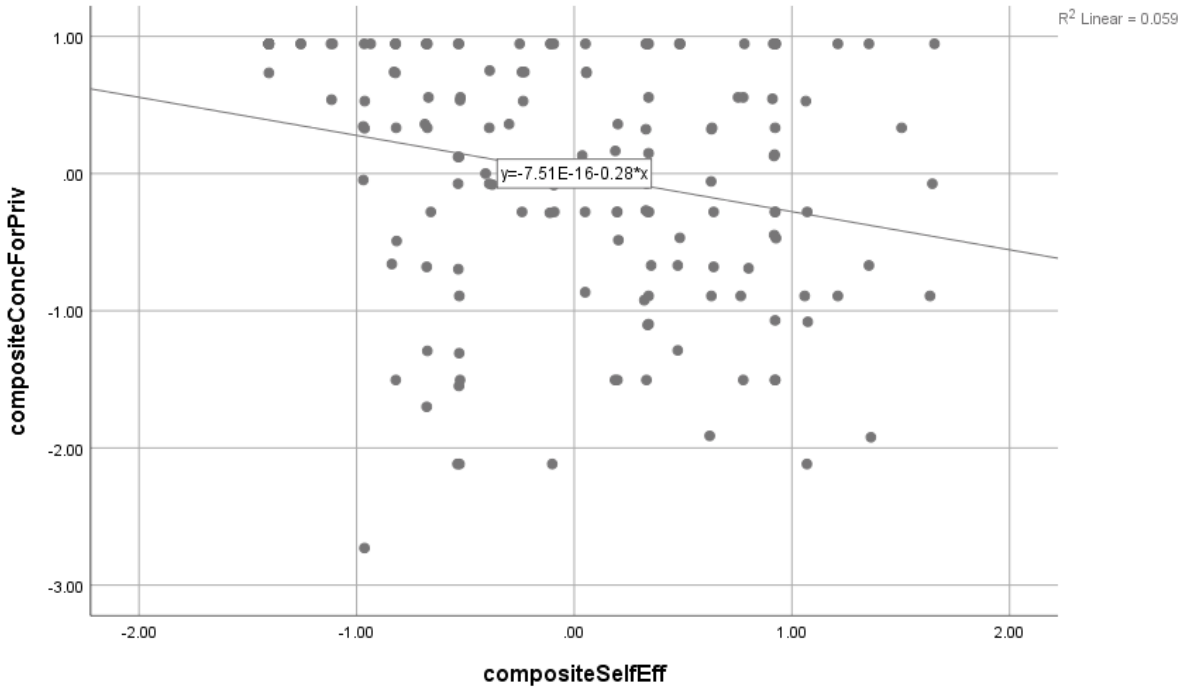
Figure 14: Scatterplot Graph for Perceived Severity and Concern for Privacy



6.3.1.6. Self-Efficacy and Concern for Privacy

Correlation analysis results showed that the relationship between the two variables was statistically significant. The correlation coefficient was found to be -0.242 with a p-value of 0.003. As this p-value was found to be less than the 0.05 level, the results were confirmed as statistically significant. This showed that the relationship between the two variables was strong and confirmed as negatively skewed. Figure 15 below shows the skewness of the relationship. The results suggest that self-efficacy is an independent variable for concern for privacy. Therefore, an individual is less likely to have concern for privacy if they believe that they can protect their privacy and hypothesis seven (H7) is supported.

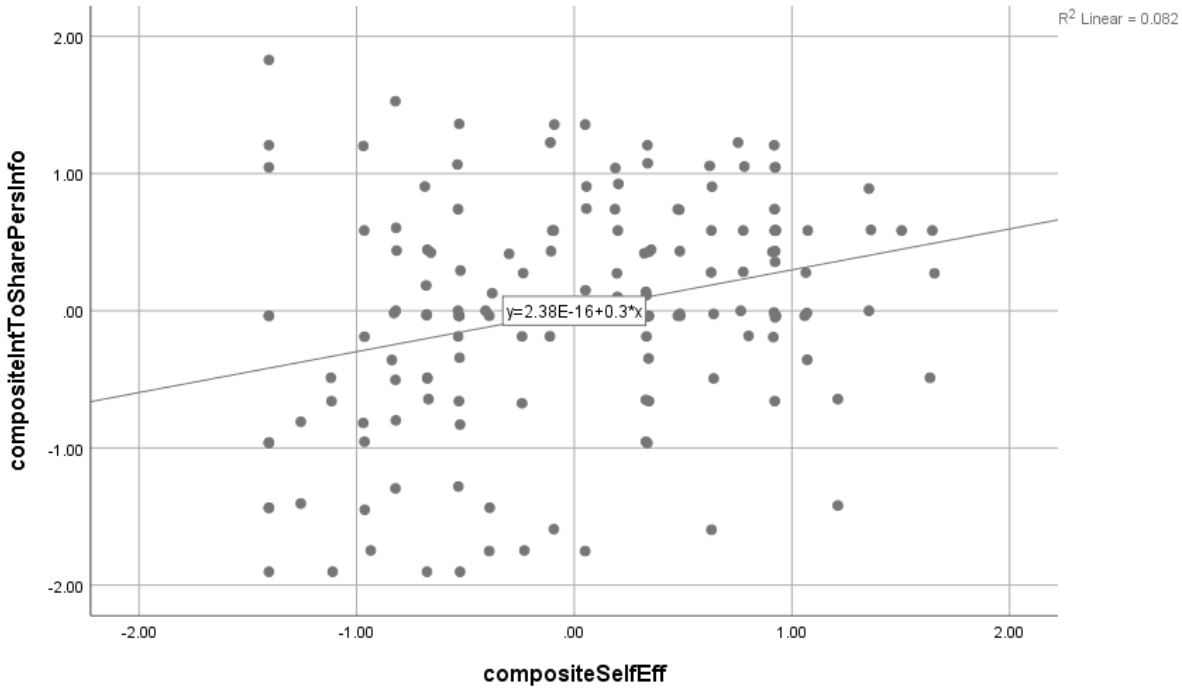
Figure 15: Scatterplot Graph for Self-Efficacy and Concern for Privacy



6.3.1.7. Self-Efficacy and Intention to Share PI Online

Correlation analysis results showed that the relationship between the two variables was statistically significant. The correlation coefficient was found to be 0.287 with a p-value of 0.000. As this p-value was found to be less than the 0.01 level, the results were confirmed as statistically significant. This showed that the relationship between the two variables was strong and confirmed as positively skewed. Figure 16 below shows the skewness of the relationship. The results suggest that self-efficacy is an independent variable for the intention to share personal information online. Therefore, an individual is more likely to share their PI online if they believe that they can protect their privacy and hypothesis eight (H8) is supported.

Figure 16: Scatterplot Graph for Self-Efficacy and Intention to Share PI Online:



6.3.1.8. Moderating Effect of Online Trust

Finally, the analysis of the moderating effect on the link between Concern for Privacy and Intention to Share PI Online was tested. This was achieved through the creation of a new Interaction variable by multiplying the composite variables for Online Trust and Concern for Privacy because moderation is defined as equivalent to statistical interaction (Teo, 2013). Thereafter, linear regression was performed to show the significance of the relationship between the Interaction Variable and Intention to Share Personal Information Online was performed. The R-squared value of Table 15 below illustrates that the moderator summary explains approximately 11.1% of the composition of individuals intention to share PI online. According to the linear regression model as illustrated by Table 16, Concern for Privacy on its own is not a significant predictor of Intention to Share PI Online. On the other hand, Online Trust on its own is a significant predictor of Intention to Share PI Online. However, interaction or the moderating effect of Online Trust on the relationship between Concern for Privacy and Intention to Share PI online is not significant as the p-value is > 0.001. The results suggest that Online Trust is not a moderator the relationship between the Interaction Variable and Intention to Share Personal Information Online.

Table 15: Moderator Model Summary

Model Summary				
Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	.334[a]	0,111	0,093	0,79254
a. Predictors: (Constant), InteractionXandMod, modTrust, xPrivCon				

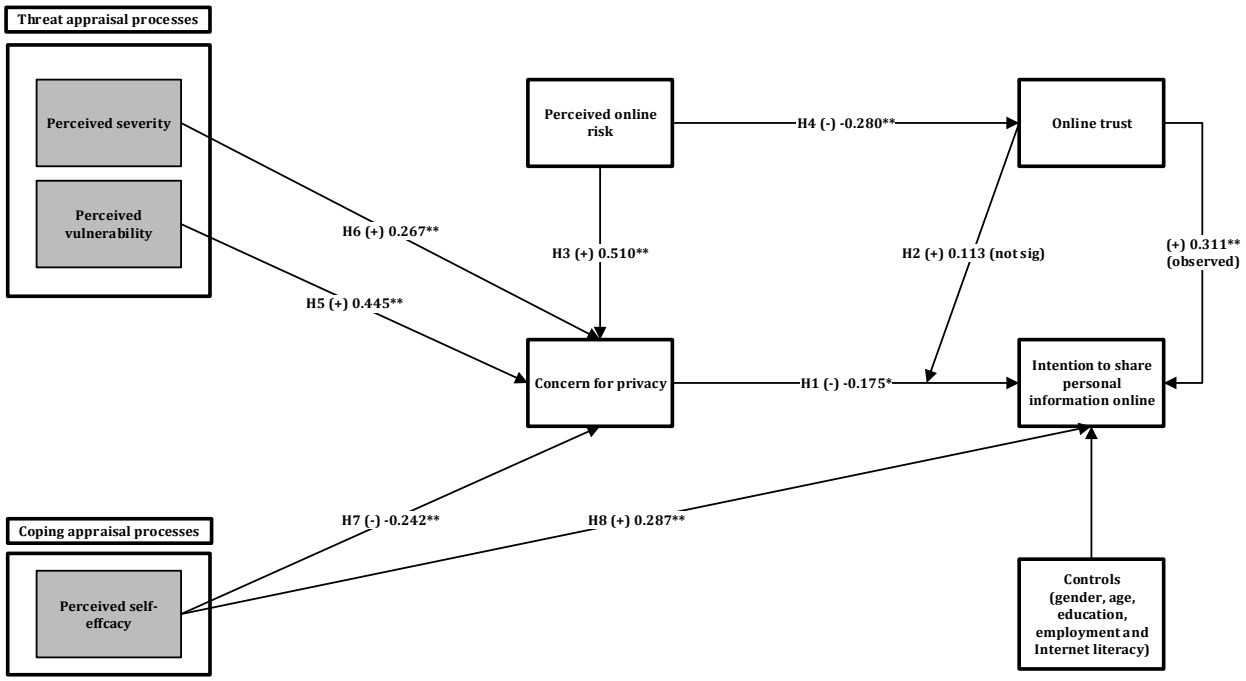
Table 16: Moderator Model Coefficients

Coefficients[a]						
Model		**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**
		B	**Std. Error**	**Beta**		
1	(Constant)	0,025	0,068		0,374	0,709
	xPrivCon	-0,1	0,076	-0,11	-1,303	0,195
	modTrust	0,25	0,08	0,262	3,128	0,002
	InteractionXandMod	0,101	0,087	0,094	1,166	0,246
a. Dependent Variable: yShare						

Based on the correlation and regression analysis performed all hypotheses were supported, except for H2. An updated conceptual model was developed showing that Online Trust is not a moderator the relationship between the Interaction Variable and Intention to Share Personal Information Online, and H2 is not significant.

Figure 16: Summary of Revised Conceptual Model

Note that figures in the arrows are correlation coefficients showing the strength and direction of relationships between the constructs.



Also, multiple linear regression analysis of the strength of the relationships for the various factors that influence privacy concerns was performed. These include the effect of H3, H5, H6 and H7 on concern for privacy. This showed that perceived online risk, perceived severity, and perceived vulnerability made up the strongest and most significant factors influencing privacy concerns and self-efficacy was found to be the least significant factor. Earlier studies have these factors have typically been related to fear appeals that drive behavioural intentions (Boss et al., 2015). This may imply that individuals' privacy concerns are driven more by their perceptions about potential threats and risks of sharing information

online as supposed to the level of trust they have in a service provider or their feelings about how well they know or understand the Internet. Please refer to the multiple regression correlation and coefficient table (Table 17 and 18) below for an explanation:

Table 17: Correlation Strength of Relationships Between H3, H5, H6 and H7 on Concern for Privacy

Correlations						
		compositeConcForPriv	**compositePercOnlineRsk**	**compositePercSev**	**compositePercVul**	**compositeSelfEff**
Pearson Correlation	compositeConcForPriv	1,000	0,510	0,267	0,445	-0,242
	compositePercOnlineRsk	0,510	1,000	0,141	0,277	-0,269
	compositePercSev	0,267	0,141	1,000	0,260	-0,041
	compositePercVul	0,445	0,277	0,260	1,000	-0,114
	compositeSelfEff	-0,242	-0,269	-0,041	-0,114	1,000
Sig. (1-tailed)	compositeConcForPriv		0,000	0,000	0,000	0,001
	compositePercOnlineRsk	0,000		0,042	0,000	0,000
	compositePercSev	0,000	0,042		0,001	0,308
	compositePercVul	0,000	0,000	0,001		0,082
	compositeSelfEff	0,001	0,000	0,308	0,082	

Table 18: Coefficient Strength of Relationships Between H3, H5, H6 and H7 on Concern for Privacy

Coefficients[a]								
Model		**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**	**95,0% Confidence Interval for B**	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	########	0,059		0,000	1,000	-0,117	0,117
	compositePercOnlineRsk	0,405	0,074	0,383	5,501	0,000	0,259	0,550
	compositePercSev	0,128	0,065	0,133	1,973	0,050	0,000	0,257
	compositePercVul	0,310	0,073	0,293	4,230	0,000	0,165	0,456
	compositeSelfEff	-0,115	0,077	-0,100	-1,492	0,138	-0,267	0,037
a. Dependent Variable: compositeConcForPriv								

6.4. Conclusion

This chapter has presented the results of the data analysis for this study. The data analysis started with a demographic analysis that highlighted that the study's respondents were predominantly male, between the age of 25 to 35 with a bachelor's degree or similar, were employed and mostly based in the Gauteng region of South Africa. After that, analysis of the study's measurement instruments was performed through principal components analysis, and this confirmed the discriminant and convergent validity as well as the reliability of the construct items. Lastly, correlation and regression analysis were performed analysis was performed to confirm the strength and direction of the relationships between the proposed construct variables. The regression and correlation analysis were performed to test the study's hypothesis and seven out of eight of the paper's hypothesis were supported: that is, H1 and H3 to H8 and one rejected, that is, H2. A summary of the results and the conceptual model are presented below:

Table 19: Summary of Hypothesis Results

Hypothesis	Description	Result
H1	The greater the concern for privacy, the less likely an individual's intention to share their PI online.	Supported.
H2	Online trust moderates the relationship between concerns for privacy and intentions to share PI online.	Rejected.
H3	The greater the perceived online privacy risk, the more likely an individual will have concern for privacy.	Supported.
H4	The greater the perceived online privacy risk, the more likely an individual will have less online trust.	Supported.
H5	The greater the perceived vulnerability about online privacy, the more likely an individual will have concern for privacy.	Supported.
H6	The greater the perceived severity about online privacy, the more likely an individual will have concern for privacy.	Supported.
H7	The greater the perceived self-efficacy to protect their online privacy, the less likely an individual will have concern for privacy.	Supported.
H8	The greater the perceived self-efficacy to protect their online privacy, the more likely an individual's intentions to share their PI online.	Supported.

7. Discussion

This chapter discusses the study's findings concerning each of the model's constructs. This study explored the factors that influence an individual's privacy concerns and then how this affects their intentions to share their PI online, and this was supported by empirical evidence. PMT constructs as well as the mediating and moderating factors of risk and trust, respectively, were used to hypothesis the effect of an individual's privacy concerns and their intentions to share PI online. The study's results showed that PMT, when extended to include the risk and trust factors, clearly explains the behaviour adopted by individuals to avoid threats. In this case, allowing others the use of one's PI online. The study's data analysis also showed that the constructs, to a greater extent, had the intended effect on an individual's intension to share PI online, as hypothesised.

7.1. Threat Appraisal Processes

Britton et al., (2011) suggests that threat appraisal processes explain the logical and emotional processes and approaches that individuals adopt to evaluate the likelihood or threats of an event. The threat appraisal process is comprised of two main constructs: that is, perceived severity and perceived vulnerability (Milne et al., 2000). These two constructs deal with the intended actions of individuals who believe that they may be exposed to a threat as well as how severe that threat may be (Milne et al., 2000). This study explored how individuals' concern for privacy is influenced by the two main constructs explained here, and after their intention to share PI online.

Therefore, the paper hypothesised that: the greater the perceived vulnerability about online privacy, the more likely an individual will have concern for privacy, and the greater the perceived severity about online privacy, the more likely an individual will have concern for privacy. Results of the study showed that they do not differ with what researchers have concluded for similar studies (Belanger & Crossler, 2019; Mou et al., 2017; Zhang & McDowell, 2009). In summary, the results of this study demonstrated through empirical evidence that individuals will tend to have privacy concerns if they believe that they could seriously be affected by online privacy issues or that they could be vulnerable to privacy issues online, thereby affecting the behavioural intention to share their PI online (Belanger & Crossler, 2019; Mou et al., 2017; Oladimeji, 2017; Zhang & McDowell, 2009).

Furthermore, between the two constructs discussed here, perceived severity proved to be the strongest factor for privacy concerns when it comes to individuals' intention to share personal information. Individuals are however likely to underestimate their chances of suffering from negative experiences: that is, perceived vulnerability tends to be underestimated, and the belief that they have fewer chances of suffering negative experiences may be regarded as one of the things preventing them from greater privacy concerns and being more cautious about sharing their PI online (Mississippi State University et al., 2011; Oladimeji, 2017). Therefore, this shows that individuals tend to be more worried about how privacy issues will affect them online if they share their PI.

7.2. Coping Appraisal Processes

Cromer (2010) posits that coping appraisal processes, as relevant to PMT, are adopted by individuals to determine possible actions for dealing with threats. This process includes three constructs: perceived response efficacy, response cost and self-efficacy. However, response efficacy, response cost has proven to be relevant for information security research that is mainly focused on policy compliance (Milne et al., 2000; Mou et al., 2017). For this study, only the self-efficacy construct was considered. Perceived self-efficacy deals with individuals' beliefs about how well they can deal with potential threats

(Cromer, 2010; Maddux & Rogers, 1983; Youn, 2009). This factor has proven to be an important motivator with how individuals manage their protection strategies as well as when deciding on their behavioural intentions (Youn, 2009). Therefore, this study explored how individuals' concern for privacy and their behavioural intentions are influenced by self-efficacy.

The paper hypothesised that: The greater the perceived self-efficacy to protect their online privacy, the less likely an individual will have concern for privacy and the more likely an individual may want to share their PI online. Results of the study showed that they do not differ with what researchers have concluded for similar studies (Junglas et al., 2008; LaRose et al., 2008). In summary, the results of this study proved through empirical evidence that individuals have lower privacy concerns and are more likely to share their PI if they believe that they know how to manage and protect themselves from potential privacy issues online (Belanger & Crossler, 2019; (Bélanger & Crossler, 2011; Belanger & Crossler, 2019; Cromer, 2010; Dinev & Hart, 2005; Milne et al., 2000; Oladimeji, 2017).Prior research shows that individuals who believe that they know how to transact online and believe that they are competent Internet users generally do not worry about privacy and their behavioural intentions online and will likely share their PI (Dinev & Hart, 2005; Junglas et al., 2008).

Through multiple regression analysis, the study compared the threat and coping appraisal constructs and perceived self-efficacy proved to be less of a significant factor than perceived severity and vulnerability with regards to individuals' privacy concerns. This could be explained by the understanding that coping appraisal is, on average, very important to behaviour: that is, sharing of PI, but not to fear and concern so self-efficacy directly determines the behavioural response: that is, privacy concern (Mou et al., 2017).

7.3. Perceived Online Privacy Risk

Perceived online privacy risk refers to individuals' beliefs that if they share their PI online then there may be a possibility that their PI will not be safe or it will be misused (Cromer, 2010; Dinev & Hart, 2006; Warkentin et al., 2017). This means that when individuals use online services they are primarily concerned about the potential for misuse or uncontrolled loss of their PI and that this involves some protection motivation trade-offs that influence their behaviour intentions: that is, to share PI online (Cromer, 2010; Dinev & Hart, 2006; Milne et al., 2000; Warkentin et al., 2017). It was therefore hypothesized that online privacy is a determining factor for online trust as well as concerns for privacy. This means that, if an individual believes that using an online service is risky then they are likely to have a greater concern for privacy, and by the same token individuals are likely not to trust potentially risky online services. Results of the study showed that they do not differ with what researchers have concluded for similar studies (Cromer, 2010; Dinev & Hart, 2006; Milne et al., 2000; Warkentin et al., 2017).

In summary, the results of this study proved through empirical evidence that perceived online privacy risk is a significant factor influencing both privacy concerns and online trust. Also, the study's proposed conceptual model was based on PMT and was extended to include perceived online risk and online trust. Multiple linear regression analysis of the strength of the relationships for the various factors that influence privacy concerns showed that perceived online privacy risk was the strongest and most significant determinants for privacy concerns. The other influencing factors for privacy concerns that were shown by the study were perceived severity and vulnerability. The risk factor was also found to be an independent predictor in addition to the influence of the two threat appraisal constructs.

This means if an individual believes that using an online service could be risky then the greater will be their concern for privacy, which will shape their behavioural intentions. Further, individuals are inclined to not trust online services they perceive as risky (Cromer, 2010; Dinev & Hart, 2006; Milne et al., 2000; Warkentin et al., 2017). Previous privacy relevant research typically concluded online risk to have a

significant influence on fear, which also has an impact on behavioural intentions (Boss et al., 2015; Oladimeji, 2017). However, this study shows that online risk could be more important than anticipated, especially when it is considered in the context of privacy concerns and intention to share PI online where PMT is extended to include online trust and risk.

7.4. Online Trust

Alashoor et al., (2017) states that online trust can be considered as individuals level of confidence in online services: that is, the level of confidence that individuals may have in the reliability of online services when handling individuals PI (Alashoor et al., 2017). As such, the paper has shown that the relationship between concerns for privacy and intentions to share PI online has an interaction with or is moderated by online trust (Alashoor et al., 2017). Therefore, the study hypothesised that online trust moderates or has a positive influence and interaction on the relationship between concerns for privacy and intentions to share PI online.

For online trust, the results of the study differed with what researchers have concluded previously for similar studies (Alashoor et al., 2017). This means that the interaction effect of online trust on the relationship between concern for privacy and intention to share PI online is not significant and online trust is not a moderator for the relationship as hypothesised. Perhaps an explanation for the differing results could be the treatment of online trust for this study. Earlier privacy research treated online trust in various ways (Junglas et al., 2008; Smith et al., 2011). Some treated online trust as a determinant of privacy concern (Alashoor et al., 2017; Krasnova et al., 2009; Oladimeji, 2017), others treated it as a determinant of disclosure outcomes (Alashoor et al., 2017; Krasnova et al., 2009; Oladimeji, 2017), a mediator between privacy concerns and behavioural intentions (Alashoor et al., 2017; Bansal et al., 2016; Oladimeji, 2017), and some treated it as a moderator of the relationship between privacy concerns and behavioural intentions (Alashoor et al., 2017; Bansal et al., 2016; Belanger et al., 2002; Dinev & Hart, 2005, 2006; Gefen, 2002; Herath et al., 2014; Herath & Rao, 2009; Pennsylvania State University et al., 2011). The different treatments of trust in the context of protection motivation and behavioural intentions implies that understanding its impact on situations that involve privacy disclosure and behavioural intentions is challenging and not fully understood.

The empirical results of this study showed that online trust was not a moderator but did however exert a direct effect on the intention to share personal information (refer Table 16). Therefore, this study has shown that the inclusion of trust has provided a useful extension to the protection motivation model.

7.5. Concern for Privacy

In recent times some modern services such as banking, shopping and bill payments are done online. These require individuals to allow others to use their or in other words to share their PI (Gao et al., 2015; Warkentin et al., 2017). This has increased online privacy concerns, and researchers believe that the basis for privacy concerns are two-fold, namely, individual interactions with technology, specifically the internet, and the social process of interacting with entities that they do not know anything about (Dinev & Hart, 2005). To understand the concept of privacy concerns: individual protection behaviours, and its effect on behavioural intentions this study adopted PMT and extended it to include online risk and online trust. The main PMT constructs that were considered were the threat appraisal (perceived severity and vulnerability) and coping appraisal (perceived self-efficacy) process.

Therefore, the paper hypothesised that the greater the concern for privacy, the less likely individuals will be to share their PI online. Results of the study showed that they do not differ with what researchers have concluded for similar studies (Bélanger & Crossler, 2011; Dinev & Hart, 2005; Junglas et al.,

2008). In summary, the results of this study proved through empirical evidence that individuals are less likely to share their PI online if they have a strong concern for privacy.

7.6. Intention to Share Personal Information Online

Ajzen (1991) suggests that individuals' intended behaviour can be predicted with great accuracy from their intentions towards the behaviour. At the same time, personal principles and beliefs handle a significant influence on actual behaviour. In terms of the study's proposed conceptual model, which was adopted from PMT to include the online risk and trusts constructs, it was shown that individual's online behavioural intentions are influenced by their privacy concerns. This confirmed a central hypothesis pf the protection motivation theory behind online behavioural intentions.

The study also considered individual characteristics that might be involved in individuals' behavioural intentions (Dinev & Hart, 2006; Kurfalı et al., 2017). The controls adopted for this study include age, gender, education and employment status with the understanding that these have a bearing on individuals' access to the internet as well as their proficiency in using the internet (Dinev & Hart, 2006; Kurfalı et al., 2017). Although this study picked up that a majority of the respondents were male, had bachelor's degrees, were employed and were based Gauteng, there were no differences in their responses during analysis.

In summary, the study's results showed that individual's intentions to share PI is driven by their concern for privacy. Furthermore, self-efficacy and trust were shown relevant to behavioural intention. Sometimes individuals overestimated proficiency with something or underestimated their vulnerability to threats (Junglas et al., 2008; Mississippi State University et al., 2011; Oladimeji, 2017). The study showed that the more individuals believed that they were proficient on the internet and understood how to protect themselves from potential privacy issues online the more likely they were to share their PI without considering any or very little protection motivation behaviours. Therefore, behavioural intention to share PI is a complex behaviour that emerges in response to privacy concerns (built on risk, severity and vulnerability), perceptions of the capability to adequately protect their information, and trust in the other party with who the information is being shared.

7.7. Conclusion

This chapter highlighted that the results of the study's statistical analysis supported the majority of the hypotheses and confirmed the factors that affect an individual's intentions to share their PI online. There were identified as mainly the threat and coping appraisal process factors as well as perceived online privacy risk and online trust. This chapter explained that when PMT is extended to include the risk and trust factors it clearly explains the behaviour adopted by individuals to avoid threats related to online privacy: that is, allowing others the use of one's PI online. The next chapter will conclude the paper and provide feedback on the answer to the research question well as discuss the limitations of the study and suggestions for future research.

8. Conclusion

This chapter will discuss the study's findings. This is the closing chapter of this paper, and this study's contribution to information privacy research in general as well as to practitioners will be highlighted here. This chapter provides feedback on the answer to the research question: "What Factors Affect Individual Intentions to Share PI Online?", and gives some context, including limitations of the study, for which the answer should be considered. The chapter closes with some suggestions for future research.

8.1. Overview of Results

This study aimed to improve understanding of the factors that influence individuals' intention to share personal information online. The adopted theory for the paper was PMT as it was better suited to help understand people's protection motivation behaviours and their subsequent behavioural intentions (Smith et al., 2011). The main factors that were considered as part of this review were individuals' concern for privacy and their intention to share personal information online. A few independent factors, as well as a mediating and a moderating factor, were considered. These made up the papers hypothesized conceptual framework. Overall, the conceptual framework included threat appraisal process factors, one coping appraisal process factor as well as the inclusion of online trust and risk factors.

Data was collected from a sample of 163 users/individuals. The total useable sample size was 152. Correlation and regression analysis were used to test the hypothesized effects. Through the empirical evidence, this paper confirmed seven out of the eight hypotheses that were defined.

This paper showed that the threat and coping appraisal process factors of perceived severity and vulnerability as well as self-efficacy were strong antecedents for people's concern for privacy and subsequently their intention to share PI online (Belanger & Crossler, 2019; Mou et al., 2017; Zhang & McDowell, 2009). These results confirm the outcomes of earlier studies in the South African context (Alashoor et al., 2017; Bansal et al., 2016; Belanger et al., 2002; Dinev & Hart, 2005, 2006; Gefen, 2002; Herath et al., 2014; Herath & Rao, 2009; Pennsylvania State University et al., 2011). However, an interesting outcome of the study was the inclusion of online risk and online trust factors. This was an important and novel extension on prior work. Firstly, this paper showed that online trust is not a moderator of the relationship between concern for privacy and the intention to share personal information. Instead, trust emerged as a direct determinant of behavioural intention. Furthermore, trust was influenced significantly by perceived risk. IS privacy researchers should thus consider trust and risk in future research into personal information sharing. The study also showed that when perceived online risk was considered with the other antecedents for concern for privacy: that is, perceived severity, perceived vulnerability and perceived self-efficacy, the factor perceived online risk was the most significant motivator, and self-efficacy was not significant in that context. This suggests that individuals' privacy concerns could be are driven more by their perceptions about potential threats and risks of sharing information online as opposed to how well they think they understand the Internet or know how to use it. Individual's bias towards caring out actions based on fear has been highlighted past privacy research were PMT including fear appeals was adopted (Boss et al., 2015; Oladimeji, 2017). Overall, the study concluded that the threat and coping appraisal factors as well as the involvement of online risk and trust factors affected individuals' privacy concerns and subsequently their intentions to share personal information online.

8.2. Contributions

This paper's contribution to IS privacy research firstly confirmed the relevance of PMT, especially for researcher interesting information privacy. Further to that, that paper confirmed that for IS privacy research where PMT is adopted, trust and risk are factors that researchers need to consider as they have been proven by this study to be more significant antecedents for people's privacy concerns than the normal PMT related factors adopted for this study: that is perceived severity, perceived vulnerability and perceived self-efficacy (Floyd et al., 2000; Maddux & Rogers, 1983). Therefore, through empirical evidence, the conclusions of this research report have also contributed, academically, in terms of a better understanding of the factors that affect individuals' information privacy concerns and their intended behaviours.

Practitioners will benefit from this research report by considering the study's proposed conceptual framework including its relevant factors when developing privacy relevant services. Some considerations for practitioners could be in the form of privacy relevant designs, application features, notices or even the initiation of new or enhancement of old personalised services (Belanger et al., 2002; Pennsylvania State University et al., 2011; Smith et al., 1996). Therefore, a proper understanding of the antecedents on individuals' privacy concerns by practitioners could make the difference between success and failure, especially where they expect individuals to allow them to use their PI. Practitioners should appreciate that individuals are becoming aware of the negative impacts of improper use of their PI, and governments, as well as regulators, are starting to punish institutions that do not handle individuals PI with care (Grootes, 2019; Tlakula, 2017). If practitioners that provide online services and products understand the factors that contribute towards earning the confidence and trust of their users, especially where sharing of PI is essential, they can improve the adoption of their services.

While training programmes might help to strengthen individual self-efficacy for information protection, results here suggest that focus must be on risk mitigation. Regardless of their perceptions of self-efficacy, perceptions of vulnerability and risk of loss must be reduced through programmes focused on the awareness of online privacy risks and the understanding of how to avoid them to build trust in using online platforms.

8.3. Limitations of Study

Even though confirmation of the study's results is based on statistical instruments and methods that have been validated by previous research, the approaches will always have some limitations around internal validity and generalisability (Bhattacherjee, 2012; Oladimeji, 2017; Saunders et al., 2009). This is so because statistical methods allow for some measure of error as well as the context in which the study was performed and how the research data was collected can cause problems with regards to validity and generalisability (Bhattacherjee, 2012; Cohen, 2017; Duffy et al., 2005; Saunders et al., 2009; Shih & Xitao Fan, 2008). The study's research population was focused on a concept that is relatively new in a developing economy like South Africa (Brown et al., 2003; Mooketsi, 2015; STATSSA, 2016). Also, the sample population was biased towards educated, economically active males living in the Gauteng region of South Africa who have access to the Internet. Therefore, claims cannot be made that the research sample population is representative of the South African demography(STATSSA, 2016). As the study's survey questionnaire was distributed online some issues regarding generalisability involving response rates as well the completion of the survey questionnaire were might have been present (Bhattacherjee, 2012; Cohen, 2017; Duffy et al., 2005; Saunders et al., 2009; Shih & Xitao Fan, 2008).

Due to the nature of this study, it was expected that there could be some inherent bias with how individuals would answer the survey questionnaire as it asks probing questions around the information privacy behaviours online which they might not be willing to share truthfully (Bhattacherjee, 2012;

Cohen, 2017; Duffy et al., 2005; Saunders et al., 2009; Shih & Xitao Fan, 2008). Lastly, the cross-sectional timeline of the study should be considered. The data for all variables were collected at the same time using the same instrument so there is no temporal precedence in the data which limits causal inferences, and any causal assumptions should only be made with reference to related research and relevant theories.

8.4. Suggestions for Future Research

Current applications of PMT for information privacy explain clearly the factors involved in privacy concerns as well as individuals intentions to share PI online considering mostly threat and coping appraisal processes (Cromer, 2010; Dinev & Hart, 2006; Milne et al., 2000; Warkentin et al., 2017). However, there has been scant research that explains how factors like risk and trust affect concern for privacy and intention to share personal information (Boss et al., 2015). Therefore, future IS privacy research should consider that trust and risk could be more important to the context of privacy concerns and intention to share PI online than we currently know and understand. In some cases, as with this study, PMT can be extended to include online trust and risk factors.

Closely related to the broadening of internet access as well as the novelty of the privacy concept in South Africa (Cameron, 2016; Mooketsi, 2015; STATSSA, 2016), future researchers should think about increasing their sample population to cover the broader demographics of South Africa, adopting a longitudinal timeline or other sampling and survey methods such as face-to-face interviews, which may help reach interested respondents who were thought of as previously unreachable, perhaps who also do not speak English, as well as help contextualise the privacy concept before participation.

Although the majority of our hypothesis was supported by statistical analysis and agreed with prior research, the prior research was conducted in other contexts such as the Internet, online retail and the use of social media (Alashoor et al., 2017; Dinev & Hart, 2005; Smith et al., 2011). For example, in agreement with the results of this study (Alashoor et al., 2017) found that trust was not a moderator of the relationship between privacy concerns and self-disclosure accuracy. However, the context of the research done by (Alashoor et al., 2017) was based on social networking. As such, future researchers should consider looking at trust as either an independent variable to privacy concerns and/or people's intention to share personal information. Also, such research should be conducted for specific contexts like online banking, online shopping or online bill payments where the PI shared includes some transactional information.

Lastly, PMT and other models that are used to explore and understand individuals' behaviour such as Technology Threat Avoidance Theory (TTAT), Fear-Appeals Model (FAM) and Health Belief Model behavioural should be considered or adapted to allow for further enquiry and understanding as well as theoretical and methodological study around the concept of privacy concerns.

8.5. Conclusion

This chapter gave an overview of the study's results, which were predominantly supported by empirical evidence as well as concurred with prior research. The study's contributions such as the enrichment of our knowledge around the factors that affect people's privacy concerns as well as their intentions to allow others to use their personal information. The limitations of the study relating to validity and generalizability were acknowledged. The limitations were traced to the lack of temporal precedence in the data collected leading to causal inferences. This meant that any causal assumptions that readers want to make can only be done with reference to literature and theory. The chapter closed by giving some suggestions on future assessments that other privacy researchers can perform. In general, it was

suggested that while PMT is an established theory that has been adopted to study privacy concerns, there might be an opportunity to extend PMT by looking at other behavioural models, especially those that include fear-related factors such as risk and trust.

9. References

Agarwal, R., & Karahanna, E. (2000a). Time Flies When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage. *MIS Quarterly*, *24*(4), 665. https://doi.org/10.2307/3250951

Agarwal, R., & Karahanna, E. (2000b). Time Flies When You're Having Fun: Cognitive Absorption and Beliefs about Information Technology Usage. *MIS Quarterly*, *24*(4), 665. https://doi.org/10.2307/3250951

Ajzen, I. (1991). The theory of planned behavior. *Theories of Cognitive Self-Regulation*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with Big Data, Privacy Concerns, and Self-disclosure Accuracy in Social Networking Websites: An APCO Model. *Communications of the Association for Information Systems*, *41*(1), 4.

Albarghouthi, A., D'Antoni, L., Drews, S., & Nori, A. (2016). Fairness as a Program Property. *ArXiv:1610.06067 [Cs]*. http://arxiv.org/abs/1610.06067

Anagnostopoulos, T., Kolomvatsos, K., Anagnostopoulos, C., Zaslavsky, A., & Hadjiefthymiades, S. (2015). Assessing dynamic models for high priority waste collection in smart cities. *Journal of Systems and Software*, *110*, 178–192.

Anderson, C., & Agarwal, R. (2010). Practicing Safe Computing: A Multimedia Empirical Examination Of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613–643.

Anic, I.-D., Budak, J., & Rajh, E. (2016). New Information Economy in Post-Transition Countries: An Economic Approach To Privacy Concern. *Transformations in Business & Economics*, *15*(2).

Armstrong, K. (2014). *Big data: A revolution that will transform how we live, work, and think*.

Ethics Clearance Certificate, Faculty of Commerce, Law and Management, University of the Witwatersrand, Johannesburg, no. CINFO/1192 (2018).

Banisar, D. (2016). National comprehensive data protection/privacy laws and bills 2016. *ARTICLE 19: Global Campaign for Free Expression*.

Banisar, D. (2019). *National Comprehensive Data Protection/Privacy Laws and Bills 2019* (SSRN Scholarly Paper ID 1951416). Social Science Research Network. https://papers.ssrn.com/abstract=1951416

Baskerville, R. L., & Myers, M. D. (2009). Fashion waves in information systems research and practice. *Mis Quarterly*, 647–662.

Bélanger, & Crossler. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017. https://doi.org/10.2307/41409971

Belanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems*, *28*(1), 34–49. https://doi.org/10.1016/j.jsis.2018.11.002

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of*

Strategic Information Systems, *11*(3–4), 245–270. https://doi.org/10.1016/S0963-8687(02)00018-5

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices*. http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1002&context=oa_textbooks

Boss, S., Galletta, D., Lowry, P., Moody, G., & Polak, P. (2015). *What Do Users Have To Fear? Using Fear Appeals To Engender Threats And Fear That Motivate Protective Security Behaviors*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2607190

Botha, J., Grobler, M., Hahn, J., & Eloff, M. (2017). *A High-Level Comparison Between The South African Protection Of Personal Information Act And International Data Protection Laws*. 57.

Boyd, D., & Crawford, K. (2011). *Six provocations for big data*. A decade in internet time: Symposium on the dynamics of the internet and society.

Britton, J. C., Lissek, S., Grillon, C., Norcross, M. A., & Pine, D. S. (2011). Development of anxiety: The role of threat appraisal and fear learning. *Depression and Anxiety*, *28*(1), 5–17. https://doi.org/10.1002/da.20733

Brown, I., & Buys, M. (2005). *Customer Satisfaction with Internet Banking Web Sites: An Empirical Test and Validation of a Measuring Instrument*. *35*, 9.

Brown, I., Cajee, Z., Davies, D., & Stroebel, S. (2003). Cell Phone Banking: Predictors Of Adoption In South Africa—An Exploratory Study. *International Journal of*

Information Management, *23*(5), 381–394. https://doi.org/10.1016/S0268-4012(03)00065-3

Cameron, A. (2016). *Understanding the market and access GAPS present in South Africa's broadband Internet sector*. 80.

Cathy O'Neil: "Weapons of Math Destruction" | Talks at Google. (2016, November 2). https://www.youtube.com/watch?v=TQHs8SA1qpk

Chen, H., Beaudoin, C. E., & Hong, T. (2016). Protecting oneself online: The effects of negative privacy experiences on privacy protective behaviors. *Journalism & Mass Communication Quarterly*, *93*(2), 409–429.

Chen, Y., & Zahedi, F. (2016). Individuals 'internet Security Perceptions And Behaviors: Polycontextual Contrasts Between The United States And China. *MIS Quarterly*, *40*(1). http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3279&context=misq

Clarke, R. (1999). Internet Privacy Concerns Confirm The Case For Intervention. *Communications of the ACM*, *42*(2), 60–67.

Clarke, R. (2016). Big data, big risks. *Information Systems Journal*, *26*(1), 77–90.

Cohen, J. (2017, August 26). *Key Issues In Quantitative Data Collection And Analysis With A Focus on Survey Methods, Lecture Notes Distributed For The Information Systems Masters Course, INFO7012 Research Methods*.

Cohen, J. (2019). *School of Economic and Business Sciences, Information Systems IBM SPSS Workbook*. University of the Witwatersrand, Johannesburg.

Coleman, E. (17 August 2017b.). *Research Methodology, Lecture Notes Distributed for the Information Systems Masters Course, INFO7012 Research Methods*.

Coleman, E. (05 March 2017a.). *Research Questions and The Research Process, Lecture Notes Distributed for the Information Systems Masters Course, INFO7012 Research Methods*.

Conner, M., Norman, P., Boer, H., & Seydel, E. (2005). *Predicting Health Behaviour: Research and Practice with Social Cognition Models*. Open University Press. https://research.utwente.nl/en/publications/protection-motivation-theory-2

Cromer, C. (2010). Understanding Web 2.0's influences on public e-services: A protection motivation perspective. *Innovation*, *12*(2), 192–205.

Culnan, M., & Armstrong, P. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Dinev, T., & Hart, P. (2005). Internet Privacy Concerns And Social Awareness As Determinants Of Intention To Transact. *International Journal of Electronic Commerce*, *10*(2), 7–29.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model For E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80.

Dorjee, K. (2017, February 28). *Power and Sample Size Calculation*. https://www.youtube.com/watch?v=iuBbJIeEUwA

Duffy, B., Smith, K., Terhanian, G., & Bremer, J. (2005). Comparing Data from Online and Face-to-face Surveys. *International Journal of Market Research*, *47*(6), 615–639. https://doi.org/10.1177/147078530504700602

Dyer, D. D., & Keating, J. P. (1980). On the determination of critical values for Bartlett's test. *Journal of the American Statistical Association*, *75*(370), 313–319.

Ellsworth, P. C., & Scherer, K. R. (2003). Appraisal processes in emotion. *Handbook of Affective Sciences*, *572*, V595.

Fichet, C. (2015). *Emerging Data Protection regulations in Africa*. 22.

Fihlani, P. (2017, October 20). Millions caught in SA's "worst data breach." *BBC News*. https://www.bbc.com/news/world-africa-41696703

Floyd, D., Prentice-Dunn, S., & Rogers, R. (2000). A Meta-Analysis Of Research On Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(2), 407–429.

Gao, Y., Li, H., & Luo, Y. (2015). An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems*, *115*(9), 1704–1723. https://doi.org/10.1108/IMDS-03-2015-0087

Gefen, D. (2002). Customer Loyalty in e-Commerce. *Journal of the Association for Information Systems*, *3*(1), 2.

Greengard, S. (2014). Smart transportation networks drive gains. *Commun. ACM*, *58*(1), 25–27.

Griffen, A. (2018, April 30). *Here's why you are getting so many emails from companies at the moment*. The Independent. https://www.independent.co.uk/life-style/gadgets-and-tech/news/gdpr-email-data-privacy-why-sending-companies-opt-in-law-security-explained-a8329986.html

Grootes, S. (2019, October 4). *Information Regulator granted leave to intervene as friend of the court*. SABC News - Breaking News, Special Reports, World, Business, Sport Coverage of All South African Current Events. Africa's News Leader. http://www.sabcnews.com/sabcnews/information-regulator-granted-leave-to-intervene-as-friend-of-the-court/

Henriques, V. (2018). *Assessing the Association between Agile Maturity Model Levels and Perceived Project Success*. University of Cape Town.

Herath, T., & Rao, R. (2009). Protection Motivation And Deterrence: A Framework For Security Policy Compliance In Organisations. *European Journal of Information Systems*, *18*(2), 106–125.

Herrmann, A., & Hirschi, A. (2013). *Calling and career preparation: Investigating developmental patterns and temporal precedence* [Application/pdf]. https://doi.org/10.7892/BORIS.62272

Hussain, A., Wenbi, R., Silva, A., Nadher, M., & Mudhsh, M. (2015). Health and emergency-care platform for the elderly and disabled people in the Smart City. *Journal of Systems and Software*, *110*, 253–263. https://doi.org/10.1016/j.jss.2015.08.041

Johnston, A., & Warkentin, M. (2010). Fear Appeals And Information Security Behaviors: An Empirical Study. *MIS Quarterly*, 549–566.

Johnston, A., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats To The Human Asset Through Sanctioning Rhetoric. *MIS Quarterly*, *39*(1). http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3224&context=misq

Jones, C. L., Jensen, J. D., Scherr, C. L., Brown, N. R., Christy, K., & Weaver, J. (2015). The Health Belief Model as an Explanatory Framework in Communication Research: Exploring Parallel, Serial, and Moderated Mediation. *Health Communication*, *30*(6), 566–576. https://doi.org/10.1080/10410236.2013.873363

Junglas, I., Johnson, N., & Spitzmüller, C. (2008). Personality Traits And Concern For Privacy: An Empirical Study In The Context Of Location-Based Services. *European Journal of Information Systems*, *17*(4), 387–402. https://doi.org/10.1057/ejis.2008.29

Kaisler, S., Armour, F., Espinosa, J. A., & Money, W. (2013). *Big data: Issues and challenges moving forward*. 995–1004.

Katal, A., Wazid, M., & Goudar, R. (2013). *Big data: Issues, challenges, tools and good practices*. 404–409.

Kayam, O., & Hirsch, T. (2012). Using Social Media Networks to Conduct Questionnaire Based Research in Social Studies Case Study: Family Language Policy. *Journal of Sociological Research*, *3*(2). https://doi.org/10.5296/jsr.v3i2.2176

Kemp, R. (2014). Legal aspects of managing Big Data. *Computer Law & Security Review*, *30*(5), 482–491.

Knowledge Center, I. (2014, October 24). *Communalities*. www.ibm.com/support/knowledgecenter/sslvmb_23.0.0/spss/tutorials/fac_cars_communalities_01.html

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards Analysing The Rationale Of Information Security Non-Compliance: Devising A Value-Based Compliance Analysis Method. *The Journal of Strategic Information Systems*, *26*(1), 39–57. https://doi.org/10.1016/j.jsis.2016.08.005

Kurfalı, M., Arifoğlu, A., Tokdemir, G., & Paçin, Y. (2017). Adoption of e-Government Services in Turkey. *Computers in Human Behavior*, *66*, 168–178. https://doi.org/10.1016/j.chb.2016.09.041

Lakens, D. (2017, November 2). *#3 Power Analysis and Sample Size Decisions*. https://www.youtube.com/watch?v=Lr-i4Ugoc5M

LaRose, R., Rifon, N., & Enbody, R. (2008). Promoting Personal Responsibility For Internet Safety. *Communications of the ACM*, *51*(3), 71–76.

Lee, Y., & Larsen, K. (2009). Threat Or Coping Appraisal: Determinants Of SMB Executives' Decision To Adopt Anti-Malware Software. *European Journal of Information Systems*, *18*(2), 177–187.

Liang, & Xue. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, *33*(1), 71. https://doi.org/10.2307/20650279

Lund, J. (2019, November 21). GDPR: What is It and How Does it Impact My Business? *CRM Blog: Articles, Tips and Strategies by SuperOffice*. https://www.superoffice.com/blog/gdpr/

Maddux, J., & Rogers, R. (1983). Protection Motivation And Self-Efficacy: A Revised Theory Of Fear Appeals And Attitude Change. *Journal of Experimental Social Psychology*, *19*(5), 469–479.

Constitution of The Republic of South Africa No. 108 of 1996, no. No. 108 of 1996 (1996). https://www.gov.za/sites/default/files/images/a108-96.pdf

Maughan, K. (2019, August 12). *Ramaphosa granted interdict to halt Mkhwebane's remedial action*. TimesLIVE. https://www.timeslive.co.za/politics/2019-08-12-ramaphosa-granted-interdict-to-halt-mkhwebanes-remedial-action/

Promotion of Access to Information Act 2 Of 2000, no. Act 2 Of 2000 (2000). https://www.justice.gov.za/legislation/acts/2000-002.pdf

Michigan, Y. (1960). Eastern Michigan University. *Exceptional Children*, *26*(5), 278–279. https://doi.org/10.1177/001440296002600509

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106–143.

Mississippi State University, Marett, K., McNab, A., Niagara University, Harris, R., & Indiana University. (2011). Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory. *AIS Transactions*

on Human-Computer Interaction, *3*(3), 170–188. https://doi.org/10.17705/1thci.00032

Mohamed, N., & Ahmad, I. (2012). Information Privacy Concerns, Antecedents And Privacy Measure Use In Social Networking Sites: Evidence From Malaysia. *Computers in Human Behavior*, *28*(6), 2366–2375. https://doi.org/10.1016/j.chb.2012.07.008

Mooketsi, T. R. (2015). Factors Affecting Internet and Broadband Penetration In South African Ordinary Schools. *Faculty of Humanities, University of the Witwatersrand*, 131.

Mou, J., Cohen, J., & Kim, J. (2017). *A Meta-Analytic Structural Equation Modeling Test of Protection Motivation Theory in Information Security Literature*. 21.

Muijs, D. (2004). *Doing quantitative research in education with SPSS*. Sage Publications.

Neighbors, C., Dillard, A. J., Lewis, M. A., Bergstrom, R. L., & Neil, T. A. (2006). Normative misperceptions and temporal precedence of perceived norms and drinking. *Journal of Studies on Alcohol*, *67*(2), 290–299. https://doi.org/10.15288/jsa.2006.67.290

Nussbaum, M. C. (2001). *Women and human development: The capabilities approach* (Vol. 3). Cambridge University Press.

Oates, B. (2006). *Researching Information Systems and Computing*. Sage.

O'Gorman, B., Wueest, C., O'Brien, D., Cleary, G., Lau, H., Power, J.-P., Corpin, M., Cox, O., Wood, P., & Wallace, S. (2019). *Internet Security Threat Report (ISTR)*

(Volume 24). https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

Oladimeji, H. (2017). *Factors influencing the use of privacy settings in location-based social networks*.

O'Neil, C. (2017, April). *The era of blind faith in big data must end*. https://www.ted.com/talks/cathy_o_neil_the_era_of_blind_faith_in_big_data_must_end

Pasluosta, C. F., Gassner, H., Winkler, J., Klucken, J., & Eskofier, B. M. (2015). An emerging era in the management of Parkinson's disease: Wearable technologies and the internet of things. *IEEE Journal of Biomedical and Health Informatics*, *19*(6), 1873–1881.

Pavlou, P. (2011). *State Of The Information Privacy Literature: Where Are We Now And Where Should We Go?* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2369375

Pennsylvania State University, Xu, H., Dinev, T., Florida Atlantic University, Smith, J., Miami University, Hart, P., & Florida Atlantic University. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, *12*(12), 798–824. https://doi.org/10.17705/1jais.00281

Privacy International. (2019, January 26). *State of Privacy South Africa*. Privacy International. https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa

Prothro, J. W., & Grigg, C. M. (1960). Fundamental principles of democracy: Bases of agreement and disagreement. *The Journal of Politics*, *22*(2), 276–294.

Reddy, K. (2012). *On Digital Forensic Readiness for Information Privacy Incidents*. https://pdfs.semanticscholar.org/7bea/8223e0d50187e01bcfc26cd981e134e55a91.pdf

Salleh, N., Hussein, R., Mohamed, N., Abdul Karim, N., Ahlan, A. R., & Aditiawarman, U. (2013). Examining Information Disclosure Behavior on Social Network Sites Using Protection Motivation Theory, Trust and Risk. *Journal of Internet Social Networking & Virtual Communities*, 1–11. https://doi.org/10.5171/2012.281869

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods For Business Students* (5th ed). Prentice Hall.

Shih, T.-H., & Xitao Fan. (2008). Comparing Response Rates from Web and Mail Surveys: A Meta-Analysis. *Field Methods*, *20*(3), 249–271. https://doi.org/10.1177/1525822X08317085

Smith, J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989–1016.

Smith, J., Milberg, S., & Burke, S. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, *20*(2), 167. https://doi.org/10.2307/249477

Sommerlad, J. (2018, May 23). *What do those endless privacy policy update emails mean?* The Independent. https://www.independent.co.uk/life-style/gadgets-

and-tech/news/gdpr-what-is-it-privacy-policy-emails-updates-eu-a8365581.html

Staff Writer. (2017, September 18). *How many people use Facebook, Twitter and Instagram in South Africa*. https://businesstech.co.za/news/internet/199318/how-many-people-use-facebook-twitter-and-instagram-in-south-africa/

Statistics Solutions. (2019). AMOS. *Statistics Solutions*. https://www.statisticssolutions.com/amos/

STATSSA. (2016). *General Household Survey 2016* (Statistical Release P0318; p. 185). http://www.statssa.gov.za/publications/P0318/P03182016.pdf

Studer, B., & Knecht, S. (2016). A benefit–cost framework of motivation for a specific activity. In *Progress in brain research* (Vol. 229, pp. 25–47). Elsevier.

Teo, T. (Ed.). (2013). *Handbook of Quantitative Methods for Educational Research*. SensePublishers. https://doi.org/10.1007/978-94-6209-404-8

Tlakula, P. (2017, March 17). *Press Statement: Information Regulator (South Africa), Ref: CCT 48 / 17*. https://www.justice.gov.za/inforeg/docs/ms-20170317-BST.pdf

Van Niekerk, B. (2017). An Analysis of Cyber-Incidents in South Africa. *The African Journal of Information and Communication*, *20*, 113–132. https://doi.org/10.23962/10539/23573

Van Zyl, G. (2017, October 20). *Biggest ever SA data breach: 60 million ID numbers leaked on real estate server*. BizNews.Com. https://www.biznews.com/global-citizen/2017/10/20/biggest-ever-sa-data-breach/

Warkentin, M., Goel, S., & Menard, P. (2017). Shared Benefits and Information Privacy: What Determines Smart Meter Technology Adoption? *Journal of the Association for Information Systems*, *18*(11), 758–786.

Warkentin, M., Johnston, A., Shropshire, J., & Barnett, W. (2016). Continuance Of Protective Security Behavior: A Longitudinal Study. *Decision Support Systems*, *92*, 25–35. https://doi.org/10.1016/j.dss.2016.09.013

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193. https://doi.org/10.2307/1321160

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*(4), 329–349.

Writer, S. (2014, August 5). *WhatsApp dominates in South Africa*. https://businesstech.co.za/news/mobile/64778/whatsapp-dominates-in-south-africa/

Yazdanmehr, A., & Wang, J. (2016). Employees' Information Security Policy Compliance: A Norm Activation Perspective. *Decision Support Systems*, *92*, 36–46. https://doi.org/10.1016/j.dss.2016.09.009

Yoon, C., Hwang, J.-W., & Kim, R. (2012). Exploring Factors That Influence Students' Behaviors In Information Security. *Journal of Information Systems Education*, *23*(4), 407.

Youn, S. (2009). Determinants Of Online Privacy Concern And Its Influence On Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs*, *43*(3), 389–418.

Zhang, L., & McDowell, W. (2009). Am I Really At Risk? Determinants Of Online Users' Intentions To Use Strong Passwords. *Journal of Internet Commerce*, *8*(3–4), 180–197. https://doi.org/10.1080/15332860903467508

Protection of Personal Information Act No. 4 of 2013 (POPIA), no. Act No. 4 of 2013 (2013). http://www.justice.gov.za/inforeg/docs.html

Commencement of Section 1, Part A of Chapter 5 and Sections 112 And 113 of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013), no. No. R. 25, 2014, Protection of Personal Information Act (2014). https://www.gov.za/documents/protection-personal-information-act-commencement-section-1-part-chapter-52-and-sections

APPENDIX A



UNIVERSITY OF THE
WITWATERSRAND,
JOHANNESBURG

Individual Intentions to Share Personal Information Online

0 %

Page 1

Good Day

My name is Kojo Arthur and I am a Master's student in the Information Systems Division at the University of the Witwatersrand, Johannesburg. I am conducting research on individual intentions to share personal information online. Use of the Internet in the modern context generally requires one to share some personal information. However, sharing such personal information on the Internet may attract some privacy risks to individuals. In such situations some individuals may be willing to share their personal information regardless of the risks and others may be reluctant (recognised as individual privacy concerns).

As individuals based in South Africa, you are invited to take part in this survey. The purpose of this survey is to find out what factors affect individual intentions to share personal online?

Your response is important and there are no right or wrong answers. This survey is both confidential and anonymous. Anonymity and confidentiality are guaranteed by not needing to enter your name on the questionnaire. Your participation is completely voluntary and involves no risk, penalty, or loss of benefits whether or not you participate. You may withdraw from the survey at any stage.

The first part of the survey captures demographic data in an anonymised format. Please tick whichever boxes are applicable. The second part of the survey comprises 32 questions. Please indicate the extent to which you agree with each statement, by ticking in the appropriate box. The entire survey should take between 10 to 15 minutes to complete. The survey was approved by the University of the Witwatersrand, Johannesburg School of Economics and Business Sciences (SEBS) Ethics Committee (Non-Medical), Protocol Number: CINFO/1192.

Thank you for considering participating. Should you have any questions, or should you wish to obtain a copy of the results of the survey, please contact me at kojo.arthur@students.wits.ac.za. My personal contact details: kojo.arthur@gmail.com or phone number: 011 846 1115. My supervisor's name and email are: Professor Jason Cohen - Jason.Cohen@wits.ac.za.

Kind regards

Kojo Arthur
Master's Student: Division of Information Systems
School of Economic and Business Sciences
University of the Witwatersrand, Johannesburg

Page 2

Gender

- ○ Male
- ○ Female
- ○ Prefer not to disclose

Age

- ○ 18-24 years old
- ○ 25-34 years old
- ○ 35-44 years old
- ○ 45-54 years old
- ○ 55-64 years old
- ○ 65-74 years old
- ○ 75 years or older
- ○ Prefer not to disclose

Education

- ○ Some high school
- ○ Completed high school (Matric)
- ○ Post high school certificate/diploma
- ○ Bachelor's degree or equivalent
- ○ Honour's degree or equivalent
- ○ Master's degree
- ○ Doctorate
- ○ Prefer not to disclose

Employment status

- ○ Employed
- ○ Self-employed
- ○ Student
- ○ Not employed
- ○ Prefer not to disclose

Province in which you live

- ○ Eastern Cape
- ○ Free State
- ○ KwaZulu-Natal
- ○ Limpopo
- ○ Mpumalanga
- ○ North West
- ○ Northern Cape
- ○ Western Cape
- ○ Gauteng
- ○ Prefer not to disclose

Please select the types of online accounts or profiles you have.

- ☐ Email
- ☐ Online Shopping
- ☐ Online Customer-to-Customer Market Place
- ☐ Online Billing
- ☐ Online Banking
- ☐ Online Ticketing
- ☐ Online Gaming
- ☐ Other (please state) _____

Page 3

This question relates to your online accounts (e. g. email, online billing, banking or travel bookings).

	Totally Disagree (1)	2	3	Neither Agree Nor Disagree (4)	5	6	Totally Agree (7)
I am often concerned that online service providers do not take enough time and effort to prevent unauthorised access to my online accounts.	○	○	○	○	○	○	○
I am often concerned that information stored on online service providers' computers can be easily accessed by unauthorised people.	○	○	○	○	○	○	○
If any of my online accounts were accessed by unauthorised people it would be a serious problem for me.	○	○	○	○	○	○	○
If any of my passwords were leaked online it would be a serious problem for me.	○	○	○	○	○	○	○

When it comes to severity of Internet security attacks, I believe that:

	Not Serious At All (1)	2	3	Neutral (4)	5	6	Very Serious (7)
The consequences of Internet security attacks for me are...	○	○	○	○	○	○	○

Page 4

To what extent does the following apply to you?

	Totally Disagree (1)	2	3	Neither Agree Nor Disagree (4)	5	6	Totally Agree (7)
I could be subjected to computer crimes.	◯	◯	◯	◯	◯	◯	◯
I feel that I am vulnerable to hacking.	◯	◯	◯	◯	◯	◯	◯
I feel that someone could steal my passwords.	◯	◯	◯	◯	◯	◯	◯

Unless other logical workflows have been specified, the participant will be redirected to Page 5.

Page 5

Are you generally anxious about sharing your personal information in order to use online services like free email, online billing, online banking or travel bookings?

	No	Yes
Answer	◯	◯

Page 6

Please indicate your level of confidence for the following when sharing your personal information online.

	Totally Disagree (1)	2	3	Neither Agree Nor Disagree (4)	5	6	Totally Agree (7)
I am confident to share my personal information online with only an online help facility to guide me.	○	○	○	○	○	○	○
I am confident to share my personal information online because I understand how online service providers treat personal information.	○	○	○	○	○	○	○
I am confident to share my personal information online because protecting my personal information online is easy for me.	○	○	○	○	○	○	○
I am confident to share my personal information online because I am familiar with the security measures for online services.	○	○	○	○	○	○	○

Page 7

Rate the degree to which you agree with the following for online services like free email services, online billing, online banking or travel bookings.

	Totally Disagree (1)	2	3	Neither Agree Nor Disagree (4)	5	6	Totally Agree (1)
I am often worried that my personal information can be easily stolen if I share it online.	○	○	○	○	○	○	○
I am often worried about sharing my personal information online because of many things others can do with it.	○	○	○	○	○	○	○
I am often worried about sharing personal information online because it could be used in many ways I cannot predict.	○	○	○	○	○	○	○

Page 8

Rate the degree to which you agree with the following for online services like free email services, online billing, online banking or travel bookings.

	Totally Disagree (1)	2	3	Neither Agree Nor Disagree (4)	5	6	Totally Agree (7)
Systems provided by online service providers are safe environments to share my personal information.	○	○	○	○	○	○	○
Systems provided by online service providers are reliable environments to perform business transactions.	○	○	○	○	○	○	○
Systems provided by online service providers handle personal information in an acceptable manner.	○	○	○	○	○	○	○

Unless other logical workflows have been specified, the participant will be redirected to Page 9.

Page 9

Rate the degree to which you agree with the following for online services like free email services, online billing, online banking or travel bookings.

	Totally Disagree (1)	2	3	Neither Agree Nor Disagree (4)	5	6	Totally Agree (7)
It is risky to share my personal information online.	○	○	○	○	○	○	○
There would be high potential for loss associated with disclosing my personal information online.	○	○	○	○	○	○	○
There would be too much uncertainty associated with giving my personal information online.	○	○	○	○	○	○	○

Page 10

How willing are you to share your personal information online to...

	Not Willing at All (1)	2	3	Neutral (4)	5	6	Very Willing (7)
Buy things like music, clothes, books, etc., by providing your physical address, credit card and contact details.	○	○	○	○	○	○	○
Buy concert, movie or airline tickets online by providing your physical address, credit card and contact details.	○	○	○	○	○	○	○
Pay accounts online by providing your physical address, credit card and contact details.	○	○	○	○	○	○	○
Sell items on online by providing your physical address and contact details.	○	○	○	○	○	○	○
Register your personal information online so that you can access free email services.	○	○	○	○	○	○	○
Register your personal information online so that you can access your online banking.	○	○	○	○	○	○	○
Register your personal information online so that you can get insurance quotes.	○	○	○	○	○	○	○
Register your personal information so that you can access and participate in online dating.	○	○	○	○	○	○	○
Register your personal information so that you can search and apply for jobs online.	○	○	○	○	○	○	○
Register your personal information so that you can participate in online gaming.	○	○	○	○	○	○	○

APPENDIX B

Faculty of Commerce, Law and Management
University of the Witwatersrand, Johannesburg

School of Economic and Business Sciences
Private Bag X3, WITS, 2050, South Africa • Telephone: +27 11 717 8004 •
email: Siyabonga.Molaba@wits.ac.za

CLEARANCE CERTIFICATE **PROTOCOL NUMBER: CINFO/1192**

PROJECT: **INDIVIDUAL INTENTIONS TO SHARE PERSONAL INFORMATION ONLINE: AN EXTENSION TO THE PROTECTION MOTIVATION THEORY MODEL**

INVESTIGATOR: Kojo Arthur

STUDENT NUMBER: **0609564K**

SCHOOL: SEBS

DATE CONSIDERED: 30 August 2018

DECISION OF THE ETHICS COMMITTEE: Approved

NOTE

Unless otherwise specified this ethics clearance is valid for 1 year and may be renewed upon application.
Please remember to include the protocol number above to your participation letter.

DATE: 04/09/2018 **CHAIRPERSON: Jean-Marie Bancilhon**

cc: Supervisor:

Prof Jason Cohen

SCHOOL OF ECONOMIC & BUSINESS SCIENCES

APPENDIX C

Analysis of the study's online survey responses indicated that there was some missing data for completed and incomplete questionnaires. A breakdown of the data received for the 16 incomplete survey questionnaires was performed to understand how much of the study's survey questionnaire was completed by these respondents. Also, the analysis was performed on all 163 responses to understand how many missing data items there for the various questions that make up the study's online survey questionnaire. The purpose of the above-mentioned exercises was to understand the structure of the responses received to perform the various data cleaning and analysis required.

Analysis of the 16 incomplete responses indicated that one respondent: that is, Respondent 103, completed 58% of the study's online survey questionnaire and responses for the questions or data items related to Online Trust, Perceived Online Privacy and Intention to Share Personal Information Online was not completed. Furthermore, two respondents: that is, Respondents 6 and 27, completed 66% of the study's online survey questionnaire and responses for the questions or data items related to Perceived Online Privacy and Intention to Share Personal Information Online was not completed. Also, only one respondent: that is, Respondent 161, completed 74% of the study's online survey questionnaire and responses for the questions or data items related to Intention to Share Personal Information Online were not completed. Lastly, the remaining 12 respondents: that is, Respondents 7, 13, 17 21, 22, 28, 87, 96, 132, 137, 141 and 142, only completed between 16% and 50% of the survey.

Analysis of the 163 responses revealed that all demographic profile questions competed including the questions regarding the types of online profiles that respondents owned. Questions related to the Threat Appraisal Process variables for the proposed conceptual model had on average six missing data items between them. Perceived Severity had four missing data items and Perceived Vulnerability had seven missing data items. The questions related to the Coping Appraisal Process variable Self-Efficacy had on average 11 missing data items. Questions related to the following variables: Privacy Concerns, Online Trust and Perceived Online Risk, for the proposed conceptual model, had on average 12, 13 and 15 missing data items, respectively. Lastly, questions related to the dependent variable, Intention to Share Personal Information Online had on average 11 missing data items.

The tables below show the results of the frequency count analysis that was performed via pivot tables in Excel for the 16 incomplete responses as well as the missing data items on various questions that make up the study's online survey questionnaire, respectively.

Table Showing an Analysis of Incomplete Responses

Response count for incomplete survey questionnaires										
Respondent Number	**Demographic Profile (total 6 questions)**	**Perceived Severity (total 5 questions)**	**Perceived Vulnerability (total 3 questions)**	**Self-Efficacy (total 5 questions)**	**Privacy Concerns (total 3 questions)**	**Online Trust (total 3 questions)**	**Perceived Online Risk (total 3 questions)**	**Intention to Share Personal Information Online (total 10 questions)**	**Missing Data Count Per Respondent**	**% of Total Questionnaire Completed Per Respondent**
6	6	5	3	5	3	3	missing data	missing data	13	66%
7	6	5	3	1	missing data	missing data	missing data	missing data	23	39%
13	6	5	3	5	missing data	missing data	missing data	missing data	19	50%
17	6	5	3	1	missing data	missing data	missing data	missing data	19	39%
21	6	5	missing data	missing data	missing data	missing data	missing data	missing data	27	29%
22	6	5	3	1	missing data	missing data	missing data	missing data	19	39%

27	6	5	3	5	3	3	missing data	missing data	13	66%
28	6	5	missing data	missing data	missing data	missing data	missing data	missing data	27	29%
87	6	missing data	missing data	missing data	missing data	missing data	missing data	missing data	32	16%
96	6	missing data	missing data	missing data	missing data	missing data	missing data	missing data	32	16%
103	6	5	3	5	3	missing data	missing data	missing data	16	58%
132	6	missing data	missing data	missing data	missing data	missing data	missing data	missing data	32	16%
137	6	5	missing data	missing data	missing data	missing data	missing data	missing data	27	29%
141	6	missing data	missing data	missing data	missing data	missing data	missing data	missing data	32	16%
142	6	5	3	1	missing data	missing data	missing data	missing data	19	39%
s	6	5	3	5	3	3	3	missing data	10	74%

Table Showing and Analysis of Missing Data Items for Survey Questions

Demographic Information						
		Gender	**Age**	**Education**	**Employment**	**Province**
N	**Valid**	163	163	163	163	163
	Missing	0	0	0	0	0

Demographic Information – Type of Online Accounts									
		DemoTypeEmail	**DemoTypeShop**	**DemoTypeMarket**	**DemoTypeBill**	**DemoTypeBank**	**DemoTypeTick**	**DemoTypeGame**	**DemoTypeOther**
N	**Valid**	158	102	10	38	134	36	18	163
	Missing	5	61	153	125	29	127	145	0

Threat Appraisal Processes – Perceived Severity						
		ThrtAppPercSev1	**ThrtAppPercSev2**	**ThrtAppPercSev3**	**ThrtAppPercSev4**	**ThrtAppPercSev5**
N	**Valid**	159	159	158	158	159

	Missing	4	4	5	5	4

Threat Appraisal Processes – Perceived Vulnerability

		ThrtAppPercVul1	ThrtAppPercVul2	ThrtAppPercVul3
N	**Valid**	156	156	156
	Missing	7	7	7

Copying Appraisal Processes – Self Efficacy

		CopAppSelfEffYes2No1	CopAppSelfEff1	CopAppSelfEff2	CopAppSelfEff3	CopAppSelfEff4
N	**Valid**	156	151	152	151	152
	Missing	7	12	11	12	11

Concern for Privacy – Privacy Concerns

		ConcForPriv1	ConcForPriv2	ConcForPriv3
N	**Valid**	151	151	151

	Missing	12	12	12

Online Trust				
		OnlineTrst1	**OnlineTrst2**	**OnlineTrst4**
N	**Valid**	150	150	150
	Missing	13	13	13

Perceived Online Privacy Risk				
		PercOnlineRsk1	**PercOnlineRsk2**	**PercOnlineRsk3**
N	**Valid**	148	148	148
	Missing	15	15	15

Intention to Share Personal Information Online											
		IntToSharPersInfo1	**IntToSharPersInfo2**	**IntToSharPersInfo3**	**IntToSharPersInfo4**	**IntToSharPersInfo5**	**IntToSharPersInfo6**	**IntToSharPersInfo7**	**IntToSharPersInfo8**	**IntToSharPersInfo9**	**IntToSharPersInfo10**
N	**Valid**	147	147	146	146	145	147	147	147	147	147

	Missing	16	16	17	17	18	16	16	16	16	16

Based on the frequency count and data analysis performed above, online survey questionnaires that had not completed more than 50% of the questions were discarded. Therefore, 11 out of the 163 responses received were discarded: that is, Respondents 7, 17, 21, 22, 28, 87, 96, 132, 137, 141 and 142 that are highlighted in the table above. As such, the total number of discarded responses for this study equates to approximately seven percent of the total population of responses received. For this study, 152 responses will be used to evaluate the measures for the proposed conceptual model, and a mean replacement strategy will be applied to the missing data items for this study's five incomplete online survey questionnaires that were included in this studies sample population: that is, Respondents, 6, 13, 27, 103 and 161.