Proposal for Masters Dissertation in Marketing (BUS5000W)

Privacy, Self-Sovereign Identity Technology and the Willingness to Provide Personal Information

Prepared for:

Supervisor: Dr. Benedikt Hirschfelder

Co-Supervisor: Dr. Pragasen Pillay

School of Management Studies

University of Cape Town

Prepared by:

MATTHEW HENDRICKS (HNDMAT008)

DATE: 2020/07/22

Submitted in fulfilment of the requirements for the degree

Of **M.com Marketing** at the University of Cape Town

SCHOOL OF MANAGEMENT STUDIES

UNIVERSITY OF CAPE TOWN

BUS5000W

DECLARATION REGARDING PLAGIARISM

By indicating my signature on this page, I agree to the following:

1. I know that using another person's ideas and pretending that they are one's own constitute plagiarism. I am aware of the potential penalties for this misdemeanour.
2. This project is my own work.
3. I have not allowed, and will not allow, anyone to copy this work with the intention of passing it off as his/her/their own work.

Signed by candidate

2020.07.16

Turnitin Score: 15%

ACKNOWLEDGEMENTS

I would like to thank my parents for their extraordinary support. My parents taught me the value of education at an early stage of my life, and how education combined with hard work can be used to surmount difficult circumstances. I want to also thank my supervisor, Benedikt Hirschfelder for his patience and assistance with this study. He encouraged me to pursue the innovative area of Self-Sovereign Identity Technology, and helped me grow personally and professionally during this period. Lastly, I want to dedicate this study to my 2 year old sister, Hope. This dedication is made to her, despite her love and obsession with pushing the off button of my personal computer, during the key moments of my statistical analysis.

ABSTRACT

The internet has caused an unprecedented increase in the amount of personal information that is available online. This personal information has been harnessed directly by companies, to provide targeted marketing to 3rd parties. It can also be used for a company's own internal marketing communication practices. Further highlighting the importance of personal information, some companies have emerged whose business models depend on the accurate collection, and monetisation of this personal information (Streitfeld, 2018). This has led to interest and concern over the misuse of personal information, and the extent companies should benefit from the acquisition of personal information of consumers and 3rd parties.

Technological innovation, specifically Blockchain Technology has created the possibility to eliminate these actual or perceived abuses of consumer data, and allow consumers to exercise greater control over their personal data. Blockchain Technology can be simply understood as a Microsoft Excel spreadsheet where hundreds of participants continuously verify each entry in the spreadsheet so that no incorrect or fraudulent inputs are made. Specifically, Self-Sovereign Identity Technology, currently in its early stages, may allow consumers to have full control of their consumer data via the Blockchain. This includes, access, distribution and may even allow consumers to monetise their own personal information. If consumers fully embrace Self-Sovereign Identity Technology, businesses will have to rethink and overhaul their data collection, marketing practices and business models. On the other hand, consumers will have to decide what they will do, with the data relating to their digital identity and how they might exchange it for their benefit.

Despite its potential to disrupt the collection of personal information by companies, a scholarly analysis of the use Self-Sovereign Identity Technology and its relationship with a consumer's willingness to share personal information has not yet happened. Thus the aim of this thesis is two-fold. Firstly, to understand what drives a consumer to disclose personal information over the internet. Secondly, to understand the connection between this willingness to disclose personal information, and the use of Self-Sovereign Identity Technology. This is investigated using a survey analysis and primary data. This study aspires to create an academic basis for the examination of Self-Sovereign Identity Technology and its relationship with the willingness of consumers to provide personal information.

In this study several factors were found to affect a South African consumer's willingness to provide personal information online. Based on the prior work of Schoenbachler and Gordon

(2010) and Phelps, Nowak and Ferrel (2000) several perceived risk factors and trust factors were hypothesised to affect this willingness to provide personal information. The trust factors included: *past experience with a company*, *reputation of a company* and *perception of dependability*. The perceived risk factors included: *type of personal information requested*, *consequences and benefits*, *individual consumer characteristics* and *consumer control over information*. All of these factors were found to be significant except for the perception of dependability, which was not supported.

Furthermore, perceived functional value was found to moderate the relationship between individual consumer characteristics and the willingness to provide personal information. Lastly, this study found evidence that a relationship exists between the willingness to provide personal information online and the willingness to use SSI technology. This relationship was found to be strong, and negative.

Contents

CHAPTER ONE: INTRODUCTION

1.1 INTRODUCTION

Knowing one's customer has become an essential part of effective marketing (Moon, 2000). The more information you have on a customer, the better the value you can offer to a customer. This value can take the form of tailored products or more efficient marketing communication (Moon, 2000). Some of this information is easy to obtain and can be gained unobtrusively, using monitoring systems whereas some information is harder to acquire and requires the use of self-disclosures such as in surveys on a computer (Moon, 2000).

The need to know your customer and the benefit it provides to companies is closely related to privacy and the 'right to be let alone' was articulated more than 100 years ago by Warren and Brandeis (1890:195). This 'right to be let alone' is more commonly known as the right to be left alone in today's era. Further, privacy invasions involve the collection, use and disclosure of data on a consumer, without proper authorisation (Wang, Lee & Wang, 1998). This means that data collection and privacy invasions are not an exclusively internet age phenomenon. However, it is likely these invasions were less severe as the internet allows for privacy invasions at unparalleled speed and scope, which was not possible before (Nam *et al.*, 2006).

Self-Sovereign Identity (hereafter referred to as SSI) Technology provides an opportunity to mitigate privacy concerns. This is because SSI technology will allow a consumer to fully control their data, effectively putting consumers, not companies and 3rd parties' in-control of their own data. SSI is type of identity that is completely owned, managed and controlled by the person or corporation the data describes or identifies (Tobin and Reed, 2016). This data is also independent and cannot be taken away from the owner (Tobin and Reed, 2016).

SSI technology is seen as the final evolution of a digital identity. A digital identity can be described as digital or electronic data which is associated with a person in an identity system (Chen, 2007). Blockchain provides a technological basis for SSI. This is because of a method to secure information available using blockchain, called "zero-knowledge proofs". This enables a user to prove a claim (i.e. you have a valid driver's license) without providing any additional details, like your age or name, which you do not wish to share (Kröger, Meyer & Hirschfelder, 2019). This allows for an individual's identity to be truly sovereign in an environment, uncontrolled by any single party (Tobin & Reed, 2016).

Several start-ups have already begun to make the concept of SSI a technological reality. For example, companies like: *Shocard, Uport, Ascribe GMBH, I/O Digital BlockVerify* are already developing blockchain based solutions for identity management (Jacobovitz, 2016). The interest in identity management on blockchain is not limited to start-ups and it has also attracted the interest of government departments such as Homeland Security of the United States, and the Australian Post Office (Jacobovitz, 2016).

The two-fold purpose of this study is to determine the factors that affect a consumer's willingness to provide personal information on the internet, and the association between this willingness to provide personal information and the use of SSI technology.

Main objectives:

1. To determine the factors that affect a South African consumer's willingness to provide personal information online.
2. To determine the relationship between a South African consumer's willingness to provide personal information online and their willingness to use SSI technology.

The willingness to provide personal information, has been investigated extensively in literature and found to have several antecedents (see Phelps, Nowak and Ferrel, 2000; Nam *et al*., 2006; Schoenbachler and Gordon, 2002). On the other hand, literature on SSI technology is limited and focused on implementing SSI technology via the blockchain.

This research seeks to illuminate the connection between the willingness to provide personal information and the use of SSI technology. Adding to the understanding of the willingness of South African (hereafter referred to as SA) consumers to disclose information online is another objective of this research. Although, globally well-researched, research focusing on the information disclosure intentions of SA consumers, can be described as limited. This investigation will be valuable for businesses, regulators, and individuals who have an interest in protecting or obtaining personal information online. Information technology professionals, and professionals interested in SSI technology, will find this research valuable, although not technical from an IT architecture point of view.

This chapter outlines my study. The chapter starts with an explanation of the willingness to disclose personal information and SSI technology. What follows is a presentation of primary and secondary research objectives, as well as the conceptual framework. Next, the

methodology is discussed as well as the significance of this study. A skeleton of the structure of this study is also provided at the end of this chapter.

1.2 RELEVANCE OF RESEARCH

It has been established that concerns linked to privacy and the use of personal information, for marketing optimisation and communication is not a new occurrence. Marketers perceived as early as 1995 that specificity of consumer information contributed to the effectiveness of marketing communication (Light, 1990 as cited by Nowaks and Phelps, 1995). This led to consumers expressing concerns about the methods marketers had used and the data they had collected (Nowak and Phelps, 1995). In fact, the first known reference to privacy or the 'right to be let alone' was articulated more than 100 years ago by Brandeis and Warren (1890).

However, privacy invasions were likely less severe then as the internet now allows for privacy invasions at unparalleled speed and scope, which was not possible before (Nam *et al.,* 2006). This severity has led to a great deal of consumer concern over privacy in the 21st century and the enactment of laws to combat the negative externalities associated with privacy infringement.

Blockchain and SSI technology provides a real opportunity to change the current paradigm of data collection, monetisation and ownership. This has far-reaching implications for marketers who rely on this data, as well as consumers who currently lack significant control over their data. This study aims to lay a foundation to understand SSI technology from a marketer's point of view, and its relationship with a consumer's willingness to currently share their personal information. This means, the study may provide a basis for:

1. The positioning of SSI technology in a marketing context.
2. A greater understanding of SSI technology.
3. A greater understanding of a consumer's willingness to share personal information in SA.

The willingness of consumers to share personal information online can be described as a globally well-researched area that is growing in interest to researchers. However, there is a lack of research that focuses on South Africa. This study focuses on South African consumer to bridge this gap, and contribute to a discussion on how South Africans share and protect their personal information. This can help guide policy makers, consumers, marketers and regulators in South Africa on how to best to navigate the data driven world that we now live in.

Understanding how readily South Africans will adopt a new technology intended to protect their privacy will also be of specific value and interest to regulators, and other stakeholders interested in how to best protect consumers from intrusive data practices.

1.3 SUBSTRUCTURE

In this section, existing literature is described which focuses on a consumers willingness to disclose personal information. This includes a discussion on trust, perceived risk and perceived value. Additionally, literature focusing on SSI technology is outlined. This includes a discussion on security fatigue which will be explained at the relevant time.

1.3.1 Personal Information and Marketing

Personal information is individual-specific data that is not generalised and describes a behaviour or trait of a consumer (Phelps, Nowak and Ferrel, 2000). The willingness of a consumer to disclose personal information, is the extent to which a consumer will provide or withhold this personal information when they are requested to provide it.

Research as early as 1990 noted a change in the way marketers perceived the potential of consumer information (Nowak and Phelps, 1995). The amount and specificity of consumer information was increasingly perceived as contributing to the usefulness of marketing communication (Light, 1990 as cited by Nowaks and Phelps, 1995). This led to consumer concern about privacy in the early nineties. Consumers expressed concern relating to the information marketers had and the methods of collecting this information. For example, an early 1991 Gallup survey revealed consumer concern over what marketers know about them (Hume, 1991 as cited by Nowaks and Phelps, 1995).

Nowaks and Phelps (1995) cited Gary (1991) and Jones and Gardiner (1991) stating that in the early 1990's marketers relied on commercial and public databases as well as data that was made accessible via the ordinary marketing process to gather personal information. Data manipulation techniques were applied thereafter to build a detailed consumer profile.

In the modern era, significantly more data is available to firms due to social media, the growth of the internet and developments in computational technology. Marr (2015) notes this abundance of information and explains that data creation in the recent past is greater than all the data created in the history of mankind. Adding to this, some authors have commented that

electronic commerce may be impossible to conduct without a customer sharing their personal information (Rust, Kannan and Peng, 2002).

A news article by Curran (2018) illustrated the data Google and Facebook may have on any particular individual. Google had 5.5 gigabytes of data on a single person which includes for example: a person's location, a record of emails that have been exchanged, videos that may have been watched, amongst other personal information. The same news article showed that Facebook has approximately 600 megabytes of data on a single person, including messages, files, audio and contacts in one's phone. Facebook, Google and Amazon may retain data for indefinite periods of time and moreover may also sell this data (Tsesis, 2014).

The availability of more data combined with modern processing technology allows businesses to gather extensively and utilise personal data, which was not possible before the beginning of the new millennium (Graeff & Harmon, 2002). Furthermore, competition between marketers has driven a greater use of technology to effectively collect and utilise personal information (Graeff & Harmon, 2002). This stems from an actual or perceived desire by consumers for personalised communication and attention (Graeff & Harmon, 2002). Research as early as 1995, found that the success of marketing communication strategies is perceived to be driven by the specificity and volume of consumer information (Nowak & Phelps, 1995).

Consumer data is intertwined with data brokers, who profit from the selling of personal information to companies. Data brokers or information resellers can be defined as "*companies that specialise in the collection and exchange of personal information.*" (Crain, 2018:90). In 2014, it was estimated that the data brokerage industry was generating more than $200 billion in annual revenue (Mott, 2014). This is likely to be a lot more in 2020.

Crain (2018) explains that data brokering can be split into two dimensions: Information procurement and information monetisation. Information acquisition includes the collection of data in three ways: directly from consumers; data purchases from private and state owned companies; and trawling publicly available information. This type of acquisition is effective and in 2014, a company called Acxiom claimed to have over 3,000 data points for each adult consumers in the United States (Axiom Corporation, 2004 as cited by Crain, 2018). After acquisition, data is sold to private companies at a fee, and used to create products and services (Crain, 2018). Tsesis (2014) notes how consumers are constrained by data brokers because of

a lack of transparency which often leads to a loss of personal control as well as reputational and privacy concerns.

1.3.2 Self-Sovereign Identity Technology and marketing

The term SSI Technology is not fully defined in literature. In this study SSI Technology is defined as system for identity management that permits a person to own and manage their electronic or digital identity. (Mühle *et al*., 2018).

There is a lack of literature that relates to the intersection between marketing and SSI technology. The only literature which focuses on the topic is that of Kröger, Meyer and Hirschfelder (2019) who propose a conceptual model, where SSI technology allows users to have more control over their data and benefit financially from the control of their data. In their model, marketers have greater assurance they receive real data from real people. This eliminates some transaction costs for companies which are associated with data brokers or intermediaries.

Other literature on SSI is mainly technical, conceptual or introductory in nature. Dunphy and Petitcolas (2018) as well as Jacobovitz (2016) evaluated the current solutions that are being developed using SSI technology. Mühle *et al*. (2018) provides an overview of the essential components of SSI and described it from a technical standpoint. Tobin and Reed (2017) provide a good description of the evolution of SSI and essential components of the technology, writing for the Sovrin foundation, a current developer of SSI technology using the blockchain.

Blockchain Bundesverband (2018) wrote a comprehensive overview of SSI explaining the concept, its potential and its implementation. Lastly, Sullivan and Burger (2017) wrote about the revolutionary Estonian e-residency program and the authors discuss the implications of this technology using blockchain with reference to SSI. The paucity of research in this area may be a result of blockchain and SSI being relatively new areas of academic and technological research. As the researcher of this study, and to the best of my knowledge, no existing study has examined the relationship between SSI technology use and a consumer's willingness to disclose personal data.

1.3.3 Theoretical Framework: Use of SSI technology and Security Fatigue as a Moderator

In this section, the theoretical framework used to meet the primary objectives of this research is described. Additionally, literature relating to security fatigue as a moderator between the use of SSI technology and the willingness to share personal information is discussed. This study adopts the definition of security fatigue described by Bada, Sasse & Nurse (2019) who described security fatigue as the stress relating to being highly vigilant and security aware. A moderator impacts the strength and the direction of the association between an independent and dependant variable (Baron & Kenny, 1986).

The measurement of SSI technology was operationalised using the work of Slade *et al.* (2015). Slade *et al.* (2015) focused on understanding why remote mobile payments experienced limited acceptance in developing countries using an adapted Unified Theory of Technology Acceptance (UTAUT) model, originally proposed by Venkatesh *et al.* (2003). Slade *et al.* (2015) examined the constructs: *performance expectancy* and *effort expectancy* as factors which influenced a behavioural intention to use mobile payment technology. Venkatesh *et al*. (2012.) defined performance expectancy in terms of benefits consumers perceive that they will receive from engaging with or using a certain technology. Effort expectancy was defined as how easy a technology is to use, and thus how much effort a consumer must exert to incorporate the technology into their daily lives (*Venkatesh et al.,* 2012).

A construct called security fatigue is proposed as a moderating variable between SSI technology use and the willingness to provide personal information. To the author's knowledge this is a novel concept.

Waite (2010) discussed a security triangle which is indicative that a balance must be created

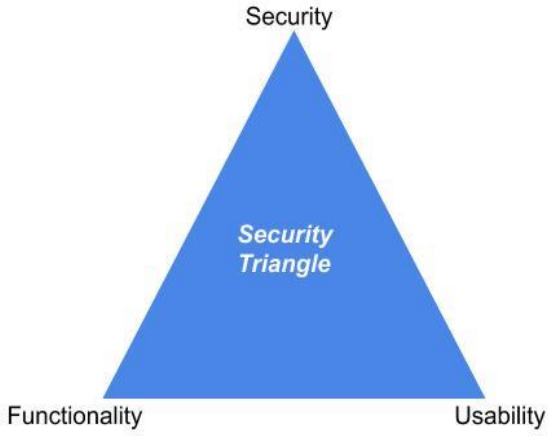

Figure 1. Security Triangle adapted from Waite (2010)

between the conflicting goals of *usability*, *functionality* and *security*. Any security solution needs to find a careful balance between each competing element to be successful. The work of Waite (2010) forms the theoretical basis for understanding security fatigue as a moderator.

Security has been cited as an essential component of SSI technology. As a part of SSI technology it can be described as a requirement that personal information is effectively protected, and that data is only exposed as far as it is necessary to conduct an activity or function (Mühle *et al*., 2018). The emphasis on a security component in SSI technology may come at the expense of usability. Dunphy & Petitcolas (2018) analysed three popular identity management systems that use blockchain (*uPort*, *ShoCard* and *Sovrin*) and found that usability was lacking. This led to the proposal of security, functionality and usability as moderators for the association between the readiness of a consumer to share personal information and the behavioural intention to use SSI technology.

1.3.3 Theoretical Framework: The Willingness to Use Personal Information

In this section, the theoretical framework used to understand and measure the willingness to share personal information is discussed. Specifically, we focus on trust and perceived risk as

the key antecedents of the willingness to share personal information which are proposed in this study.

Trust is a key influencer of a consumer's willingness to disclose personal information. This is inspired by the conceptual model proposed of Schoenbachler and Gordon (2010) (Refer to Figure 2). Other authors such as Hoffman, Novak and Peralta (1999); Milne and Boza (1999); White (2004) have all investigated and found that trust is an important factor, influencing the willingness of consumers to disclose personal information.

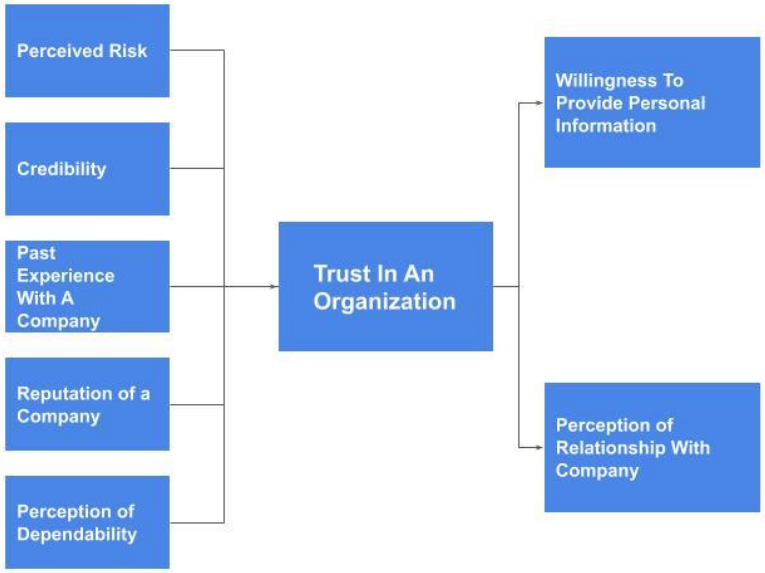

Figure 2. Trust and the Willingness to Provide Personal Information, Schoenbachler and Gordon (2010)

Trust can be defined as a state where expectations are clear and agreed on by both parties (Schoenbachler and Gordon, 2010). The factors that Schoenbachler and Gordon (2010) hypothesised to influence trust were: *perceived risk*, *credibility*, *past experience*, *reputation and dependability*.

Schoenbachler and Gordon (2010) tested their conceptual model using a survey and a regression analysis. Perceived risk, credibility and past experience with the company was found to be influential on trust. Conversely, a significant association between trust and the reputation of a company as well as perception of dependability was found.

When the survey data was analysed on an industry basis it was found that reputation and perceptional dependability still showed a significant relationship with trust. However, past

experience showed a significant relationship with trust, in certain industries (telephone, apparel, computer and catalog industries), with was not seen before. Based on the findings of Schoenbachler and Gordon (2010) past experience with a business and perception of dependability were incorporated as key variables to explain the association between trust and the willingness to disclose personal information.

Another significant factor which has been found to affect the willingness of a consumer to share personal information is perceived risk. In this study, perceived risk is used interchangeably with the term privacy concern which is often cited in literature. More specifically, it is defined as knowledge and measurement of risks related to infringement of a person's privacy (Tan *et al.*, 2012).

Several authors have studied the relationship between privacy concern, or perceived risk and the willingness to provide personal information. For example, authors such as Nam, Song and Park (2006); Sheehan and Hoy (2000); and Malhorta *et al.* (2004) all studied this relationship. However, this study relies on the well-cited work of Phelps, Nowak and Ferrel (2000) as the theoretical basis to describe the relationship between perceived risk and the willingness to provide personal information.

The conceptual framework proposed by Phelps, Nowak and Ferrel (2000) consisted of four input factors. This is indicated in Figure 3. Each of the constructs proposed by Phelps, Nowak and Ferrel (2000) have been incorporated in this study, and will be discussed in more detail.

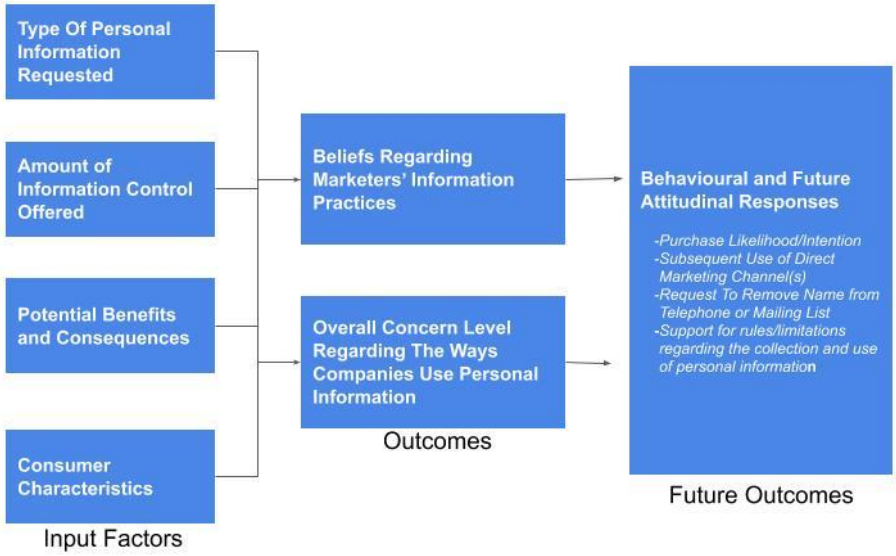

Figure 3. Conceptual Model Proposed by Phelps, Nowak and Ferrel (2000)

Consumers have been found to be less resistant to disclose certain types of information types compared to others. Some authors have found that consumers are less willing to disclose certain information types like race, political and religious views, financial information and medical history (Gupta, Iyer & Weisskirch, 2009; Metzger, 2004). Moreover, the amount of information control a consumer experiences over their personal information, has been found to have an influence on the disclosure attentions of consumers. For example, Milne and Boza (1999) found a negative relationship between disclosure intentions and perceived control, operationalised as awareness of opt-in procedures. Other authors such as Hoadley *et al.* (2011) as well as Phelps, Souza and Nowak (2011) have also found this relationship to be significant.

Equally significantly, consumer characteristics have been found to influence the willingness to disclose personal information. In South Africa, Jordaan (2007) found that age, language, income grouping and gender had an effect on disclosure intentions of consumers. Other authors such as Lee, Wong and Chang (2016) and O'Neil (2001) found consumer characteristics to be significant. When benefits have been offered in-order to gain personal information Phelps, Nowak and Ferrel (2000) discovered that it led to a higher disclosure intention, whereas Wards, Bridges and Chitty (2005) as well as Li, Sarathy and Xu (2010) found it led to less disclosure intentions. Lastly, monetary benefits have been found to positively increase disclosure intentions of consumers (Xie, Teo and Wan, 2006).

1.3.4 Theoretical Framework: Perceived Functional Value as a Moderator

In this section the use of perceived value as a moderator for the relationship between perceived risk, trust and the willingness to share personal information is illuminated upon. Tai (2011)

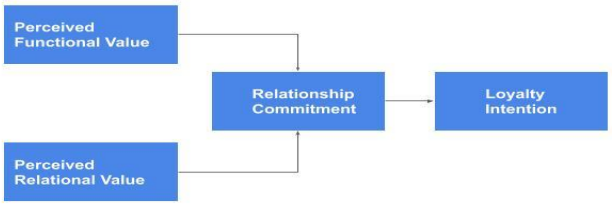

Figure 4. Perceived Value adapted from Tai (2011)

investigated the impact of perceived value on relationship intentions. Relationship intentions were defined by Tai (2011) as a desire by a consumer to create a longstanding relationship with a service or product provider which in turn could lead to a loyalty intention. This loyalty intention decreases the likelihood that a customer will be distracted by competitor offerings, and will thus act in a way that is likely to benefit both trading parties (Tai, 2011). Tai (2011) measured perceived value, with two constructs: perceived functional value and perceived relational value. Perceived functional value can be viewed as relating to the benefit derived from the product or service that a firm provides a consumer (Tai, 2011). Additionally, perceived relational value is a belief that a relationship built with a provider of a good or service, will have benefits in the future (Tai, 2011). The conceptual model proposed by Tai (2011) is illustrated Figure 4. Tai (2011) found that both functional and perceived value had a positive effect on relationship intention.

Not proposed by Tai (2011), in this study perceived value as a moderator. To-date, literature proposing perceived value as a moderator between perceived risk and trust, and the willingness to provide personal information was not found. However, perceived functional value has been found to be significant and impact knowledge sharing. Knowledge sharing was defined by Von der Trenck *et al.* (2015) as providing useful or helpful information when a person is requested to do so. This provides some support for the inclusion of perceived value as a moderator.

Similarly to functional value, relational value has been found to be significant for sharing of information in online or virtual communities by Chiu, Hsu and Wang (2006). These communities can be described as containing the following characteristics: aggregation of

people; rational utility-maximisers; interaction that is not physical; a social exchange process consisting of mutual production and consumption; and social interaction that includes a shared objective (i.e. environmental protection). This provides some support for the inclusion of relational value as a key factor which will have a moderating effect.

The theoretical framework and objectives of this thesis are discussed in the next section. This combines and utilises the aforementioned theoretical frameworks, and combines them into one comprehensive model. The primary and secondary research objectives of this thesis are stated explicitly in the next section.

1.4 THEORETICAL FRAMEWORK AND RESEARCH OBJECTIVES

Many consumers are not cognisant of the personal information that remains on websites after they visit them, nor the value that their data has (Kröger, Meyer and Hirschfelder, 2019). This raises some ethical considerations as individuals which the personal information relates too, do not derive income or benefit from this personal information (Kröger, Meyer and Hirschfelder, 2019 citing Taplin, 2017). Sharing data (knowingly or unknowingly) may also have high costs for consumers if the data is leaked and used fraudulently. For marketers the current paradigm of acquiring data themselves or via third parties may also have high costs. Data acquired directly from consumers could be faked. Marketers are also unable to determine how accurate the data is, that they purchase from intermediaries (Kröger, Meyer and Hirschfelder, 2019).

SSI technology, currently in its infancy, may solve the problems faced by both marketers and consumers. SSI technology allows users to completely own their data, and control its access and distribution, as high privacy protection is embedded into the system (Kröger, Meyer and Hirschfelder, 2019). On the other hand, since the data will be validated, it is more likely that marketers can acquire more accurate data from consumers.

With the above in-mind, this thesis aims to illuminate whether consumers will readily use SSI technology and what relationship this use has with a consumer's current attitude towards sharing personal information. The research is directed by the following research topic. *Self-Sovereign Identity, Privacy and the Willingness of Consumers to Provide Personal Information.* The primary and secondary objectives of the research are restated below.

Primary Objectives:

1. To determine the factors which affect a South African consumer's willingness to provide personal information to a website over the internet.

Secondary Objectives:

2. To determine the relationship between the willingness to provide personal information on the internet and the use of Self-Sovereign Identity Technology, in South Africa.

To understand the willingness to provide personal information and meet the primary objective, this study combined the work of Phelps, Nowak and Ferrel (2000) to understand perceived risk, and the work of Schoenbachler and Gordon (2010) to understand trust. The work of Tai (2011) on perceived value was relied upon, to understand perceived value as a moderator of the willingness to provide personal information and its antecedents. The work of Slade *et al.* (2015) was used to operationalise SSI technology via behavioural intention and its relationship with the willingness to provide personal information. Lastly, the work of Waite (2010) was relied upon to conceptualise security fatigue as a moderator of the aforementioned association between SSI use and the willingness to provide personal information. This final combined theoretical framework is depicted in Figure 5.

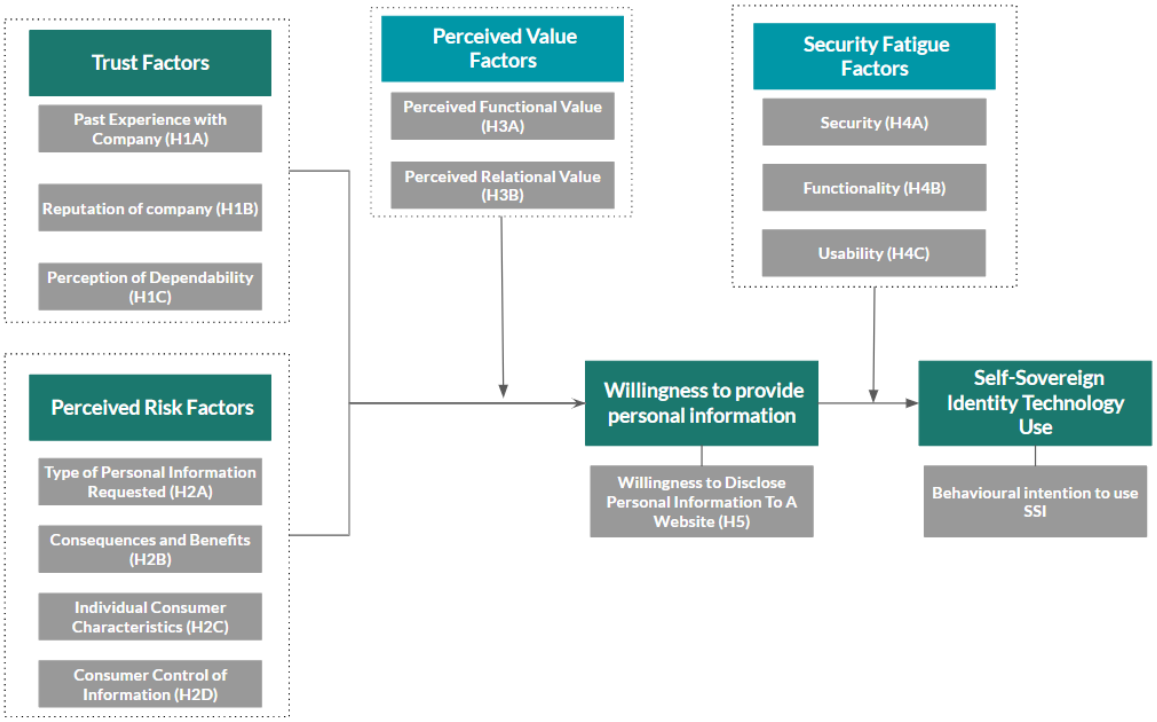

Figure 5. SSI and the Willingness to Provide Personal Information. Theoretical Framework

The theoretical foundations as depicted in Figure 5 are discussed in more detail in later chapters. With the primary and secondary research objectives in mind, as well as the theoretical framework, a set of hypotheses were developed. These hypotheses are depicted below.

Hypothesis 1A:

There is a positive relationship between past experience with a company and the willingness of an online consumer to disclose personal information to a website.

Hypothesis 1B:

There is a positive relationship between the reputation of a company and the willingness of an online consumer to disclose personal information to a website.

Hypothesis 1C:

There is a positive relationship between perception of dependability of a company and the willingness of an online consumer to disclose personal information to a website.

Hypothesis 2A:

There is a positive relationship between the type of personal information requested and the willingness of an online consumer to provide personal information to a website.

Hypothesis 2B:

There is a positive relationship between benefits received and willingness of an online consumer to provide personal information to a website.

Hypothesis 2C:

A younger consumer age has a positive relationship with the willingness of an online consumer to provide personal information to a website.

Hypothesis 2D:

Information control has a negative relationship with the willingness of an online consumer to provide personal information to a website.

Hypothesis 3A:

Perceived functional value moderates the relationship between:

i. Past experience with a company and the willingness of an online to provide personal information on a website.
ii. Reputation of a company and the willingness of an online consumer to provide personal information on a website.
iii. Perception of dependability and the willingness of an online consumer to provide personal information on a website.
iv. Type of personal information requested and the willingness of an online consumer to provide personal information on a website.
v. Benefits received and the willingness of an online to provide personal information on a website.
vi. Individual consumer characteristics and the willingness of an online consumer to provide personal information on a website.
vii. Consumer control over information and the willingness of an online consumer to provide personal information on a website.

Hypothesis 3B:

Perceived relational value moderates the relationship between:

i. Past experience with a company and the willingness of an online consumer to provide personal information on a website.
ii. Reputation of a company and the willingness of an online consumer to provide personal information on a website.
iii. Perception of dependability and the willingness of an online consumer to provide personal information on a website.
iv. Type of personal information requested and the willingness of an online consumer to provide personal information on a website.
v. Benefits received and the willingness of an online consumer to provide personal information on a website.
vi. Individual consumer characteristics and the willingness of an online consumer to provide personal information on a website.
vii. Consumer control over information and the willingness of an online consumer to provide personal information on a website.

Hypothesis 4A:

Security moderates the relationship between the behavioural intention to use SSI technology and the willingness of an online consumer to provide personal information.

Hypothesis 4B:

Functionality moderates the relationship between the behavioural intention to use SSI technology and the willingness of an online consumer to provide personal information.

Hypothesis 4C:

Usability moderates the relationship between the behavioural intention to use SSI technology and the willingness of an online consumer to provide personal information.

Hypothesis 5:

The willingness of an online consumer to provide personal information over the internet has a negative relationship with the behavioural intention to use SSI technology.

1.5 METHODOLOGY

The aim of this study is firstly to demonstrate that trust and perceived risk factors affect the willingness to provide personal information in South Africa; and secondly to prove that the willingness to provide personal information has an influence on the behavioural intention to use SSI technology. This research followed a descriptive approach, by visualising the problem using hypotheses.

A questionnaire was used to prove or disprove the hypotheses. This questionnaire was delivered online and a pilot-test was concluded, to confirm the effectiveness of the questionnaire as well as to verify the theoretical framework which was used. Both these phases are described in Chapter 5. After the preparation and the compilation of a dataset, an analysis was conducted using SPSS and the SmartPLS statistic programs. The next sections describe the details of the methodology used in this study. Measurement and scaling are described in detail, as are design, sampling, preparation, analysis and data collection.

1.5.1 Measurement and scaling

A negligible amount of literature and secondary data exists that focuses on the willingness to provide personal information and its relationship with the behavioural intention to use SSI technology. This made it necessary to evaluate primary data via a questionnaire. This questionnaire was divided into seven broad constructs, with 3 to 4 questions relating to each variable in the construct. The 7 broad constructs were:

1) Trust in an Organisation
2) Perceived Risk
3) Perceived Value
4) Willingness To Provide Personal Information
5) Security Fatigue
6) Self-Sovereign Identity Technology Use
7) Socioeconomic

The socioeconomic construct contained questions on age, and geographical location to ensure that the respondents met the criteria for the intended demographic group. This thesis adopted a single cross-sectional design which involves drawing a sample of respondents from the intended population, and this information is extracted only one time (Birks and Malhorta, 2006). This study also utilised a non-comparative scaling technique. This is method where each object undergoes independent scaling, and is not scaled jointly with other objects in the set (Birks and Malhorta, 2006). The specific non-comparative scaling technique that was used was an itemised scale, called a 7-point Likert scale. Three positive and three negative options are provided to the respondent, with one neutral option. A neutral option was provided, as some users may not understand the technicalities of SSI technology, or fully comprehend what personal information is.

This approach is somewhat supported by existing literature. Schoenbachler and Gordon (2002), Phelps, Nowak and Ferrel (2000) and Tai (2011) all used Likert scales, which varied from 7-point to 6-point scales.

1.5.2 Questionnaire Design

Birks and Malhorta (2006) describe a questionnaire as a set of questions which are used to solicit data from a respondent. Appropriate consideration was taken for ethical considerations, as the survey involves human subjects. Thus, the questionnaire met and incorporated the relevant ethical requirements (see Appendix A).

At the start of the survey a lengthy extract explains the intention of the research to the respondents. In Part 1 a brief explanation is provided on what personal information is; in Part 3 self-sovereign identity technology is explained, which includes a video a respondent can watch. These were attempts to surmount a respondent's potential reluctance to answer the survey because they did not understand the questions related to SSI technology. This is aligned

with the view of Birks and Malhorta (2006) who suggest the researchers must try to entice a respondent to answer and reduce any unwillingness they may have.

Conforming to the recommendation of Birks and Malhorta (2006), basic information is acquired first and identification and classification is only included in the final part of the survey. Birks and Malhorta (2006) recommend this ordering as classification and identification information may alienate respondents, if it is asked first.

1.5.3 Sampling

The objective of a marketing research project is to obtain information about a population (Birks and Malhorta, 2006). This study obtains information from the population using a sample, instead of census. A sample is a portion or subgroup of a population (Birks and Malhorta, 2006). In this study the budget for obtaining information from the population was small and the time available was short. In line with the views of Birks and Malhorta (2006) this led to the use of a sample as opposed to a census.

The target population can be described as respondents currently residing or have resided in South Africa. The age of respondents are limited to individuals who are 18 years and older. Minors were not of specific interest to the study, and were excluded.

Non-probability sampling was used, and specifically convenience sampling. Convenience sampling does not utilise probability (Birks and Malhorta, 2006). For this form of sampling an interviewer obtains sampling units, based on what is most easily available to the interviewer (Birks and Malhorta, 2006).

The sample size was set at 300 usable questionnaires. The survey was created using the software Survey Monkey and was distributed and answered online. It was distributed to respondents in the researchers own network, and shared on social media networks as widely as possible.

1.5.4 Data Gathering and Preparation

Data gathering was conducted over the internet and disseminated among the network of the researcher. Data gathering was limited to the 2nd of June 2020 to the 23rd of June 2020.

Following the preparation of a preliminary plan of data analysis, the questionnaire was analysed for completeness. Afterwards, responses that were incomplete were discarded. The next step prescribed by Birks and Malhorta (2006) was editing. In this step responses were reviewed to increase accuracy and precision. No edits were needed. Survey Monkey allows a

user to make questions ‘required’. All the questions in the survey were set as required. This means a user has to answer all the questions to complete the survey. A limit was also set for a question, so that a user could only select one response. This ensured that responses were both accurate and precise.

Regarding coding and transcribing, Survey Monkey automatically codes and transcribes each question. Following this step, the data was also cleaned which combined the handling of omitted responses and an analysis of the consistency of the data.

The software used to create the survey and collect data (Survey Monkey) cannot prevent a user from failing to complete the survey. This meant that the data contained missing responses. A missing response can be described as a variable which is not known because the answers cannot be interpreted or they have not been recorded properly (Birks and Malhorta, 2006). No statistical adjustment was conducted for the data which was collected.

1.5.5 Statistical Considerations

Descriptive and inferential analyses were conducted on the survey results. Descriptive statistics describe the most essential aspects of data in a study (Trochim, n.d.). The descriptive statistics were analysed using Microsoft Excel as well as by using the statistics software SmartPLS.

On the other hand, inferential statistics aim to make conclusions on the population based on the sample. This requires the formation of conclusions that extend beyond the sample data (Trochim, n.d.). Partial least squares structural equation modelling (PLS SEM) was used to evaluate the inferential statistics. This allowed for the operationalising of the hypotheses. PLS SEM has some challenges when analysing an extensive moderation model. This led to the use of SPSS and the macro PROCESS to confirm any hypotheses linked to the moderation model (Hayes, 2015).

1.6 COMPOSITION OF THIS STUDY

This section, the introduction, focused on providing an overview of the willingness to provide personal information and SSI technology. It also offers a snapshot of the methodology and theoretical underpinnings of the thesis work. This aims to give the reader familiarity with the research topic.

The next chapter, Chapter 2, is an extensive evaluation of the current literature. This chapter outlines the existing academic literature on each variable and constructs included in the

aforementioned theoretical model. This is done so that the reader understands what research has been conducted before, and the gaps that exist in current literature.

Chapter 3 extensively describes the methodological approach used in this study. This chapter focuses on design, data gathering, statistical considerations as well as measurement and scaling. This gives the reader an in-depth understanding of how the hypotheses were evaluated.

Chapter 4 outlines the outcomes of the methodological approach which was applied to the data that was collected. This evaluates the SmartPLS and SPSS results, which were statistical programs used to evaluate the hypotheses in this thesis. Finally, Chapter 5 summarises the findings, outlines the limitations of this study and offers insight into the implications of this research.

1.7 CONCLUSION

This introduction has aimed to give the reader a snapshot of this study. A brief, but concise substructure was described, which unpacks current research which focuses on SSI technology and the sharing of personal information. This included a description of the theoretical framework as well as the relevant hypotheses. The methodology section gave the reader an understanding of how the hypotheses were evaluated and how data was collected, for the purposes of evaluation.

The importance and relevance of this research was also described. This study will contribute to the understanding of SSI technology. Furthermore, the willingness to share personal information was illuminated upon, as well its importance for marketers and consumers. Lastly, a roadmap of the other sections of the thesis was described. This was done to give the reader, an understanding of how the chapters relate to each other, and a preview of what is to come.

CHAPTER TWO. LITERATURE REVIEW

2.1 INTRODUCTION

This chapter focuses on research which relates to one of the focus areas of this study - namely, the willingness to provide personal information over the internet and SSI technology. The literature review will provide the reader with a comprehensive summary of the research that has already been conducted in these focus areas. By doing so, the reader will also gain an understanding of the gaps that exist in current literature. Furthermore this chapter will contribute to an understanding of the theoretical foundations of the research.

The structure of the literature review is as follows. First, personal information is discussed. Next, a discussion on literature relating to organisational trust and its link to sharing of personal information is described. The term organisational trust is also defined in this section. Research relating to each antecedent to trust included in the theoretical model is also illuminated upon. What follows is an analogous approach to the constructs *perceived risk* and *perceived value*. Research relating to these constructs and their antecedents are defined and expanded upon.

Next, the literature view focuses on current research relating to SSI technology. The term SSI technology is defined in this section, as well as the way in which SSI technology was operationalised. The moderator of SSI technology, *security fatigue* is also described in detail, as well as its antecedents: *security*, *functionality* and *usability.*

Lastly, this chapter ends with a conclusion. The conclusion outlines the main findings of the literature review, what gaps exist in the literature and paves the way for the methodology that follows. Figure 6 indicates the literature review, and its linkage with the theoretical model.

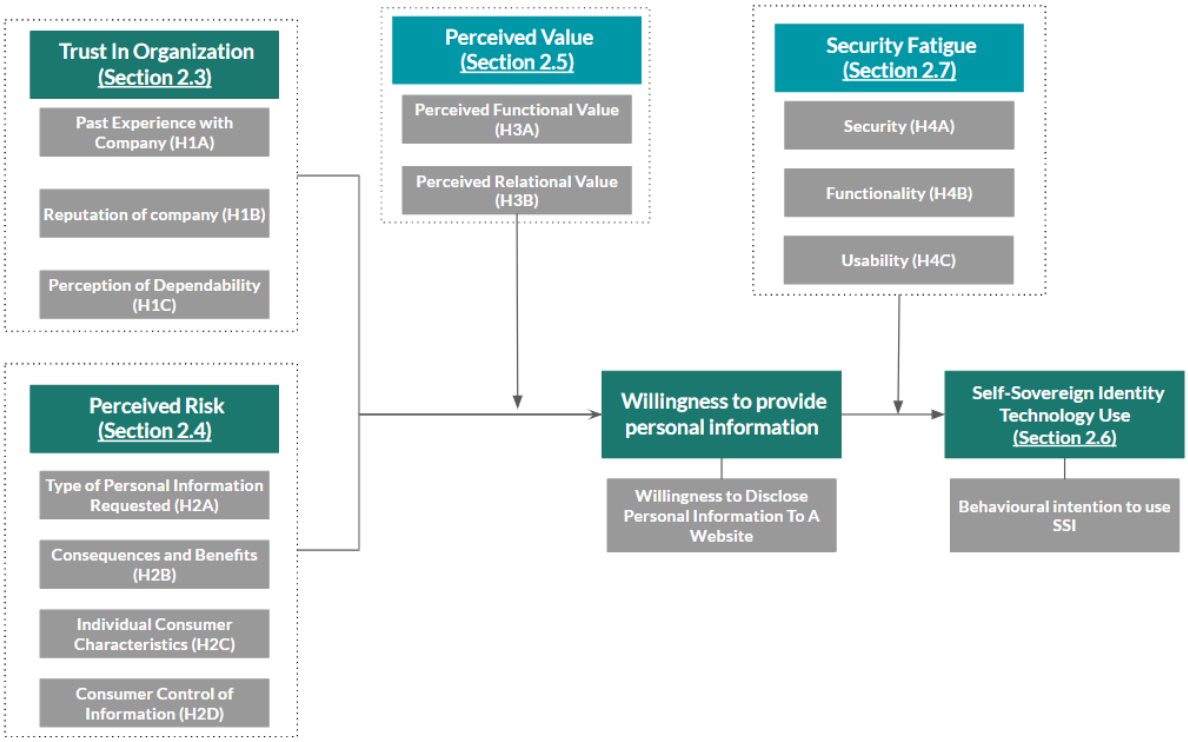

Figure 6. Theoretical Model with the relevant sections of the literature review

2.2 DEFINING PERSONAL INFORMATION

This section focuses on defining the 'willingness to disclose personal information'. To understand what is meant by willingness to disclose personal information, it useful to first comprehend what is meant by personal information. In-order to define the term personal information, we unpack the definitions of the term proposed in prior academic literature. In this study, the term personal information is used interchangeably with personal data as well as personal identifiable information.

Personal information must be distinguished from market-level information. According to Nowak and Phelps (1995) this type of information refers to generalised, and not individual-specific data on a consumer group, market segment or any other type of grouping. The same authors found that personal information as opposed to data that exists at a market-level is of a greater concern to consumers.

Personal information is rarely fully-defined in literature. Instead, literature focuses on defining personal information in terms of what type of data it is. Examples include: name, surname, age and other demographic characteristics (Nowak and Phelps, 1995). In a study by Acquisti, John and Loewenstein (2013) personal information was referenced in relation to linking a consumer's name to purchasing data, but was not fully defined.

Culnan and Bies (2003:326) defined personal information as: *"information identifiable to an individual".* Al-Fedagi and Al-Azmi (2012) defined personal information with reference to two types of information: Atomic personal identifiable information (a single human referent, i.e. John) and Compound personal identifiable information (more than one human referent, i.e. John and Mary). Lastly, Krishnamurthy and Wills (2009) defined personal identifiable information as data which allows an individual to be identified or can be combined with other information to identify an individual.

In this study the definition of Kirshnamurthy and Wills (2009) to understand personal information is utilised. By extension, the willingness to disclose personal information can be defined as a measure which seeks to understand how reluctant or willing a consumer is to disclose this personal information over the internet

Now that personal information and the willingness to share personal information has been discussed, research describing the key construct 'trust in an organisation' is expanded and this followed by a discussion on the antecedents of trust in an organisation.

2.3 ORGANISATIONAL TRUST AND PRIVACY

2.3.1 Introduction

Organisational trust has been considered in a wide variety of contexts. It has been studied in areas as diverse as communication (Griffin, 1967), negotiation (Bazerman, 1964), game theory (Milgrom and Roberts, 1992) and labour management relationships (Taylor, 1989). Trust has also been studied in a marketing context, where the focus has been on delivery channels as well as buyer-seller relationships (Yang and Emurian, 2005).

Seppänen, Blomqvist and Sundqvist (2007) mention that in marketing and sales management research, understanding trust is focused on 'exchange relationship' as it is a core part of marketing. Examples of exchange relationships are commercial negotiations, buyer-seller relationships and relationship marketing (Seppänen, Blomqvist and Sundqvist, 2007). This study focuses on trust in relation to a buyer-seller relationship which has been recognised as an important variable by marketers (Young and Wilkinson, 1989).

Trust has been studied extensively in online environments. Shankar, Urban and Sultan (2002) provide a summary of the trust construct in a digital environment. According to Shankar, Urban and Sultan (2002), when the first websites were created, trust was viewed simply as a aspect of website security linked to the protection of sensitive personal information. Later, it was

linked to privacy issues and whether consumers were willing to disclose personal information. Finally, it was viewed as a multi-dimensional construct that has antecedents and consequences. In the next part of this section there is a focus on trust, and the definition of trust utilised in this study. After which, existing literature relating to the intersection of trust and the willingness to share personal information is expanded upon. Lastly, existing literature relating to the antecedents of trust included in the theoretical model are discussed.

2.3.2 Defining and Understanding Trust

Definitions of trust vary greatly across disciplines (Pirson and Malhorta, 2011). However, many definitions have an inclusion of 'risk' or 'vulnerability' (Rousseau *et al.*, 1998). A commonly used conception of trust is based on the work of Rousseau *et al.* (1998) who refer to it as an acceptance of vulnerability because one party believes that positivity will results from the intentions or behaviour of the other party.

Ganesan and Hess (1997) provide an explanation of the different forms of trust that can exist in buyer-seller relationships (which is a focus of trust in the marketing discipline). Firstly, the authors define *interpersonal trust as a* type of trust that exists between an individual buyer and sales person. Secondly, *intra-organisational trust* is defined as the "*trust that exists between an employee and an employer…*" (Gánesan and Hess, 1997:440). Next, the authors define *inter-organisational trust* as a summation of trust that exists between employees at different Organisations at multiple hierarchical levels. Lastly, the authors define *organisational trust* as the trust that buyers and sellers have in the Organisation they are interacting with when they buy or sell something to the Organisation.

This study adopts a definition of trust that exists within marketing literature. This definition was expressed by Moorman, Desphpande and Zaltman (1993) who defined it in terms of the dependence one partner places on another, when an exchange is taking place. Overall, researchers across disciplines have found it challenging to define trust. This is due to the abstract, multi-faceted nature of trust, and its interrelation with credibility, reliability and confidence (Wang and Emurian, 2005).

Online trust is different from its offline counterpart. Online trust relates to website, internet or technology (Bart *et al.*, 2005). Online trust can be defined as the trust which exists when a business conducts it activities via the internet or an electronic medium like a website (Shankar, Urban and Sultan, 2002). Relating this to a buyer-seller relationship, a website can be viewed

as a salesperson who needs to build trust with the users of the website or customers (Jarvenpaa, Tractinsky and Saarinen, 1999).

This is different from offline trust which focuses on the offline commercial activities of a business (Shankar, Urban and Sultan, 2002). For offline trust the object of trust is not a website but typically a human or organisation (Shankar, Urban and Sultan, 2002). However, offline and online trust are interrelated and some commonality does exist. This may include dimensions such as product quality and reputation.

2.3.3 Trust and the Willingness to Provide Personal Information

Culnan and Armstrong (1999) studied the intersection of privacy concern, procedural fairness and trust in institutions. Procedural fairness is a view by a participant that an activity is being conducted fairly (Lind and Tyler, 1988 as cited by Culnan and Armstrong, 1999). The authors found that procedural fairness (operationalised as fair information practices) operated as a standard which is essential for trust creation when control measures, relating to social ties and contact were not possible (Culnan and Armstrong, 1999).

Hoffman, Novak and Peralta (1999) found that a lack of trust in web providers exists because consumers feel that they do not have control over the use of their personal data. Specifically, consumers feel that web providers will use their data for purposes beyond supporting a transaction, and may sell their data to third parties (Hoffman, Novak and Peralta, 1999).

Milne and Boza (1999) found that trust was negatively related to concern and that trust had a negative relationship with concern. Milne and Boza (1999) also found that the constructs, trust and concern, had a relationship with self-reported purchasing behaviour. This suggests that the construct can influence actual and not only intended behaviour.

White (2004) investigated the incentives consumers had for disclosing personal information to marketers. The authors defined ‘deep relationships’ as relationships characterised by longevity, where trust is at a high level and fulfilment with the relationship is significant (White, 2004). White (2004) found that participants who had deep relationship perceptions were less reluctant to disclose personal information. Conversely, they were more reluctant to reveal embarrassing data. Embarrassing information was defined as information that related to the acquisition history of magazines involving nudity and related to sex (e.g. Playboy or Playgirl magazine) and purchase of condoms.

Bart *et al*. (2005) focused on analysing the influencers of online trust on several types of website categories and consumer groups. The authors found that security was not a driver of trust for any website category. One possible explanation is that the security level of the websites the authors analysed were already above a minimum security threshold. Privacy was found to be influential on the website categories: travel, e-tail (online retailers) and community websites.

Bart *et al*. (2005) found that a large segment of consumers determine trust according to the brand strength and advice. However, brand strength has a greater effect on trust when a respondent has with a higher education compared to a lower education. Advice in this context was defined as a part of a website that helps a consumer acquire a answer to a problem or issue that they are experiencing, on the website (Bart *et al.*, 2005).

Myerscough, Lowe and Alpert (2008) used experimental procedure by creating eight different webpages as stimuli to measure the effect of brand power and the power of the privacy declaration on firstly the willingness to provide personal information and secondly privacy risk. A negative connection between privacy risk and the willingness to provide personal information. Privacy statements had little to no effect on reducing privacy risk, whereas brand building and developing a trusted brand had a strong effect on reducing privacy risk and encouraging consumers to reveal personal data.

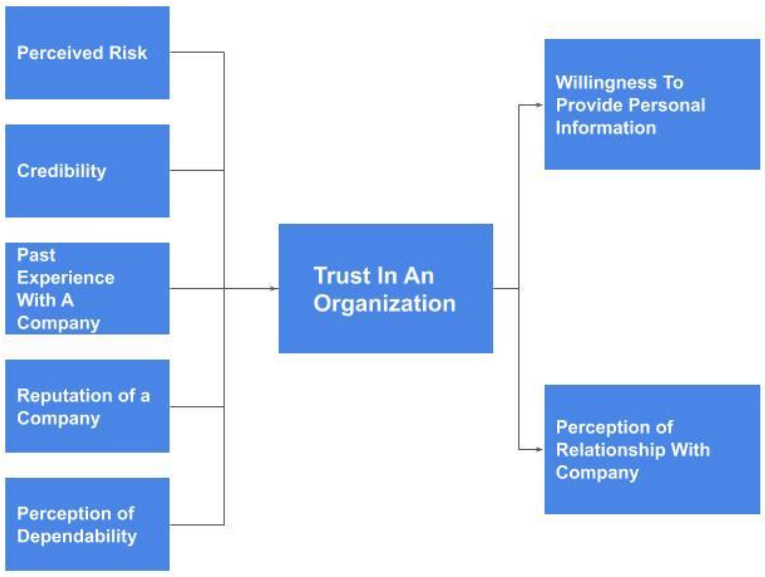

Figure 7. Trust and the Willingness to Provide Personal Information adapted from Schoenbachler and Gordon (2002)

In this study the recent work of Schoenbachler and Gordon (2002) is relied upon to investigate the relationship between trust and the willingness to provide personal information in a database marketing context. Database marketing was defined as a type of marketing where marketers rely on databases (which contain customer information) to develop a relationship with clients (Schoenbachler and Gordon, 2002). This is done by recognising aspects such customer needs, preferences and wants via data (Schoenbachler and Gordon, 2002). The authors proposed the conceptual model depicted in Figure 7. Their model incorporates trust as the central component, which they defined as a state where expectations are clear and agreed on by both parties (Schoenbachler and Gordon, 2002). They hypothesised that p*erceived risk, credibility, past experience*, *reputation* and *dependability* would affect trust. Each antecedent was defined as follows:

1. **Perceived Risk:** The costs or benefit of providing personal data to a party that is not known.
2. **Credibility:** Organisational messages, statements and other communication that are visible to customers.
3. **Past Experience:** Prior interactions and positive or negative experience that can build or detract from trust.
4. **Reputation:** The firm's reputation, in terms of privacy protection and the safeguarding of personal information.
5. **Perception of Dependability:** Whether a firm is likely to deliver on specific promises or claims.

They tested their conceptual model using a survey and a regression analysis and analysed the data on an industry basis as well as across industries. When analysed across industries, it was found that *perceived risk, credibility* and *past experience* with the company did not have a significant relationship with trust. However, when past experience was analysed on an industry basis it was found to have a strong relationship with trust in a number of industries such as communications, apparel, computer, and catalogue industries. Additionally, and holding across industries, *reputation of a company* as well as *perception of dependability* were found to have a relationship with trust.

Some studies have reported the difference between actual and intended behaviour linked to privacy disclosures and trust. Norberg, Horne and Horne (2007) hypothesised that trust would influence actual privacy disclosure behaviour whereas risk would determine intention to

disclose, but not actual behaviour. However, it was found that trust did not have a significant influence on actual behaviour.

The antecedents to trust dimension proposed in the conceptual model, are *past experience with a company*, the *reputation of a company* and *perception of dependability*. These antecedents are discussed in the section which follows.

2.3.3.1 Past Experience with a company and trust

The definition of past experience with a company focused on understanding how prior interactions, and positive or negative experiences build or detract from trust (Schoenbachler and Gordon, 2002). Rempel, Holmes and Zanna (1985) viewed trust as a progression of past experience and prior interactions. These prior interactions were found to either build or detract from building trust in relationships (Rempel, Holmes and Zanna, 1985). However, it should be noted that this literature was based on a social science context.

In a marketing context, Doney and Cannon (1997) analysed the nature of trust in buyer-seller relationships. The authors viewed trust development as consisting of distinct processes: *calculative process, prediction process, capability process* and *intentionality process*. Relevant to the discussion on past experience is the prediction process. This process is described by Doney and Cannon (1997) as trust that is created because of the ability to estimate behaviour. For example, once trust is formed, one party is able to more reliably predict other parties' behaviours. Thus past experience and a variety of experiences with a party can lead to the creation of trust via a prediction process.

Later research by Milne and Boza (1999) analysed trust and concern linked to information management practices. In the qualitative part of their study, the authors presented data linked to a key question asked of respondents: *What makes you trust an organisation with your personal information?* Findings suggested that the main reason provided by respondents was their past experience with the company.

Using an email survey, Ha (2004) investigated the factors which influenced consumer perceptions of brand trust in online environments. They found that customers who experienced enjoyment linked to a website had increased levels of trust. The author developed a hypothesis based on factors such as a 'recency effect' where consumers tend to remember their last experience the best. The hypothesis also linked experience with relationship building. Later work by Ruparelia, White and Hughes (2010) built on the work of Ha (2004) but used a construct for experience that was more related to the past, as opposed to present experience.

Ruparelia, White and Hughes (2010) found that past experience had a positive relationship with trust.

Focusing on trust on the internet, Chen *et al*. (2010) hypothesised that trust has a positive relationship with past experience. The authors viewed past experience as interacting with trust via two dimensions: first, past experience helps with future predictions surrounding interactions with a company; and second past experience influences loyalty positively and each positive interaction increases the likelihood of future interactions. From this study it was found that a causal relationship between trust development and past experience exists.

2.3.3.2 Reputation and trust

Schoenbachler and Gordon (2010) defined a firm's reputation as the degree that a firm sustains privacy and ethical sharing of personal information. This is developed via media and word of mouth. This definition is adopted in the study.

Doney and Cannon (1997) defined reputation in a marketing context. It was defined as a belief that a company is truthful and shows concerns for their clientele. Reputation was found to be important in traditional marketing exchanges as well as in an electronic commerce context. When literature was reviewed for reputation and trust, an electronic commerce context was focused upon. However, it is important to note that companies may be able to transfer 'brand equity', or their positive reputation, from an offline to online environment (Urban, Sultan and Qualls, 2000).

Fung and Lee (1999) investigated the antecedent factors linked to trust in electronic commerce. They defined electronic commerce as commercial activities that are done over the internet. Fung and Lee (1999) proposed that reputation is key to the formation of trust, and that reputation on the internet is dependent on at least two constructs: *existing brand name* and *seals of approval*. Seals of approval are linked to an information security dimension where if a website has seals of approval, consumers can be assured of high security on the website.

Sultan and Mooraj (2001) researched trust by focusing on senior managers and executives. Their interviewees belonged to companies that were described as having a high-level of involvement in the internet. Findings suggested that brand recognition and reputation led to business success through the development of trust (Sultan and Mooraj, 2001).

In an e-commerce context, Xie, Teo and Wan (2006) note that reputation can be viewed as a way to lower uncertainty and create trust with those who engage with a company. Xie, Teo and

Wan (2006) found that there was a positive relationship between reputation and a consumer decision to reveal accurate and up to date personal information. This highlights the importance of reputation in personal information provision as well as the creation of trust.

Eastlick, Lotz and Warrington (2006) studied trust and privacy in online environments using a survey analysis. The authors found that reputation has a positive relationship with trust. Moreover, reputation was found to have a negative effect on privacy concern. Their findings confirmed those from the earlier work by Milne and Boza (1999) where privacy concerns has a negative relationship with trust.

2.3.3.3 Trust and Perception of Dependability

This study adopts the definition of perception of dependability, proposed by Schoenbachler and Gordon (2010), where dependability defines whether a firm is likely to deliver on particular promises or claims.

In an early study, Swan *et al*. (1988) measured the dimensions of trust in an offline environment via a mail survey. Dependability was defined as the alignment between outcomes of buyers and the promises made by a salesperson. (Swan *et al*., 1998). Among all the factors they tested, dependability was found to be the most important single predictor of trust.

Hon and Grunig (1999) proposed that trust had three dimensions: competence, integrity and dependability. Hon and Grunig (1999) referred to dependability as a belief that an organisation actions will be aligned with what an organisation stated they would do. However, this research was not tested empirically and was in a public relations setting.

Macintosh (2002) studied trust and dependability in a travel agency setting in order to understand the aspects that facilitated trust and satisfaction with travel counsellors. In the study, dependability was defined as how easily the intentions of one party could be predicted by another party (Macintosh, 2002:62). Supported by data analysis, they hypothesised that a positive relationship existed between perceived dependability and trust. .

In an online setting, Yoon (2013) analysed end user trust in data repositories via semi-structured interviews. Data repositories were defined as a place where research data is kept so that it can be utilised again (Yoon, 2013:19). Based on these interviews, the author found that trust was related to dependability. This is because dependability was defined by participants as a key component of trust. More specifically, trust was defined by several of the participants as

including a component of delivering on expectations or being able to count on the organisation in question.

Jiang, Jones and Javie (2008) studied the effect of third-party certification programs on consumer trust, and they viewed dependability as part of a broader trust dimension. The author's defined dependability in terms of whether consumers believe a company will deliver on specific claims or promises. If consumers perceive that the delivery of specific claims or promises are likely to occur by a company, they view the company as more dependable and trustworthy (Jiang, Jones and Javie, 2008).

In an early study by Moorman, Desphande and Zaltman (1993) the factors that affected trust in market research relationships was researched using a questionnaire. In this work, dependability was defined in terms of predictability of actions. It was found that this perceived dependability was unrelated to trust. Dependability may be unrelated to trust in some contexts.

This section and its subs-section have extensively outlined existing literature focusing on organisational trust and its relationship with the sharing of personal information. The key antecedents of trust used in this study were also reviewed in the literature. Following a similar approach, perceived risk is now discussed.

2.4 PERCIEVED RISK

2.4.1 Introduction

In this section, literature related to perceived risk and its interrelation to the willingness to provide personal information is expanded upon. This section begins with a definition of perceived risk. This is followed by a summary of literature which has focused on perceived risk, and its interrelation with the willingness to provide personal information. Lastly, this section expands on the following constructs which are proposed as antecedents to perceived risk: *type of personal information requested; consequences and benefits; individual consumer characteristics* and *consumer control of information.*

2.4.2 Defining Perceived Risk

In this study, perceived risk is viewed interchangeably with 'privacy concern'. This is because privacy concern has been strongly associated with an element of risk. For example, Tan *et al*. (2012) define privacy concern as a consumer's knowledge and valuation of risk relating to privacy intrusions. It has also been simply defined as a concern over a loss of privacy (Bansal and Gefen, 2010). However, the emphasis of these definitions on a concern over a 'loss' would

mean that risk is still important to an understanding of privacy concern. This is because measurement of a prospective loss requires a calculation of risk to be done. Specifically, we adopt the definition of perceived risk, proposed by Lo (2010), where an expectation of loss occurs when disclosing personal information.

2.4.3 Privacy Concern and Perceived Risk

The concept of information privacy has also been operationalised in information systems research by the variable 'information privacy concerns' (Xu *et al*., 2011). Privacy concern has been found to be multidimensional. Bellman *et al*. (2004) found that the prevailing regulatory framework, lack of experience with the internet, and cultural differences influence privacy concern.

Nam, Song and Park (2006) studied the link between privacy concern and the willingness to provide personal information. They hypothesised that a negative relationship existed between privacy concerns on a website and an intention to disclose personal information. They furthermore tested three antecedents of privacy concern: *convenience, reputation* and *third party certifications* and found a negative relationship with privacy concern.

Sheehan and Hoy (2000) investigated the different dimensions of privacy concern in US consumers. Three factors were found to have an effect on privacy concern. Firstly, control over storage and utilisation of data where it was found that when consumers were given more control they felt less of a privacy concern. Secondly, the benefit received from giving up their information was found to have an impact on privacy concern and specifically it was discovered that there was a negative relationship between privacy concerns and value given to consumers. Lastly, established long-term relationships with online entities and consumers were found to lessen privacy concerns.

Siyavooshi, Sanayei and Fathi (2013) studied the effect of perceived risk on the willingness to provide personal information. The authors hypothesised a negative relationship between providing personal information and perceived risk. However, this hypothesis was not tested empirically.

Phelps, Nowak and Ferrel (2000) created a theoretical framework to measure privacy concern as well as other variables. The antecedents to privacy concern proposed by these authors have been adopted in this study to measure perceived risk. Their conceptual framework consisted of four input factors which are indicated in figure 8.

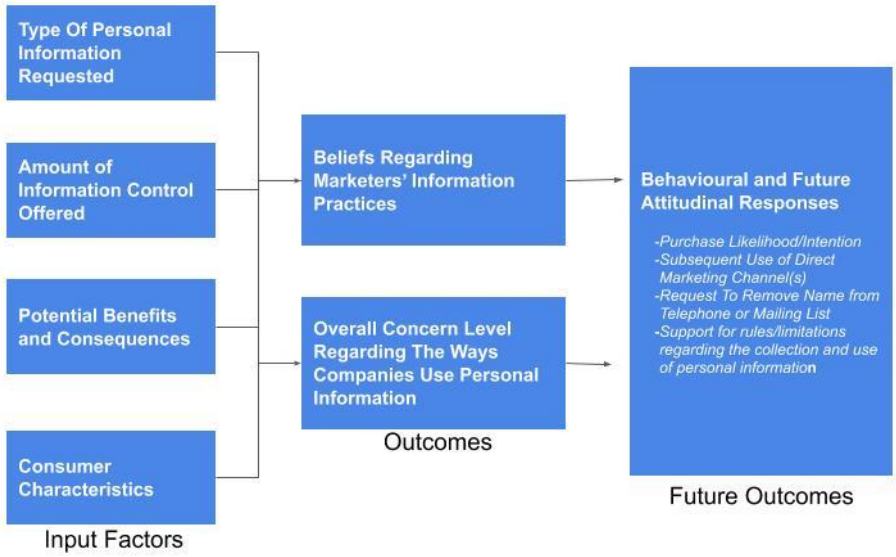

Figure 8. Conceptual model adapted from Phelps, Nowak and Ferrel (2000)

Figure 8 shows how the four input factors were hypothesised to influence consumer beliefs regarding marketers as well as privacy concerns. Input factors were also predicted to have an impact on the behavioural and attitudinal responses of consumers. In the next sub-sections, literature is reviewed for the input factors each which form an important basis of the combined, and aforementioned theoretical model adopted in this study.

2.4.3.1 Type of Personal Information Requested

Phelps, Nowak and Ferrel (2000) hypothesised that consumers would be the most reluctant to share demographic, life and finance, and personal identifier information, and the most willing to share demographic and lifestyle information. This hypothesis was supported by the survey data in their study. Furthermore, it was found that consumers were the most reluctant to provide financial and personal identifier information.

In support of Phelps, Nowak and Ferrel (2000), Leon *et al*. (2013) investigated how willing consumers are to let business collect 30 different data types. Consumers were the most reluctant to share provide personal identifiable information, while several respondents showed a willingness to share their country of origin and gender. Figure 9 depicts the results of the survey conducted by Leon *et al*. (2013).

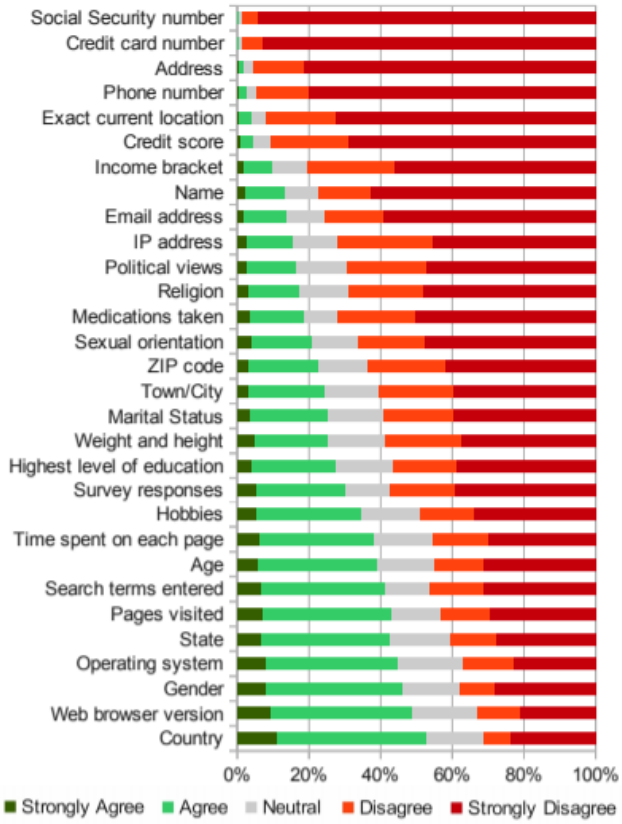

Figure 9. Participants' responses to the statement, "I would be willing to allow advertising company to use and store" adapted from Leon et al. (2013)

According to research conducted by Leon *et al*. (2013), the willingness to share other types of information varied according to the period that the information would be retained and the scope of its use. Overall Leon *et al*. (2013) found that changes to scope of use and the period data is stored had a statistically significant impact on the willingness of consumers to share information.

Metzger (2004) measured the willingness of consumers to share information to a fictitious website. Participants were found to be least reluctant to disclose demographic information, and more reluctant to provide data relating to purchase behaviour, religion, political party affiliation, race, hobbies/interests and occupation. Furthermore, consumers were protective of

contact information such as email and telephone numbers, and financial information, and reluctant to share this information.

Gupta, Iyer and Weisskirch (2009) analysed willingness to share personal information online. The authors measured geographical discrepancies of consumers in India as well as the, US to share different categories of data. It was found that consumers in both countries were less willing to disclose date of birth, home and work addresses as well as phone numbers, credit card details, medical history and financial history. This supports the findings of Phelps, Nowak and Ferrel (2000) where consumers were more reluctant to disclose financial information, and less reluctant to disclose lifestyle and demographic information. Consumers in the US and India had a different degree of willingness to disclose certain types of information. This suggests that geographic differences exist when analysing the willingness to disclose information. This may be because of internet experience, differing cultural perspectives, or lack of awareness of the consequences of personal information disclosure (Gupta, Iyer and Weisskirch, 2009).

2.4.3.2 Amount of control offered

Control is often included as a key component of most privacy definitions. Culnan and Bies (2003) cited Westin (1967) and defined privacy as the degree to which a consumer can control how their personal information is obtained and utilised. Altman (1975) as cited by Martin and Murphy (2017) included control as a central component of privacy - the selective control of access to the self. Foxman and Kilcoyne (1993) defined privacy in terms of which party controls a consumers personal data and if consumers are conscious and knowledgeable of their rights relating to privacy.

Milne and Boza (1999) studied trust and concern in relation to personal information. Perceived control was also measured and operationalised in terms of whether respondents recognise opt-out procedures. The authors found that perceived control was negatively related to concern. This means that the more perceived control a consumer had, the less concerned a consumer was with their privacy. Data analysed by the authors, suggested that consumers have a desire to control their personal information.

Supporting earlier work by Milne and Boza (1999), Phelps, Nowak and Ferrel (2000) found that consumers generally desire more control over their personal information. This is true regardless of their concern over the acquisition of this information by marketers. Moreover, it was found by Phelps, Nowak and Ferrel (2000) that more control leads to greater purchase

intentions, and if intention translates into behaviour, more control could even lead to increased profits.

Phelps, Souza and Nowak (2001) examined the antecedents of privacy concerns and focused on understanding the amount of control a consumer desired over information as well as the consumer's attitude towards direct marketing. The more a consumer desires control over personal information, the more a consumer will express privacy concerns. In other words, privacy concerns can be reduced with increased control over personal information (Phelps, Souza and Nowak, 2001).

The link between privacy concern and control over personal information was also analysed in a social media setting. Hoadley *et al*. (2011) analysed privacy concerns on Facebook after the launch of a news feed feature. The authors found that changes to the perceived control over personal information may be leading to increased privacy concerns. Before the launch of the news feed feature, users had to take active steps to find information on their friends. After the introduction of the feature, Facebook posted any changes to personal information, making it easier to access information which was obtainable before. This led to a decrease in the perceived control a user felt that they had, leading to privacy concerns. In concluding remarks, Hoadley *et al*. (2011) noted that a challenge for regulators is that perceived and actual control may differ. This could lead to situations where more privacy control actually led to less perceived privacy.

This regulatory challenge was confirmed by the work of Brandimarte, Acquisiti and Loewenstein (2013). The authors measured perceived control and the willingness of consumers to share personal information and found evidence for a 'control paradox'. If the willingness to share personal information increases enough due to perceived control, a consumer will disclose information that leaves them at a greater risk. This can mean that procedures designed to increase perceived control may actually have a negative effect on the risk faced by consumers. Consumers place too much importance on the control over the *release* of their information and the risk this represents. Equal or greater risk relates to *access and usage* of this personal information by other parties, once the information has been *released.* This can lead to increased perceived control over the release of information leading to a greater risk for consumers, as they undervalue the risk posed by *access and usage*.

2.4.3.3 Consumer Characteristics

Phelps, Nowak and Ferrel (2000) analysed several demographic characteristics of sex, marital status, age, education, employment status and income. The only characteristic that was found to influence privacy concern was education. Specifically, it was found that the highest privacy concern was experienced by consumers with vocational school or college education.

Zukowski and Brown (2007) focused on demographic factors and their relationship with privacy concerns, based on a survey of 199 internet users. Age, education and income level were found to be significant factors that influenced privacy concern. On the other hand, gender and internet experience were found to have no influence on privacy concern.

Jordaan (2007) investigated privacy concern in South African and found that age, language, income and gender influenced privacy concerns. Lee, Wong and Chang (2016) investigated the effect of gender, age, educational attainment and income level on privacy concern. The authors found that men with high educational attainment and income levels had greater privacy concerns than women. This positive relationship between income levels and privacy concerns were confirmed by the work of O'Neil (2001) who studied privacy concerns in the US. The relationship between educational attainment and privacy concern, was also confirmed by Sheehan (2002), where a positive relationship was found. According to Lee, Wong and Chang (2016), teenagers do exhibit high levels of privacy concern and participants in their twenties to thirties had the significantly higher levels of privacy concern. This is somewhat contrary to the findings of Hoofnagle *et al*. (2000) who found that young adults (18-24 years) do care about privacy and there were no statistically significant results to indicate that different ages create significantly different privacy concerns. Blank, Bolsover and Dubois (2014) found in a UK internet survey that there was a negative relationship between age and privacy concern. This means young people were found to be more concerned than older people. Overall, the varied results indicate that age and its link to privacy concern remains unsettled in literature.

2.4.4.4 Consequences and Benefits

Phelps, Nowak and Ferrel (2000), Ward, Bridges and Chitty (2005) investigated the effect of offering benefits on personal information. In respect of cost savings and tailored services, it was found that these benefits do not directly influence consumer concerns. When both savings and tailored service benefits were offered, a marginal decrease in privacy concern was found. However, the authors believed it reflected a cynicism among consumers that 'nothing is really for free' and that benefits would be linked to unwanted spam and undesired relationships with

online companies. Similarly, Li, Sarathy and Xu (2010) observed that financial rewards can weaken information disclosure in situations that involve the information disclosure that is not pertinent to the transaction.

Other authors have found evidence that financial benefits positively affect the willingness to provide personal information. Xie, Teo and Wan (2006) found that a financial reward in the form of a voucher is influential on a consumer's intention to disclose accurate personal identifiable information. However, these financial rewards are not influential on the disclosure of demographic information. It was hypothesised by the authors that there was less resistance to provide demographic information without reward because it does not equip a company to trace a consumer. This means that consumers may perceive that lower risk of privacy invasion is present (Xie, Teo and Wan, 2006).

The cost-benefit analysis by consumers in an information exchange is sometimes described as 'privacy calculus'. Li, Sarathy and Xu (2010) described a type of cost-benefit trade-off. This trade-off describes the factors which detract from or support a decision to disclose personal information to a company. They investigated whether fairness elements modified the privacy calculus undertaken by consumers, and found evidence that perceived fairness did influence the assessment of privacy costs (Li, Sarathy and Xu, 2010).

Wang, Duong and Chen (2016) investigated the intention to disclose personal information on mobile applications. The authors found that perceived benefits had a greater influence on the intention to disclose information compared to the perceived risks. More specifically, self-presentation and tailored services led to greater disclosure intentions, because they had a positive relationship with perceived benefits. Self-presentation was described as the regulation of a consumer's private image in the eyes of others. In contrast, perceived severity (i.e. negative consequences perceived due to a security threat) and perceived control were found to be antecedents to perceived risk and they negatively affect a consumer's intention to disclose personal information.

Mothersbaugh *et al*. (2012) measured how the provision of benefits affects a consumer's willingness to provide personal information. The authors applied prospect theory in their study. Prospect theory focuses on how consumers quantify gains and losses when making choices that have risk associated with them (Kahneman & Tversky, 1979). The theory proposes a value function which translates actual gains and losses into perceived gains and losses experienced by consumers (Mothersbaugh *et al*., 2012).

Mothersbaugh *et al*. (2012) explained that an important dimension of prospect theory is that gains are perceived as having less of an impact than losses. This has implications for benefits given to consumers in an information disclosure setting. Prospect theory would suggest that benefits will have a decreasing effect on a consumer's willingness to disclose information as losses are perceived to increase. Mothersbaugh *et al*. (2012) proposed that the more sensitive information is, the greater the perceived loss connected with potential information disclosures. Sensitivity of information is defined simply as the possibility for an individual to experience loss because they chose to share their personal information (Mothersbaugh *et al*., 2012). Overall, this led to the authors predicting and finding that benefits have less of an impact on the willingness to provide information, when this information was more sensitive (and vice versa). Note that these authors measured benefits in terms of website customisation benefits derived from information disclosure and not monetary rewards or shopping benefits.

The previous two sections have provided an overview of literature relating to the two main antecedents of the willingness to share personal information which are proposed in this study: trust and perceived risk. In the next section, perceived value as a moderator is introduced, as well as existing literature linked to perceived value.

2.5 PERCEIVED VALUE

2.5.1 Introduction

In this section we describe the construct of perceived value and its antecedents: *perceived functional value* and *perceived relational value*. Functional value and perceived relational value are hypothesised to moderate the relationship between trust, perceived risk and the willingness to share personal information.

This study relies on the work of Tai (2011) who investigated perceived value in information sharing services among consumers, and its consequences for relationship intentions. Tai (2011) defined a 'customer relationship intention' as a desire to create a long-term connection with a company. A higher relationship commitment was theorised by the author to create higher positive behavioural intentions towards a company, as consumers find it important to invest effort in maintaining a relationship with a firm (Tai, 2011). This relationship commitment can be augmented by increasing the perceived value consumers experience from the relationship with the firm (Tai, 2011). This study does not focus on the creation of a relationship commitment, but rather on an understanding of perceived value. However, the relationship

between perceived value and relationship commitment suggests that perceived value may have an influential relationship with trust.

Tai (2011) viewed perceived value as consisting of two components: *perceived functional value* and *perceived relational value.* In their view, perceived functional value is benefit a consumer experiences from the use of a product or service. Perceived relational value, on the other hand, is a belief held by a customer that a relationship with a provider of services will have a future benefit or future value. This study proposes that perceived value acts as a moderator of a consumer's willingness to provide personal information to a firm.

In early literature, perceived value was viewed two dimensionally by focusing on the utility derived from a product or service. Benefits received and sacrifices made either contributed or detracted from to the creation of perceived value (Sanchez *et al*., 2006).

Other authors view perceived value as a construct with several dimensions. This view takes into account advances in consumer behaviour and the role that emotions have in purchasing behaviour (Sanchez *et al*., 2006). Most studies that view perceived value as a multidimensional construct take into account an affective dimension, as well as a functional one (Sanchez *et al*., 2006). This affective dimension is emotive and relates to moods triggered by a product or service which is offered (Sanchez *et al*., 2006). Another dimension of perceived value, less often cited in literature, is experiential value. Experiential value is derived from the experience itself - from direct usage or a thankfulness for goods or service (Mathwick, Malhorta and Rigdon, 2002). This study focuses only on functional and relational value as a moderator and not on affective or experiential value.

2.5.2 Perceived Functional Value

This study adopts Von der Trench *et al*. (2015) definition of functional value in a knowledge sharing context as the perceived benefits from willingly disclosing personal information. Von der Trench *et al*. (2015) defined knowledge sharing as the sharing of helpful information in response to a request for it, and as being derived from a cause. This cause may be external (request by a company) or internal (within an individual). After perceiving this cause, a cost benefit analysis is done. If benefits exceed costs, the information is shared (and vice versa). This creates an apparent relationship between knowledge sharing and a consumer's willingness to share personal information. Von der Trench *et al*. (2015) provided another type of functional value relating to knowledge sharing which relates to the value that can be derived from the use of shared knowledge when a problem is faced by the requester for this information. For

example, Wasko and Faraj (2000) found individuals derived a tangible gain from knowledge sharing to receive help for a specific problem.

2.5.3 Perceived Relational Value

Perceived relational value is defined in this study as a customer's perceived belief that future benefits will result from establishing a connection with a supplier of a good or service (Tai, 2011)

This section focuses on relational capital in virtual communities. According to Sridhar Balasubramanian (2001), virtual communities can be described as containing the following characteristics: accumulation of people; rational utility-maximises; contact that is not physical; a social exchange process consisting of joint creation and consumption; and social interaction that includes a collective objective (e.g. environmental protection). Although these virtual communities exist over the internet, and involve knowledge sharing, it is different from an online exchange of information between a consumers and firm. For example, there is often no creation by consumers, when consumers exchange information with a website selling a product. Despite this, it is proposed that the literature linked to social capital theory and relational capital is still relevant, as information sharing still occurs when personal information is provided.

Chiu, Hsu and Wang (2006) focused on what led to knowledge sharing or information sharing in virtual communities. Virtual communities find it challenging to entice members to share their knowledge with other members of the community (Chiu, Hsu and Wang, 2006). This makes the work of these authors relevant to understanding of how relational value might affect information sharing. Chiu, Hsu and Wang (2006) relied on social capital theory to understand relational value. Actions of individuals in a social network are affected by the existence or lack of social capital according to social capital theory. Social capital refers to resources which facilitate cooperation, mutual benefit and connection for individuals within a network (Chiu, Hsu & Wang, 2006). Social capital has three categories: cognitive, relational and structural (Nahapiet and Ghoshal, 1998). This relational dimension focuses on relationships which influence behaviour, and can be leveraged in a relationship (Nahapiet & Ghoshal, 1998).

Key dimensions relating to the formation of relational capital are *trust, reciprocity* and *identification* (Nahapiet & Ghoshal, 1998; Chiu, Hsu & Wang, 2006). Trust focuses on predictability between two parties that are interacting with one another, and one party will not take advantage of the other. Reciprocity relates to a mutual understanding that benefits

provided by one party, will be returned to the other. Lastly, *"community identification is defined as an own conception of self with respect to the defining features of a social group"* (Chen & Sharma, 2011:271).

Wasko and Faraj (2005) measured the impact of relational capital in electronic networks. These electronic networks can be described as online discussion forums that enable the exchange of ideas and advice. This means that sharing of information occurs, although it may not be personal information. The focus of the work of Wasko and Faraj (2005) was on commitment and reciprocity experienced on a legal electronic network in the US. They measured commitment and reciprocity using a study-based survey. The authors found no relationship between the quality of the response and reciprocity or commitment. In terms of quantity of responses, a negative relationship was found between reciprocity and the quantity of contributions. Furthermore, no link was found between commitment and the quantity of contributions.

Building on the work of Wasko and Faraj (2005), Chiu, Hsu and Wang (2006) hypothesised that trust, reciprocity and identification would have a relationship with the volume and quality of information or knowledge sharing in virtual communities. It was found that reciprocity and identification had a positive relationship with knowledge sharing, while trust was found to not have an effect on the quantity of knowledge sharing. An explanation provided by the authors is that users are willing to share information because of close, regular interaction in the virtual community.

Lu and Yang (2011) studied information exchange in virtual communities, during disaster conditions such as an earthquake. Relational capital had a significant positive effect on information quality but no significant impact on information quantity according to Lu and Yang (2011).

A review of early literature suggests an interrelationship between the dimensions of relational value: *trust, reciprocity* and *identification* with information quality and information quantity. This suggests that relational value may have a significant relationship with the willingness to provide information by affecting both the information quality and quantity provided by consumers during information exchanges.

This section focused on the willingness to share personal information; trust; and perceived risk as key factors that influence the willingness to disclose personal information. Perceived value

as a moderator of these relationships was discussed. In the next section, SSI technology and security fatigue will be discussed.

2.6 SELF-SOVEREIGN IDENTITY

2.6.1 Introduction

This section begins with a description of a digital identity and how SSI technology can be described as the final evolution of a digital identity. Thereafter, the interrelation between SSI and blockchain is described, followed by a description of the key characteristics of SSI.

2.6.2 The Evolution of Digital Identity

The term SSI Technology is not fully defined in the literature. However, the definition of Mühle *et al* (2018) is adopted in this study. Mühle *et al* (2018) is defined as system for identity management that permits a person to own and manage their electronic or digital identity. For further clarification, a digital identity can be simply described as digital data which relates to a person in a specific identity system (Chen, 2007).

SSI can be described as the final evolution of this digital identity Allen (2016). Allen (2016) described the 4 stages of development of a digital identity. This evolution was graphically depicted in the work by Tobin & Reed (2016) in their study "The Inevitable Rise of Self-Sovereign Identity" as follows:

Figure 10. The different stages of development of an identity adapted from Tobin & Reed (2016)

Tobin & Reed (2016) provide an explanation of each of the stages of developmental stages of a digital identity (Figure 10). Firstly, a *centralised identity* describes an identity owned and controlled by a single party. This common identity is present on several e-commerce and social media websites where an individual must log-in to each website with a unique login and

password. In essence, your identity is linked to an entity, who often has authority to erase your identity with impunity.

Secondly, a *federated identity* differs from a centralised identity by giving a user increased movability of their digital identity and in more complex instances, the distribution of details of a user between sites is possible. Single sign on services like Facebook and Google are practical examples of this identity. Single sign on, allows you login to other sites using your Facebook or Google profile.

Taking a bigger step towards a self-sovereign identity, a *user-centric identit*y allows a user to be in control of their own data in terms of both its growth as well as its transfer. However, this type of identity relies on claim suppliers, personal data stores and individual identity suppliers, so has yet to transition into a truly sovereign or independent state.

The final state of a digital identity is the *self-sovereign identity*. This type of identity has levels of control similar to the user-centric identity, and it includes an independent dimension where the digital identity exists independently from any provider or external party and thus 'cannot be taken away'.

2.6.3 Blockchain and SSI

In this sub-section a description of how SSI technologies relationship with blockchain technology is discussed. Blockchain can be described as a Microsoft Excel spreadsheet where hundreds of participants continuously verify each entry in the spreadsheet so that no incorrect or fraudulent inputs are made. The underlying technology which drives blockchain is referred to as Distributed Ledger technology. Bitcoin is an application of blockchain technology, but is only one of the many applications.

Blockchain provides a technological basis for SSI. This is because of a cryptographical method called 'zero-knowledge proofs'. This enables a user to prove a claim (i.e. you have a valid driver's license) without providing any additional details relating to your identity (Kröger, Meyer and Hirschfelder, 2019). This allows for an individual's identity to be truly sovereign in an environment, uncontrolled by any single party (Tobin and Reed, 2016).

An explanation on how blockchain can solve identity problems on the internet is described by Windley (2018). Windley (2018) uses an example of presenting a digital driver's license to a digital bar. The department of motor vehicles (DMV) gives a registered licence holder a digital driver's licence. The DMV digitally 'signs' this licence so someone who views the digital

license can see it was issued by the DMV. The holder also countersigns the licence to prove it belongs to them. This digital license is then stored in the holders digital wallet. At the digital bar, the licence holder presents this licence to the bar to verify they are above 18 years of age. The bar is then able to verify this claim using the blockchain (and trust this claim due to the DMV's signature). This is the basics of how most applications of SSI using blockchain could work.

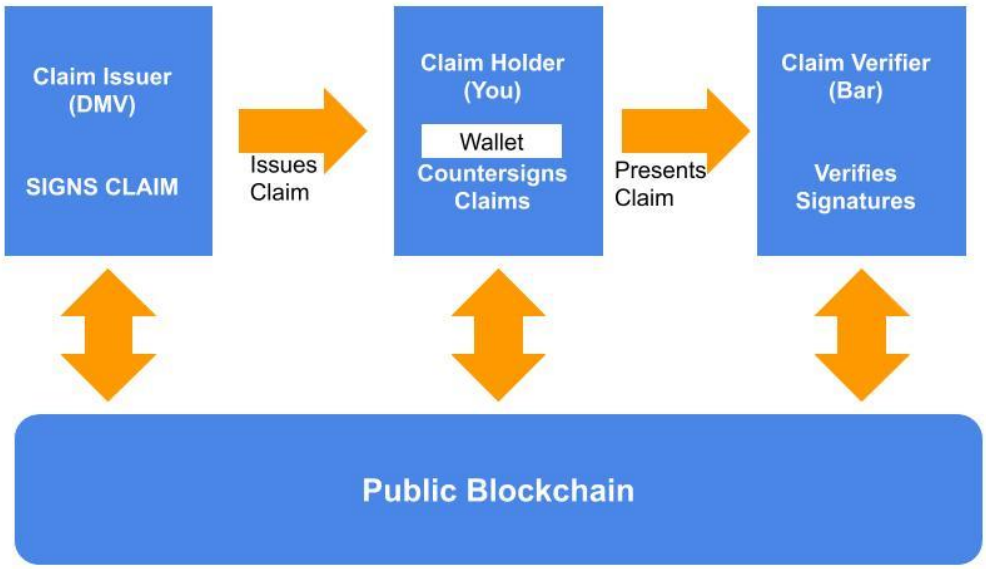

Figure 11. How SSI could work using blockchain adapted from Windley (2018)

2.6.4 SSI and Prior Literature

In this section, current research on SSI technology is discussed. Kröger, Meyer and Hirschfelder (2019) wrote a paper titled *A win-win solution: The potential benefits of blockchain technology for users, marketers and society.* This paper highlights how marketers and society can benefit from the use of SSI technology. At the time of writing, this was only the only literature that was found which focuses on the intersection of marketing and SSI technology.

A conceptual model is proposed in this work (Figure 12) which relates to how blockchain can change the process flow in digital advertising. This conceptual model shows how payment and data flows are disrupted due to SSI. In the current model, service providers amass payments

from advertisers and data from users. In the future model, data is collected directly from users and users also obtain the corresponding payment.

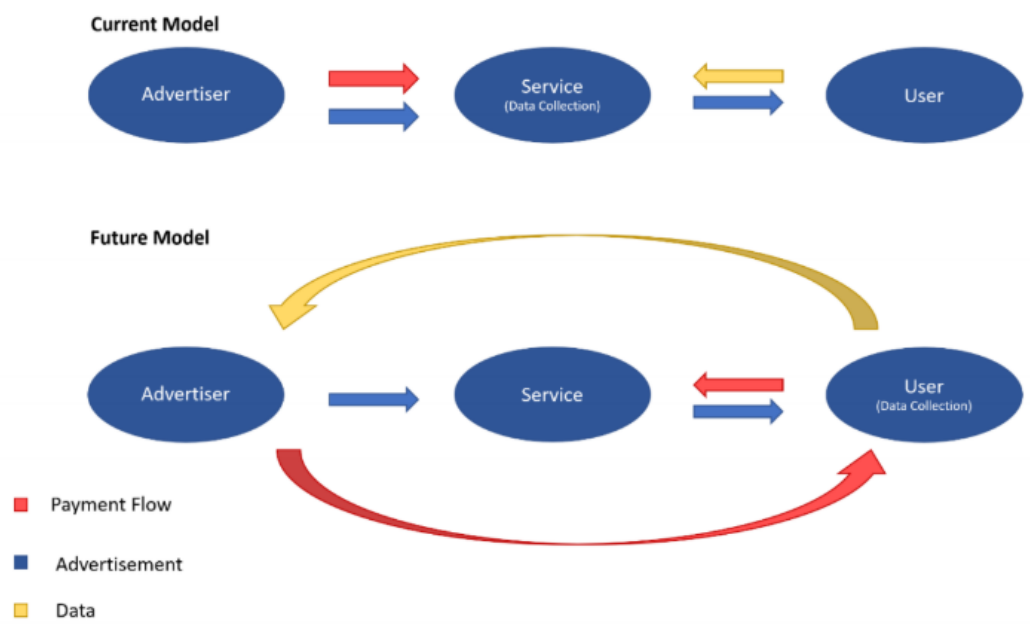

Figure 12: Conceptual model proposed by and adapted from Kröger, Meyer and Hirschfelder (2019)

Other research on SSI technology was conducted by Dunphy and Petitcolas (2018) who evaluated blueprints for identity management systems that use distributed ledger technology. Examples of systems they analysed were those of Sovrin, uPort and OneName. They found that usability was a concern as users were assumed to understand how to conduct effective cryptography management. They also noted concerns relating to the obligations placed on data controllers under the tightening regulatory landscape, and whether providers can meet all these expectations.

Tobin and Reed (2017) provide a good description of the evolution of SSI and essential components of the technology. Tobin and Reed (2017) wrote a white paper for the Sovrin Foundation, a current developer of SSI technology using blockchain. Similarly Blockchain Bundesverband (2018) wrote a comprehensive overview of SSI explaining the concept of SSI, its potential and its current implementation.

Sullivan and Burger (2017) wrote about the Estonian e-residency program and discussed the implications of this technology using blockchain with reference to SSI. Other papers on the topic of SSI are technical from an IT architecture standpoint. The work of Stokkink and

Pouwelse (2018), Diebold (2017), Bakre, Patil and Gupta (2017), Alboaie and Cosovan (2017), Toth and Piddy (2018) describe applications of SSI technology in detail with some descriptions of SSI system architectures.

2.6.5 Key characteristics of SSI

All the essential dimensions of SSI described by Allen (2016) are graphically depicted below by the work of Tobin and Reed (2016), who categorised them into security, controllability and portability.

Table 1. Christopher Allen's Ten Principles of Self-Sovereign Identity summarised by and adapted from Tobin and Reed (2016)

Security *The Identity of Information Must be Kept Secure*	**Controllability** *The user must be in control of who can see and access their data*	**Portability** *The user must be able to use their identity data wherever they want and not be tied to a single provider*
Protection	Existence	Interoperability
Persistence	Persistence	Transparency
Minimisation	Control	Access
	Consent	

Mühle *et al.* (2018) described security as protecting personal information and ensuring data is exposed only as far as it is needed to fulfil a function. Allen (2016) described each element within security as follows:

1. *Protection.* The user's rights and liberties are always greater than the needs of the network.
2. *Persistence.* Identities must exist for the period the user want the identity to last. The user must have a right to be forgotten and be able to change their own identity.
3. *Minimisation.* Data should only be disclosed to the degree needed to fulfil an activity.

The controllability dimension is defined by the logic that users are in control of who views and is able to access their data (Tobin & Reed, 2016). More specifically, control as a sub construct of controllability is explained by Allen (2016) as users being able to fully change their digital identity, remove it, or update it.

1. *Existence* is defined as "....*based on the ineffable "I" that's at the heart of identity and consent…the kernel of self that is upheld and supported*" (Allen, 2016). Existence is also tied to independence and that each user's identity must be independent.

2. *Persistence* has already been discussed and refers to longevity of a user's identity that should not counteract the right to be forgotten.
3. *Control* focuses on a user controlling their identity. The user is the main power over their own identity. This means a user can delete, update, hide or refer to their own identity (Allen, 2016).
4. *Consent* encompasses an element of permission, that a user must agree to all use or sharing of their data (Allen, 2016).

Portability means that identity should not be tied to any single identity provider (i.e. a Google account tied only to Google) and that this identity should be usable and accepted everywhere (Tobin & Reed, 2016).

1. The sub construct *interoperability* means an identity should be widely accepted, and operational where the user needs to use it (Allen, 2016).
2. *Transparency* means that the architecture and system providing the digital identity must be well-known, independent and examinable by anyone (Allen, 2016).
3. *Access* means that a user must be able to review and retrieve their own data; but does not mean they can adjust all their data or that a user has access to the data of other users (Allen, 2016).

This study focuses on the relationship between the use of SSI technology and the willingness to provide personal information. However, as SSI technology is still being refined and developed, a conceptualisation of SSI technology used in this study is based on the key characteristics: *security*, *portability* and *controllability* that were put forward by Allen (2016).

2.7 SECURITY FATIGUE

2.7.1 Introduction

This subsection begins with an explanation of the link between security fatigue and SSI technology. Next, literature which focuses on security fatigue is discussed. Thereafter, security fatigue is defined and literature relating to functionality, usability and security are used to operationalise security fatigue are discussed.

The concept of SSI technology is interlinked with security. Mühle *et al* (2018) described the security component of SSI as the safeguarding of user data and disclosing the least amount of data required to complete a task. Using SSI technology for the security of personal data may

create ‘security fatigue’ by individuals who use the technology. Security fatigue caused by SSI may be similar to the fatigue created by the Platform for privacy preferences project (P3P).

The full implementation of a P3P gives the user an ability to make active choices about every request that was made for their personal information (Weitzer *et al*., 2008). It was found that these choices could quickly become overpowering to a consumer and could lead to fatigue (Weitzer *et al*., 2008). Arguably this fatigue could be experienced with the use of SSI technology. This made it important to incorporate fatigue as a construct in the proposed model.

In a privacy environment, Choi, Park and Jung (2018) conceptualise security fatigue as consisting of two dimensions: *emotional exhaustion* and *cynicism*. The authors define cynicism as frustration and other negative feelings relating to a consumers attitude towards an object (Choi, Park and Jung, 2018:4). Emotional exhaustion as a persistent period where a person’s emotional, mental and physical state can be described as extremely fatigued (Cropanzano, Rupp and Byrne, 2003:160). Research by Choi, Park and Jung (2018) found a strong link between privacy behaviour and security fatigue based on a survey of 324 internet users. They found that security fatigue led to greater disclosure intentions among consumers. A common consequence of fatigue is an inability to make a decision (Ream and Richardson, 1996). This fatigue may find application in a privacy context by a choice to release personal information, without thinking about privacy protection (Choi, Park and Jung, 2018).

Waite (2010) discussed a security triangle in order to understand security fatigue. This triangle is depicted in Figure 13. This security triangle is indicative of a balance that must be created between the conflicting goals of *usability*, *functionality* and *security*. Any security solution needs to find a careful balance between each competing element to be successful. The dimensions of functionality, usability and security are incorporated as key antecedents of security fatigue in this study and are explained in greater depth below.

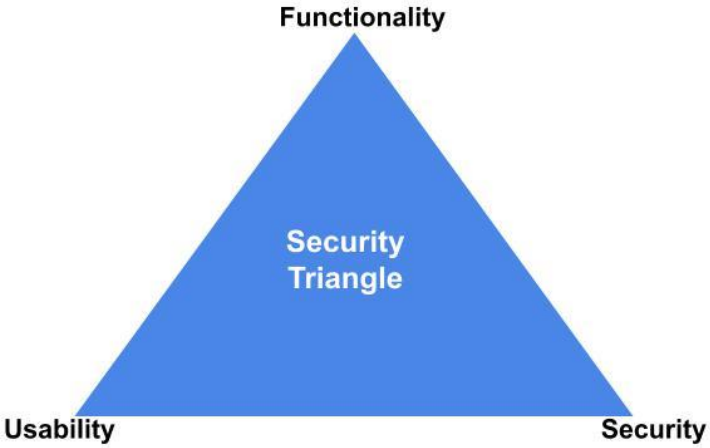

Figure 13. Security, Functionality and Usability Triangle adapted from GreyCampus (n.d.)

2.7.2 Defining security fatigue

In this study security fatigue is described as the stress relating to being highly vigilant and security aware (Bada, Sasse and Nurse, 2019). The concept of security fatigue has been linked to the concept of 'weariness'. Weariness can be described as a *"...a reluctance to see or experience any more of something*" (Stanton *et al*., 2016:26). When this concept of weariness is interlinked with IT security, the concept of security fatigue is created (Stanton *et al*., 2016). Other authors such as Furnell and Thompson (2009) described security fatigue as a state where a user becomes weary or disheartened with safe information security practices. Some authors have also defined security fatigue as simply meaning fatigue linked to security tasks (Coopamootoo, Groß and Pratama, 2017).

Security fatigue is the focus of this study, however other types of IT related fatigue exist. For example, Schermer, Custers and Hof (2014) describe *consent fatigue*, where users become desensitised to privacy rules and simply consent to every privacy policy offered to them by a company. *Breach fatigue* has also been discussed in the literature, and can be described as an exhaustion with the abundance of data breaches leading consumers to ignore data breaches (Kwon and Johnson, 2015). Lastly, Choi, Park and Jung (2018) defined the concept of privacy fatigue as a user experiencing tiredness with privacy in an online setting.

Usability, functionality and security are incorporated as key variables that are used to operationalise security fatigue in this study and these will be discussed in greater depth.

2.7.3 Functionality and usability

This study defines functionality as functions or capabilities of an IT system to get a job done (Goodwin, 1987). This job may be complex or simple, known or unknown to a user. Furnell (2010) described usability in an IT context, as having three dimensions: *user interface, operation and performance.* According to Furnell (2010) a user's perspective on usability requires an IT system to be *understandable* (presentation of security features are meaningful), *locatable* (users can find the features they need), *visible* (users can see the extent that security features are being applied) and *convenient* (security is not too time consuming).

Related to functionality and usability, Thompson, Hamilton and Rust (2005) described feature fatigue. Before using a product, a consumer values the capabilities (or functionality) of a product more than its usability. After using a product, usability has a greater value. This results in consumers selecting complex products that do not maximise their satisfaction and lead to 'feature fatigue' (Thompson, Hamilton & Rust, 2005). Keith *et al*. (2014) applied this concept of feature fatigue to a privacy setting, describing the theoretical extension as 'privacy fatigue'. They found that before using privacy controls, capabilities were a good predictor of expected utility. However, capabilities did not predict actual usage and ease of use was a more important factor that predicted actual usage.

SSI solutions may find a balance between usability and functionality difficult to achieve. Dunphy and Petitcolas (2018) analysed three popular identity management systems that use blockchain (*uPort*, *ShoCard* and *Sovrin*). After analysing these systems, the authors found that usability was a key area of improvement and concluded that, current identity management systems on the blockchain did not adequately focus on creating an effective user experience. The expected the user to understand how to conduct complex, technical tasks.

The distinction and intersection of functionality and usability has been studied by several authors. Goodwin (1987) found that designers of IT systems incorrectly view usability as similar to functionality or as limiting functionality. This means that a lack of usability may not be a problem that is specific to SSI technology. Goodwin (1987) provided evidence in prior literature that usability should be viewed as complementary to functionality. Supporting this, Davis (1989) found that increased usability has been found to ease the difficulty user's experience with managing functionality. Bass and John (2003) noted that functionality can

have a positive effect on usability, if the user is provided with functionality that can save them time during their use of a website. Adding to this, Fisher *et al*. (2008) found that not including enough functionality can deter navigation of a website. Consequently, this may have an impact on usability.

Calisir *et al*. (2010) studied functionality and usability factors for digital bidding and shopping websites. The authors studied the following functionality factors: *security* or features to protect privacy; *search options* or the ability to search for a good or service, usually in a navigation bar on a website; *information provision* or the adequacy of the information provided about a product, service or goods; *service/facilities* that allow a customer to achieve their goals, *user guidance or support;* and *customisability* or the ability to change website navigation to suit a user's preferences. They found that search option criteria were the most important factors among all the functionality criteria.

Calisir *et al*. (2010) studied the following 'usability factors' for a website: *navigation* or finding desired information; *interaction* or responses to the users actions; *learnability* or the level of energy needed to operate the system; *ease of use; response time* or the time needed for the system to respond to the user; *memorability* or how easy it is to recall how to use the main functions of a website when it is revisited*; efficiency* or how effectively a website allows a user to work quickly; and *satisfaction* or the general pleasure when using a website. Navigation and interaction were found to be the most important factors to customers. Overall, it was found that these usability factors were more significant than the aforementioned functionality factors.

Topaloglu *et al*. (2013) investigated the significance of usability and functionality for E-Health websites. These E-health websites were places on the internet where a consumer can acquire health information and advice (Totaloglu *et al*., 2013). Many of the same factors used in the work of Calisir *et al*. (2010) were adopted within the usability and functionality dimensions. However, the author's added *differentiation of information types* (selection of information offered) as well as *thesaurus* (functionality that helps someone understand complex medical terms) to the functionality dimension.

The functionality factors: *service/facilities* and *personalization/categorization* of information were found to be the most important functionality dimensions. Functionality factors: search options and differentiation of information types were also ranked 3rd and 4th respectively. Overall, the work of Topaloglu *et al*. (2013) indicates that for e-health services on the internet functionality may be more important than usability. When compared to the aforementioned

results for online shopping websites, this may suggest users may value usability and functionality for differently depending on the types of website.

The work of Korhan and Ersoy (2016) assessed both the usability and functionality dimensions of social media websites. They used a Likert type scale to measure these factors, based on the aforementioned work of both Toaploglue *et al*. (2013) as well as Calisier *et al*., (2010).

According to Korhan and Ersoy (2016) for social networking sites, ease of use and learnability was the most important usability factors across age groups. Interestingly, it was observed that the younger generation (16-25) value response time, navigation and satisfaction more. On the other hand, older generations consider interaction, memorability, and efficiency as the most important factors. Regarding functionality, personalisation was the most important. In the next section, literature focusing on security is discussed. Security is the last dimension used to operationalise security fatigue and forms the last part of the security triangle.

2.7.4 Security

Security is defined in this study as privacy protection features offered by a website to protect a consumer. Calisir *et al*. (2010) incorporated security as a dimension within a broader functionality dimension. The authors found security to be one of the least important factors to younger consumers, when they conducted their study on online auction and shopping websites. Research by Tandon, Kiran and Sah (2016) focused on online shopping in India and found that privacy and security were the least important determinants of website functionality that influenced perceived usability of a website. However, the authors also find that privacy and security was a significant dimensions of website functionality.

2.8 CONCLUSION

This chapter has outlined the literature pertaining to each construct in the proposed theoretical model, as well as that related to the five major constructs: *organisational trust, perceived risk, perceived value, self-sovereign identity technology* and *security fatigue*. The variables used to operationalise these five major constructs were discussed in detail. This was done to give the reader a comprehensive understanding of the literature which formed the basis of the theoretical model and topic areas. Furthermore, existing gaps in the literature were foregrounded. The next chapter on methodology outlines precisely how the hypotheses that were conceptualised in this study were tested. This includes a description of sampling, measurement and scaling as well statistical considerations.

CHAPTER THREE: METHODOLOGY

3.1 Introduction

This chapter describes the methodology used to meet the primary and secondary objectives of this study. What proceeds this section is an explanation and recap of the main intention of this study. This is followed by a description of the primary and secondary research objectives. Next, the research framework for the study is proposed and the hypotheses are restated. Thereafter, measurement and scales to substantiate the aforementioned hypotheses are discussed, which are linked to a questionnaire. Penultimate, sampling and sizing is specified. Finally, a data analysis plan is described and a summary of the main points of this chapter is included as part of a conclusion.

3.2 Intention

The intention of this study is to present the factors which affect a consumer's willingness to share personal information. The relationship between this willingness to share personal information and a consumer's desire to use SSI technology is also a principal objective of this research. The project utilised an online survey. Blockchain and SSI technology provides a real opportunity to change the current paradigm of data collection, monetisation and ownership. This has far-reaching implications for marketers who rely on this data, as well as consumers who currently lack significant control over their data. This study aims to lay a foundation to understand SSI technology from a marketer’s point of view, and its relationship with a consumer’s willingness to currently share their personal information

3.3 Objectives

Primary Objectives:

1. To determine the factors which affect a South African consumer’s willingness to provide personal information on the internet.

Secondary Objectives:

2. To determine the relationship between the willingness to provide personal information on the internet and the use of Self-Sovereign Identity Technology, in South Africa.

3.4 Research Context: *SSI Use and Information Sharing Framework*

To meet the research objective stated above, this study relies on research conducted by Schoenbachler and Gordon (2010), Phelps, Nowak and Ferrel (2000), Tai (2011) and Waite

(2010). This research provides a basis to conceptualise the relationship between a user's willingness to share personal information on the internet, and their willingness to use SSI technology. A combined theoretical framework is proposed in this study which incorporates the models and findings of the research of the aforementioned authors. This theoretical framework allows the primary and secondary research objectives to be met. It measures the factors which influence the willingness to provide personal information, as well as the relationship between this willingness to provide personal information and SSI

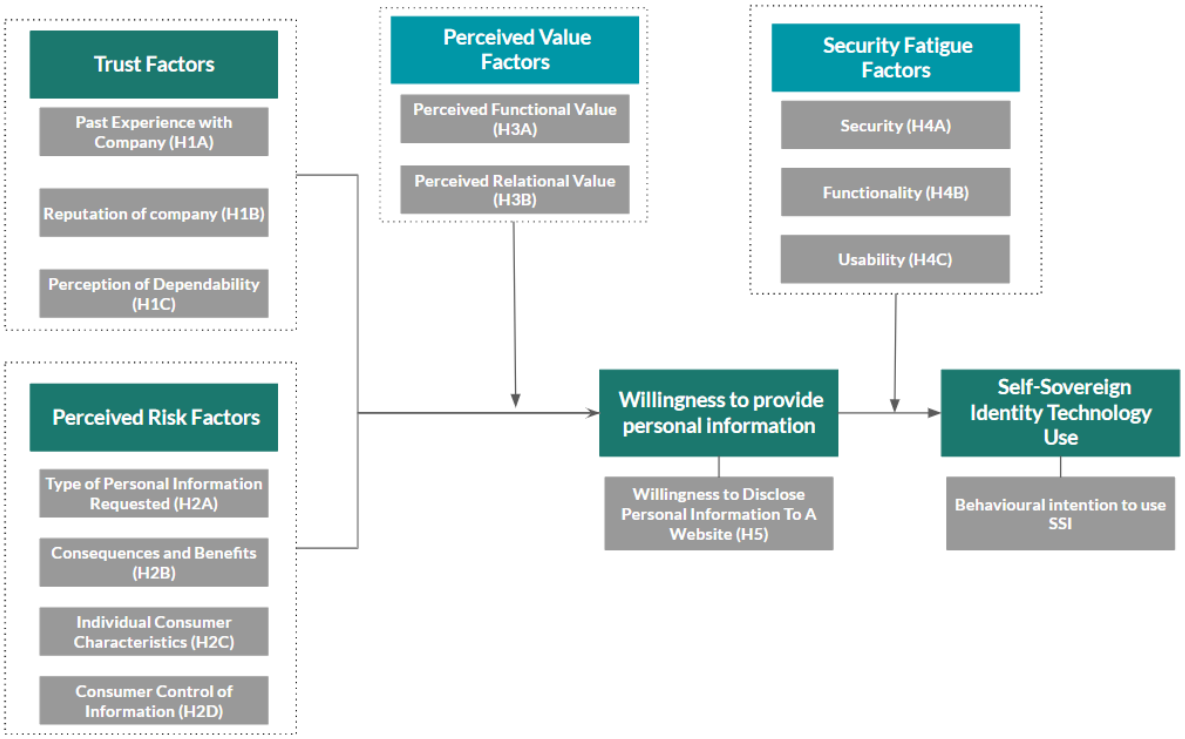

Figure 14. SSI and Willingness to Use Personal Information. Theoretical Framework

The conceptual model proposes three constructs that affect a consumer's willingness to provide personal information:

1. Trust in an organisation
2. Perceived risk
3. Perceived value

Related to the above, the model proposes two constructs that will affect a consumer's willingness to use self-sovereign identity technology:

1. The willingness to provide personal information

2. Security fatigue

Each of these five constructs is concisely illuminated upon in the sub-sections below. A more comprehensive description of each of these constructs is included as a part of the literature review.

3.4.1 Trust in an Organisation

Trust in an organisation is communicated by: *past experience with a company*, *the reputation of a company* and the *perception of dependability*. These sub-constructs are adapted from the work of Schoenbachler and Gordon (2010) and are used to operationalise trust in the organisation. The relevant hypotheses linked to trust in an organisation are restated at the end of this subsection.

As mentioned in the literature review, Schoenbachler and Gordon (2010) found empirical support that trust has a positive relationship with willingness to provide personal information. White (2004) also found that participants who had 'deep relationships' characterised by high-levels of trust, were less reluctant to reveal personal data. This provides support for the relationship between trust factors and a consumers' willingness to provide personal information.

Supporting Schoenbachler and Gordon (2010), Milne and Boza (1999) provided evidence that a direct relationship exists between past experience with a company and the willingness to provide personal information. Other authors such as Ruparelia, White and Hughes (2010), Doney and Cannon (1997) and Chen *et al*. (2010) found support for a positive relationship between trust and past experience with a company. This supports the creation of hypothesis 1A. Fung and Lee (1999), and Sultan and Mooraj (2001) found support for a positive relationship between trust and reputation. Moreover, Xie, Teo and Wan (2006) found a positive association between reputation and decisions to disclose personal information. This supports the creation of hypothesis 1B. Lastly, Swan *et al*. (1988), Yoon (2013), Jiang, Jones and Javie (2008) found positive relationships between trust and dependability which supports the creation of hypothesis 1C.

Hypothesis 1A:

There is a positive relationship between past experience with a company and the willingness of an online consumer to disclose personal information on a website.

Hypothesis 1B:

There is a positive relationship between the reputation of a company and the willingness of an online consumer to disclose personal information on a website.

Hypothesis 1C:

There is a positive relationship between perception of dependability of a company and the willingness of an online consumer to disclose personal information on a website.

3.4.2 Perceived Risk

The relationship between perceived risk factors and the willingness to provide personal information is illuminated with hypotheses relating to the: *type of personal information requested, consequences and benefits, individual consumer characteristics* and *consumer control over information.* These elements are taken from the work of Phelps, Nowak and Ferrel (2000).

As discussed in the literature review, empirical support was provided by Phelps, Nowak and Ferrel (2000), Leon *et al*. (2013) and Metzger (2013) that consumers had differing degrees of willingness to reveal different categories of personal information. These provided support for hypothesis 2A.

If a consumer is given a benefit in exchange for personal information, it has been found to influence the perceived risk posed by disclosing that information. Xie, Teo and Wan (2006) found monetary benefits can lead to greater information sharing of certain categories of information. Additionally, Wang, Duong and Chen (2016) found a negative relationship between benefits and perceived risk via a cost-benefit trade-off mechanism. This led to the suggestion of hypothesis 2B.

Hypothesis 2C, was suggested built on the work of Phelps, Nowak and Ferrel (2000) who after testing a variety of consumer characteristics found that education influenced privacy concern. Age was the focus on this research because Jordaan (2007) found age to be a factor that affected privacy concern in South Africa. The relationship between age and privacy concern was

supported by Zukowski and Brown (2007) as well as Lee, Wong and Chang (2016). These authors found that an older age led to greater privacy concern.

Lastly, Hoadley *et al*. (2011) found that a positive relationship exists between perceived control and privacy concerns. This relationship was supported by the work of Acquisiti and Loewenstein (2013), who illustrated that perceived control can lead consumers to share personal information. This leads to the hypothesis 2D.

Hypothesis 2A:

There is a positive relationship between the type of personal information requested and the willingness to provide personal information to a website.

Hypothesis 2B:

There is a positive relationship between benefits received and willingness to provide personal information to a website.

Hypothesis 2C:

A younger age has a positive relationship with the willingness to provide personal information to a website.

Hypothesis 2D:

Information control has a negative relationship with the willingness to provide personal information to a website.

3.4.3 Perceived Value

Perceived value is hypothesised to function as a moderator. The role of perceived value as a moderator is further operationalised by the sub-constructs: *perceived functional value* and *perceived relational value.* This paper adopts the definition of perceived functional value proposed by Von der Trench *et al*. (2015) who defined it as the perceived benefits from willingly disclosing personal information. Furthermore, we defined perceived relational value as a belief that a relationship with a service or product provider will have a benefit in the future (Tai, 2011).

To-date, literature could not be found that suggests that perceived value acts as a moderator of a consumer's willingness to provide personal information. Authors such as Von der Trench *et al*. (2015) and Wasko and Faraj (2000) suggested that functional value has an impact on

knowledge sharing via a benefit and cost calculation by consumers. Where, if the benefit exceeds the cost, the knowledge will be shared. To some extent, this supports the suggestion of functional value as a moderator. This is because knowledge sharing does not always involve the sharing of personal information but it is still a sharing of information with another party.

As mentioned in the literature review, other authors such as Nahapiet and Ghoshal (1998), Chiu, Hsu and Wang (2006) and Wasko and Faraj (2005) have investigated and found varying relationships between relational capital and information sharing quality and quantity. This provides some support for hypothesis H3B.

Hypothesis 3A:

Perceived functional value moderates the relationship between:

i. Past experience with a company and the willingness to provide personal information on a website.
ii. Reputation of a company and the willingness to provide personal information on a website.
iii. Perception of dependability and the willingness to provide personal information on a website.
iv. Type of personal information requested and the willingness to provide personal information on a website.
v. Benefits received and the willingness to provide personal information on a website.
vi. Individual consumer characteristics and the willingness to provide personal information on a website.
vii. Consumer control over information and the willingness to provide personal information on a website.

Hypothesis 3B:

Perceived relational value moderates the relationship between:

i. Past experience with a company and the willingness to provide personal information on a website.
ii. Reputation of a company and the willingness to provide personal information on a website.
iii. Perception of dependability and the willingness to provide personal information on a website.
iv. Type of personal information requested and the willingness to provide personal information on a website.
v. Benefits received and the willingness to provide personal information on a website.
vi. Individual consumer characteristics and the willingness to provide personal information on a website.
vii. Consumer control over information and the willingness to provide personal information on a website.

3.4.4 Self-Sovereign Identity Technology Use and Security fatigue

To-date, no literature was found which investigates a consumer's willingness to use SSI technology. SSI technology use and its linkage to the willingness of an online consumer to share personal information is a novel concept which has not been proposed before.

In this study, it is proposed that a consumer's willingness to share personal information will have a negative relationship with the use of SSI technology. It is likely that if a consumer will readily share information, using a technology that will allow a consumer to have more control over their information would be unnecessary to these consumers. This led us to hypothesis H5.

Furthermore, this paper proposes that security fatigue will play a role in moderating the relationship between the willingness of consumers to provide personal information and SSI technology use. This paper adopts the definition of security fatigue described by Bada, Sasse & Nurse (2019) as the stress relating to being highly vigilant and security aware.

The sub-constructs: *functionality*, *security* and *usability* are used to further understand and operationalise security fatigue as a moderator. Security is defined in this study as the features on a website that allow a consumer to protect their privacy (Calisir *et al.*, 2010). It is hypothesised that security will moderate and increase the strength of the relationship between

the willingness to share personal information and the use of SSI technology (H4A). This is because a fundamental reason that a consumer might use SSI technology is likely due to its ability to strengthen the security they have over their personal data.

It is hypothesised that usability will moderate and strengthen the relationship between the willingness to share personal information and the use of SSI technology. A more usable technological solution is likely to encourage users who are not willing to share their personal information, to utilise the solution.

Lastly, it is hypothesised that functionality will moderate and lessen the strength of the relationship between security fatigue and the willingness to share personal information. This was proposed because the more functions a tool or service has, the more stress a consumer will experience as they must learn and understand the functionality that they are exposed to.

Hypothesis 4A:

Security moderates the relationship between the behavioural intention to use SSI technology and the willingness to provide personal information.

Hypothesis 4B:

Functionality moderates the relationship between the behavioural intention to use SSI technology and the willingness to provide personal information.

Hypothesis 5:

The willingness to provide personal information has a negative relationship with the behavioural intention to use SSI technology.

The next section focuses on combining the constructs and corresponding hypotheses with suitable measurement scales.

3.5 Measurement and Scaling

Measurement is the linkage of numbers and symbols to objects according to certain predefined rule (Birks and Malhorta, 2006). Scaling involves assigning objects numerical values according to predetermined rules (Birks and Malhorta, 2006).

This focus of this study is to understand the influencers that affect a consumer's willingness to share personal information over the internet; and as a secondary objective, wishes to prove that

there is a negative relationship between a consumer's willingness to provide personal information over the internet and their use of SSI technology.

Research design describes the process required to acquire information which is needed to answer a research problem (Birks and Malhorta, 2006). Research designs can be classified into either exploratory or conclusive designs. Exploratory research has the aim of unravelling marketing phenomena and provide greater insight into these phenomena (Birks and Malhorta, 2006), whereas conclusive research is used to examine hypotheses and unravel relationships (Birks and Malhorta, 2006). Differences and similarities in characteristics, findings and the methods used in exploratory and conclusive research design are depicted in Table 2.

Table 2. Differences between exploratory and conclusion research adapted from Birks and Malhorta (2006).

	Exploratory	**Conclusive**
Objectives	To provide insights and understanding of the nature of marketing phenomena To Understand	To test specific hypothesises and examine relationships To Measure
Characteristics	Information needed may be loosely defined Research process is flexible, unstructured and may evolve Samples are small Data analysis can be qualitative or quantitative	Information needed is clearly defined Research process is formal and structured Sample is large and aims to be representative Data analysis is quantitative
Findings/results	Can be used in their own right May feed into conclusive research May illuminate specific conclusive findings	Can be used in their own right May feed into exploratory research May set a context to exploratory findings
Methods	Expert Surveys Pilot Surveys Secondary data Quantitative Interviews Unstructured Observations Quantitative exploratory multivariate methods	Surveys Secondary data Databases Panels Structured Observations Experiments

This research follows a conclusive research design and therefore aims to examine specific hypotheses as well as the specific relationships between the constructs. There are two types of conclusive research design: descriptive and causal research. The aim of descriptive research is to describe something, such as the features of a marketplace. Although, similar to exploratory research, it differs by including the predefined creation of questions and their hypotheses.

Causal research is used to understand cause and effect relationships (Birks and Malhorta, 2006). Both types of research design have a premeditated and organised design however causal research is the more appropriate approach to determine causal relationships (Birks and Malhorta, 2006).

Given these differences, the design of this research follows a descriptive approach as we seek to better understand the behaviour of consumers who provide information to companies on the internet. When adopting a descriptive research approach, the researcher may further choose to use a cross-sectional or longitudinal design (Birks and Malhorta, 2006). The main difference between these approaches is that a cross-sectional design involves the collection of a sample of population elements only a single time. Longitudinal design involves repeated measurement of a fixed sample *(*Birks and Malhorta, 2006). My study adopts a single cross-sectional design. This differs from a multiple cross-sectional design. In a multiple cross-sectional design there are multiple samples of respondents, and data from each sample is extracted only one time. Primary data was used to illuminate the main research objectives. In order to assess primary data an online questionnaire was developed using a set of predefined questions.

Birks and Malhorta (2006) distinguish scaling techniques into comparative and non-comparative scales. Objects are compared directly in comparative scales (Birks and Malhorta, 2006). This differs from non-comparative scales which involves the independent scaling of each object in the set. According to Birks and Malhorta (2006) non-comparative scales are more extensively used as a scaling technique in market research. This led to the adoption of a non-comparative scale in this research. Continuous rating scales and itemised rating scales are two types of non-comparative scaling techniques. In a continuous rating scale, there is no limitation linked to marks on a scale set by the researcher. The respondent may place a mark at an appropriate position anywhere on the scale (Birks and Malhorta, 2006). Continuous scales have been found to make scoring challenging and unreliable, which has led to limited use in market research (Birks and Malhorta, 2006).

Itemised scales are scales which contain a number or descriptor linked to each category (Birks and Malhorta, 2006). These type of scales have been utilised frequently in market research (Birks and Malhotra, 2006). This paper uses an itemised scale called a Likert scale. This is a measurement scale that has response options such as ‘strongly agree’ and requires a respondent to indicate the extent of the level of their agreement with certain statements linked to objects in the survey (Birks and Malhotra, 2006).

After deciding on the type of scale used, a researcher must make six key decisions. These decisions and the recommendations linked to each decision are provided by Birks and Malhorta (2006) and depicted in Table 3.

Table 3. Recommendations for each factor of an itemised scale (Birks and Malhorta, 2006)

Number of Categories	Although there is no single, optimal number, traditional guidelines suggest there should be between five and nine categories.
Balanced versus unbalanced	In general, the scale should be balanced to obtain objective data.
Odd or even number of categories	If a neutral or indifferent scale response is possible from at least some of the respondents, an odd number of categories should be used.
Forced versus unforced	In situations where the respondents are expected to have no opinion, the accuracy of the data may be improved by a non-forced scale.
Verbal description	An argument can be labelling all or many scale categories. The category descriptions should be located as close to the respond categories as possible.
Physical form	A number of options should be tried and the best one selected.

Guidelines suggest that between five and nine categories are ideal (Birks and Malhorta, 2006). This research adopted seven categories anchored between 'strongly agree' and 'strongly disagree'. The scale used in this research can be described as balanced because three negative options and three positive options are provided to a respondent. One neutral option is also provided. Some respondents may not understand or be familiar with SSI technology, and may give a neutral response. It is for this reason, an odd number of categories was used, as recommended by Birks and Malhorta (2006).

To reduce uncertainty it was decided that all scale categories would be labelled and strong anchors were used. It was noted by Birks and Malhorta (2006) that the adjectives used in the rating scale can influence the response distribution. Response distributions are more peaked when strong anchors are present, vice versa (Birks and Malhorta, 2006). Lastly, several physical forms of a survey are possible - the physical form of the survey is included in the Appendices. The next section develops scales for this thesis, and independent, dependent and moderation models will be described.

3.5.1 Independent variables

The independent variables in my study are *perceived risk, trust in an organisation, perceived value* and *security fatigue.* To operationalise and ensure consistency a 7-point Likert type scale was used for all the independent variables. Likert type scales ask a respondent to indicate their agreement based on the anchors (i.e. strongly agree to strongly disagree) that are present to them. An equal number of anchors that were positive and negative was used, furthermore a

neutral and impartial category was included which does not force respondents to express an opinion. This is different from the approach of Schoenbachler and Gordon (2002) as well as Phelps, Nowak and Ferrel (2000) who did not include a neutral or impartial category. A neutral category was needed because SSI technology is a new technology and some respondents may have no opinion on the technology.

Twelve (12) independent variables were measurable: *past experience with a company; reputation of a company; perception of dependability; type of personal information requested; consequences and benefits; individual consumer characteristics; consumer control of information; perceived functional value; perceived relational value; security; functionality;* and *usability.* For each of these 12 independent variables, a 7-point Likert type was presented to respondents. Two to three statements were made for each variable. A respondent was then asked to indicate the extent of their agreement or disagreement with the given statement.

3.5.2 Dependent Variables

This study has two dependent measures: the willingness of an online consumer to use self-sovereign identity technology, and the willingness of consumers to provide personal information. These dependent variables was operationalised as the respondent's intention and attitude. In the questionnaire, respondents indicated the extent they agreed with statements linked to the two dependent variables, using a 7-point Likert type scale.

3.5.3 Moderating Variables

This study proposes that perceived value moderates the relationship between perceived risk as well as trust in an organisation with the willingness to provide personal information. Similarly, it is proposed that the relationship between the willingness to provide personal information and the use of SSI technology is moderated by the construct security fatigue.

3.6 Questionnaire Design

Specifically, the goals of the questionnaire and how the questionnaire was created are illuminated upon in this section. The final questionnaire which all respondents were shown is indicated in Appendix B. This questionnaire was optimised during pilot-testing.

A questionnaire has three main aims: translate information into questions that respondents are able to answer; inspire respondents to answer, engage and complete the questionnaire and it should minimise response errors (Birks and Malhorta, 2006).

Since the study involves human subjects special consideration was taken for ethical concerns which relate to this questionnaire. This questionnaire was created and met the relevant ethical requirements. The ethical clearance document is attached in Appendix A.

At the start of the survey a lengthy extract is provided which explained the intention of the study. Assurances were given to each respondent with regard to their anonymity, and the protection of their personal information. This initial step is intended to ensure that respondents are confident and informed when answering the survey. A question is also provided to get consent from the respondent to use and disseminate the information that they provide for research purposes, in line with ethics requirements provided by the Commerce Faculty Ethics Research Committee.

In the survey several extracts are provided in Part 1 and Part 3 of the questionnaire. These are explanatory in nature and are intended to ensure that respondents understand what is meant by personal information and SSI technology. The aim was to surmount the respondent's reluctance to answer questions on topics they might not understand or be familiar with. This is aligned with the view of Birks and Malhorta (2006) who suggest that researchers must attempt to reduce barriers that may prevent a respondent from answering.

The more difficult questions form the last part of the questionnaire. This increases the likelihood that respondents will answer these questions once rapport has been established. It was assumed that questions which measure the use of SSI technology would be the most difficult for respondents to answer. This was because respondents were asked to assess their use of a technology they have likely never experienced before.

Conforming to the recommendation of Birks and Malhorta (2006), information relating to the research problem is acquired first and personal identifiably and demographic information is only included in the final part of the survey. Birks and Malhorta (2006) recommend this ordering as classification and identification information may alienate respondents, if it is asked first.

The questionnaire is divided into logical sections that are organised around each of the constructs and sub-constructs depicted in the conceptual model. More specifically, the questionnaire is divided into three parts. The first part is organised around the construct and sub-constructs: perceived risk, trust in an organisation, willingness to provide personal information. The second part relates to questions linked to the use of SSI information and

security fatigue. The final part relates to the classification and identification information of the respondents.

Lastly, voluntary entry into a prize draw for a voucher for online shopping was also provided as part of the survey. This was an incentive to respondents to answer the questionnaire. Birks and Malhorta (2006) acknowledge that an exchange of value occurs when a respondent answers a questionnaire, and one of the desires from a respondent for answering a questionnaire may be a tangible reward.

3.6.1 Part 1: Developing the willingness to provide personal information section

This section focuses on how part 1 of the questionnaire was developed. Part 1 relates to the willingness of an online consumer to provide personal information, as well as its antecedents. The measurement of a consumer's willingness to provide personal information has frequently been operationalised with a survey. As mentioned before, the trust construct relied upon in this study is based on the work of Schoenbachler and Gordon (2002). In the work of these authors, a survey was also used, which validates the use of a survey in this paper to measure the same constructs. Regrettably, the original questions used in the work of Schoenbachler and Gordon (2002) could not be obtained. This meant that other authors were relied upon to create survey questions.

Similarly, the work of Phelps, Nowak and Ferrel (2000) was used to measure the perceived risk construct that is proposed in this study. Fortunately, the questions used by Phelps, Nowak and Ferrel (2000) could be located, and were used as the basis of the sub-constructs: *type of personal information request, individual consumer characteristics* and *consumer control over information.*

Lastly, for perceived value, the work of Tai (2011) was used. Tai (2011) used a self-reporting survey with a 7-point Likert scale to gather data. The questions used and proposed by Tai (2011) to measure the functional and perceived value constructs were used as the basis to measure functional and relational value in this study. To illuminate functional value further, questions based on the work of Bernardo, Marimon and Del Mar Alonso-Almeida (2012) were also used. The work of these authors focused on measuring e-service quality using a structured questionnaire which was delivered via telephone.

Table 4. Questions utilised in the survey and their basis

Independent Variable	Research from which the questions was adapted from
Past experience with a company	Chen, Y.H., Chien, S.H., Wu, J.J. and Tsai, P.Y., 2010. Impact of signals and experience on trust and trusting behavior. Cyberpsychology, Behavior, and Social Networking, 13(5), pp.539-546.
Reputation of a company	Li, Y., 2014. The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision support systems*, *57*, pp.343-354.
Perception of dependability	Macintosh, G., 2002. Building trust and satisfaction in travel counselor/client relationships. Journal of Travel & Tourism Marketing, 12(4), pp.59-74.
Type of personal information requested	Phelps, J., Nowak, G. and Ferrell, E., 2000. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), pp.27-41.
Individual consumer characteristics	
Consumer control over information	
Consequences and benefits	Wang, T., Duong, T.D. and Chen, C.C., 2016. Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*(4), pp.531-542.
Perceived Functional Value	Tai, Y.M., 2011. Perceived value for customers in information sharing services. Industrial Management & Data Systems, 111(4), pp.551-569. Bernardo, M., Marimon, F. and del Mar Alonso-Almeida, M., 2012. Functional quality and hedonic quality: A study of the dimensions of e-service quality in online travel agencies. Information & Management, 49(7-8), pp.342-347.
Perceived Relational Value	Tai, Y.M., 2011. Perceived value for customers in information sharing services. Industrial Management & Data Systems, 111(4), pp.551-56
Willingness to provide personal information	Wang, T., Duong, T.D. and Chen, C.C., 2016. Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*(4), pp.531-542.

A consumer's willingness to disclose personal information was operationalised based on the questions proposed in the work of Wang, Duong and Chen (2016). The authors measured a consumer's intent to disclose personal information via a mobile application. In some instances, questions were added as deemed relevant and based on the authors own knowledge and understanding of personal information and SSI technology.

In an attempt to encourage respondents to complete the survey, questions were limited to 2-4 per variable or sub-construct. An explanation was provided at the start of these sections to explain what could be classified as personal information, so as to reduce the respondent's reluctance to answer questions because they did not know what personal information was.

3.6.2 Part 2: Willingness to use SSI technology

This section focuses on the development and design of Part 2 of the survey which sought to measure a respondent's willingness to use SSI technology. The questionnaire began with an explanation of SSI technology via text and an informational video. It was necessary to add this explanation as respondents were unlikely to have heard the term SSI technology before, and even less likely to have had any experience with the technology.

The willingness to use SSI technology was operationalised based on an understanding of a behavioural intention to use technology as found in Slade *et al*. (2015). Security fatigue was included as a moderator of the use of SSI technology. Table 5 indicates the research that led to the development of questions relating to security fatigue. These survey questions were largely based on the work of Tandon, Kiran and Sah (2016) as well as Lund (2001) and were adapted as necessary to contextualize security fatigue for SSI technology. Similar to the previous section, additional questions were added based on the authors own knowledge and experience.

Table 5. Questions utilised in the survey and their basis (section on SSI)

Security	Tandon, U., Kiran, R. and Sah, A.N., 2016. Customer satisfaction using website functionality, perceived usability and perceived usefulness towards online shopping in India. *Information development*, *32*(5), pp.1657-1673.
Functionality	
Usability	Lund, A.M., 2001. Measuring usability with the use questionnaire. *Usability interface*, *8*(2), pp.3-6.
Use of SSI Technology	Slade, E.L., Dwivedi, Y.K., Piercy, N.C. and Williams, M.D., 2015. Modeling consumers' adoption intentions of remote mobile payments in the United Kingdom: extending UTAUT with innovativeness, risk, and trust. Psychology & Marketing, 32(8), pp.860-873.

3.6.3 Part 3: Demographic Information and Competition

Phelps, Nowak and Ferrel (2000) proposed that individual consumer characteristics would influence the behavioural and attitudinal response of a consumer and their personal information use. The study also sought to measure the effect of individual consumer characteristics on the willingness to provide personal information of consumers. Birks and Malhorta (2006) mentioned that classification and identification information might alienate respondents. This led to the the positioning of identification questions formed the last part of the survey. Furthermore, since entrance into the competition for a voucher may also alienate respondents, as this requires a respondent to provide an email address, it was left to the final question.

3.6.4 Pilot-testing considerations

Pilot-testing is the analysis of a questionnaire on a smaller sample of respondents to reduce errors in the final survey. Birks and Malhorta (2006) view this process as an important part of questionnaire design and recommend that a questionnaire is not used in a field survey without sufficient pilot-testing. It is recommended that pilot-testing is extensive and includes the same layout, sequence, wording and other key characteristics of the questionnaire (Birks and Malhorta, 2006). Adding to this, the pilot-test should be sourced from the same population or sample as the final survey. The sample size of a pilot-test is usually small and consists of 15 to 30 respondents (Birks and Malhorta, 2006).

A pilot-test or pre-test was conducted and was distributed as an online survey to the researcher's network. The pilot test was drawn from the same population as the final survey, namely South African citizens over the age of 18. Questions were included in the survey to confirm that a respondent had lived in South Africa, and was over the age of 18 years. Unfortunately, due to lockdown restrictions imposed by the South African government on account of Covid-19 infections, it was not plausible to conduct pilot-testing via personal interviews (recommended for pilot-testing by Birks and Malhorta, 2006). Fifty two usable questionnaires resulted from the pilot.

After obtaining data from the pilot-testing, the results were analysed. The results were analysed using a factor analysis. Using a factor analysis allows the identification and alteration of questions with a poor response rate. The factor analysis lead to the elimination and rewording of several questions, which had an indicator reliability below 0.4. Indicator reliability is the "*...reliability of a summated scale where several items are summed to form a total score* (Birks

& Malhorta, 2006:314). An indicator reliability above 0.4 and close to 0.7 is recommended by Wong (2013).

This analysis eliminated potential problem areas related to the questions in the questionnaire and provided a more coherent starting point for the final survey to be distributed among a larger sample set.

3.7 Sampling

Once the questionnaire has been adequately designed, the next step was to consider sampling. The goal of a marketing research project is to acquire data about a population. This population can be described as combination of elements that share common traits, and comprehensively describe the whole universe as it relates to a specific market research problem (Birks and Malhorta, 2006).

Obtaining information from a population can be done by taking a census or sample. A census is a complete account of the entire population that relates to the market research problem. On the other hand, a sample is a portion of this population (Birks and Malhorta, 2006). In my study the budget for obtaining information from the population was small and the time available was short. For these reasons a sample was used rather than a census.

Using a sample, means that statistics are employed to make conclusions about the whole population. Birks and Malhorta (2006) described a six step sampling process. This six step process is described below.

3.7.1 Define the target population

The target population is demographically limited to respondents who are currently residing or have resided in South Africa. This is due to budget and resource constraints, which prevented the inclusion of a wider population. The age of respondents was limited to individuals who are 18 years and older. Minors were not of specific interest to the study and were thus excluded.

3.7.2 Sampling Frame

A sampling frame can be described as a method of understanding and describing the characteristic elements of a target population (Birks and Malhorta, 2006). In this study, the sampling frame is a random selection of people who reside in South Africa. To ensure respondents match the sampling frame criteria the question has filter questions at the end which ask a respondent if they reside in South Africa and if they are over the age of 18 years.

3.7.3 Sampling Technique

One of the most critical decisions linked to sample techniques is the use of sampling that utilises or does not utilise probability. Sampling does not utilise probability focuses on the intuition or judgement of the researcher (Birks and Malhorta, 2006). For probability sampling on the other hand, chance is introduced and selected using chance as a key element (Birks and Malhorta, 2006). Due to operational considerations, non-probability sampling was used specifically convenience sampling Birks and Malhorta (2006) describe convenience sampling as the acquisition of a sample in the easiest possible way by the researcher, where the sampling is done at the discretion of the researcher.

Convenience sampling has several benefits over other sampling techniques. It is the least costly and time-consuming of all the techniques which can be used to sample a population (Birks & Malhorta, 2006). This technique also allows increased accessibility to the sample, more assistance and easier measurement (Birks & Malhorta, 2006). Due to the aforementioned reasons, convenience sampling method was used in this study. However, this sampling technique also has several restrictions. Birks and Malhorta (2006) mention selection bias and the sample not being illustrative of any definable population as serious limitations.

3.7.4 Sample Size

Due to time and resource constraints the sample size was set at 300 respondents at a minimum. SmartPLS allows surveys with sample sizes below 100 which made the use of 300 respondents feasible. Supporting this, Wong (2016) notes that PLS-SEM operates effectively on small sample sizes, or sample sizes below 200.

3.7.5 Executing the Sample Process

In this section an outline of the sampling design decisions described above, are depicted.

1. Target population: All genders, 18-65 years old.
2. Sample frame: Random-digit questionnaire procedure.
3. Sample Size: 300
4. Implementation: Providing an online survey to respondents that can be answered online and is distributed to the researchers own network.

3.8 Data Collection and Preparation

This section illustrates how data was collected and prepared. Survey data collected and analysed in this study is classified as primary data. Primary data is created by the researcher to understand and illuminate the research problem (Birks and Malhorta, 2006).

3.8.1 Data Collection

The internet was used for data collection and the survey disseminated among the electronic network of the researcher. Data was collected from the 1st of April 2020 to the 30th of June 2020. The appropriate ethical clearance that was obtained before the commencement of the research (see Appendix A).

3.8.2 Data Preparation

Birks and Malhorta (2006) outlined an 8 step data preparation process which was adopted for this study. This preparation process is depicted in Figure 15.

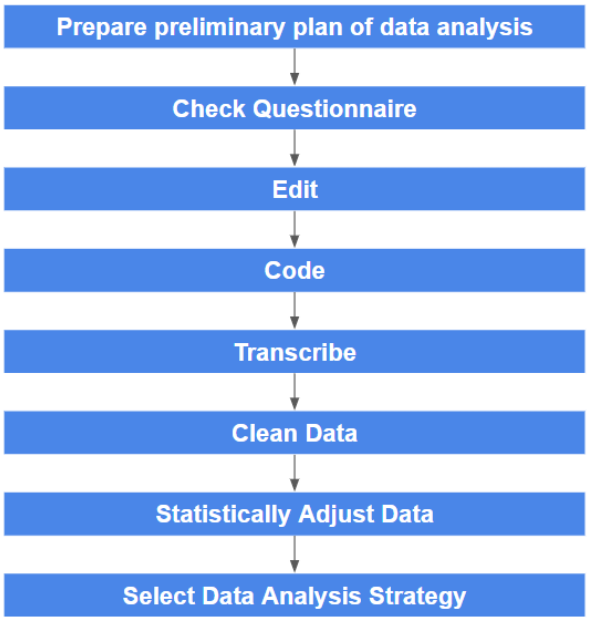

Figure 15. Data Preparation adapted from Birks and Malhorta (2006)

Following the preparation of a preliminary strategy for data analysis, the first step is to check the questionnaire for completeness. Responses that were incomplete were discarded as part of this step. The next step prescribed by Birks and Malhorta (2006) is editing. No edits were necessary as the survey did not contain unstructured questions. Unstructured questions typically require more extensive editing (Birks & Malhorta, 2006). All the questions were also set as required, which means a user could not answer only some of the questions - the user needed to answer all questions. A limit was also set for a question, so that a user could only select one response. This ensured responses were both accurate and precise.

Regarding coding and transcribing, the software used to deliver the survey (Survey Monkey) coded the data automatically. Transcribing was unnecessary as the data was collected via the

internet, and Survey Monkey automatically transcribes the data. This aligns with the views of Birks and Malhorta (2006) who viewed transcribing as unnecessary if data has been acquired over the internet.

Following this step, the data was also cleaned. This combined a handling of missing responses and certain consistency checks. This ensured that data which can be described as out of range, inconsistent and of an extreme value, could be eliminated.

The software used to create the survey and collect data (Survey Monkey) cannot prevent a user from failing to complete the survey. This meant that the data contained missing responses. A missing response can be described as a variable which is not known because the answer is unclear or the answer was not properly recorded (Birks and Malhorta, 2006).

When dealing with missing responses, Birks and Malhorta (2006) describes casewise deletion. Casewise deletion involves disregarding respondents with omitted responses (Birks and Malhorta, 2006). Using casewise deletion can result in sample sizes where are too small (Birks and Malhorta, 2006). This study utilised casewise deletion as the resultant sample was sufficient, when respondents with missing responses were disregarded.

The penultimate step, statistical adjustment is not always necessary but it may be able to enrich the quality of the data analysis (Birks and Malhorta, 2006). There are various methods available for statistical adjustment. Birks and Malhorta (2006) mention three methods: *Weighting, variable re-specification* and *scale transformation*. Weighting describes the assignment of weights to a respondent or case in a database based on their relative importance (Birks and Malhorta, 2006). Variable re-specification involves the formation and modification of new variables by altering data (Birks and Malhorta, 2006). Lastly, scale transformation can be simply described as the manipulation of scale values to ensure comparability (Birks and Malhorta, 2006). How this study approaches missing responses, statistical adjustment and data analysis is described comprehensively in the next chapter which covers the survey results.

3.9 Statistical Analysis

This study utilised the following categories of statistical procedures: descriptive and inferential statistics. Descriptive statistics define the simple features of the data obtained in the research (Trochim, n.d.). Conversely, inferential statistics aim to make conclusions on the population based on the sample, this involves making inferences that extend beyond the sample data (Trochim, n.d.).

3.9.1 Descriptive Statistics

According to Vengura *et al.* (2008:1) descriptive statistics is beneficial when analysing a population by associating a descriptive model with it. The descriptive outcomes of this study were obtained by using Microsoft Excel as well as the software SPSS. To ensure all the questions were well understood by respondents, a factor analysis was conducted. Filter questions were also used to ensure that respondents fit the target group.

3.9.2 Inferential Statistics

On the other hand, inferential statistics is a branch of statistics that is useful when an inference on the sample population is desirable, and a subset of sample data from the population is available (Vengura *et al.*, 2008). Simply put, inferential statistics involve making predictions about the population based on a sample of data, these predictions are operationalised with hypotheses on the population.

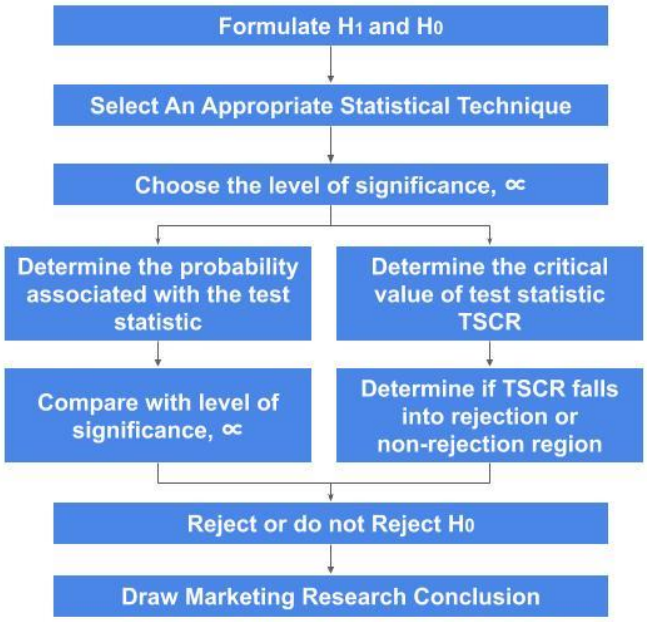

Figure 16. General Procedure for Hypothesis Testing adapted from Birks & Malhorta (2006)

Birks and Malhorta (2006) describe a general procedure to test a hypothesis which is indicated in Figure 16. According to Birks and Malhorta (2006) the steps indicated in Figure 16 allow the acceptance or rejection of a hypothesis.

3.9.2.1 Visualisation of the model

The theoretical model proposed in this study is complex. There are multiple dependent and independent variables. The main objective of this research however, is to demonstrate, or not, the willingness to use a new technology.

Structural equation modelling (hereafter referred to as SEM) relies on a mixture of factor and regression path analysis (Hox and Bechger, 1999). This model is interested in theoretical constructs represented by latent factors (Hox & Bechger, 1999). According to Steenkamp and Baumgartner (2000) SEM is based on three principles. Firstly, when a single indicator is unable to capture a full understanding of an underlying construct, SEM's focus on construct operationalisation is a useful and unique feature. Secondly, an "*...interplay between constructs and measures play a crucial role in theory development and model testing*" (Steenkamp and Baumgartner, 2000:196). This assists with measurement fault and the correspondence between measures and constructs. Lastly, SEM is covariance-based rather than variance-based. This means SEM places greater emphasis on marketing phenomena, as opposed to approximating outcome variables. These benefits make SEM highly suitable for the visualisation of the proposed model in this study.

This study uses of partial least squares SEM. Covariance-based SEM is another form of SEM which focuses on the validation and denial of theories by comparing how well a model estimates a covariance matrix (Hair *et al*., 2013). Partial least squares (hereafter referred to as PLS) SEM focuses on exploratory research and focuses on variance which relates to latent variables (Hair *et al*., 2013). It is advisable to use PLS SEM when the sample size is not large and applications do not have a large volume of existing literature or theory (Wong, 2013). Conforming to the above, PLS SEM was used as this research focuses on the creation of new theories and the sample size was small.

An important first step, when a research project involves SEM is to prepare a path model. A path model shows the hypotheses and indicates the variable relationships that will be analysed (Hair *et al*., 2014). According to Hair *et al*. (2013), the path model should include the following elements: *indicator variables, factor variables, measurement model* and *structure model*. These variables and the path model are depicted in Figure 17.

Hair *et al*. (2014) describes how elements of a path model are visualised. In a path model, circles or ovals show the constructs that are not directly measured. Rectangles show indicators which are directly measured variables that contain the raw data. Relationships between various constructs are indicated using arrows. Single headed are always used to assist with the depiction of directional relationships. A structural model or inner model is also depicted in a path model. This represents the constructs and the relationship between these constructs. This visually signifies the 9 hypotheses concerning the willingness to provide personal information, as well as the willingness to use SSI. A measurement model is also shown which indicates the relationship between constructs and their indicator variables. There are generally two types of models are used for measurement. A model for exogenous latent variables which are constructs that explain other constructs in the model, and a model for endogenous latent variables that are being explained within the model.

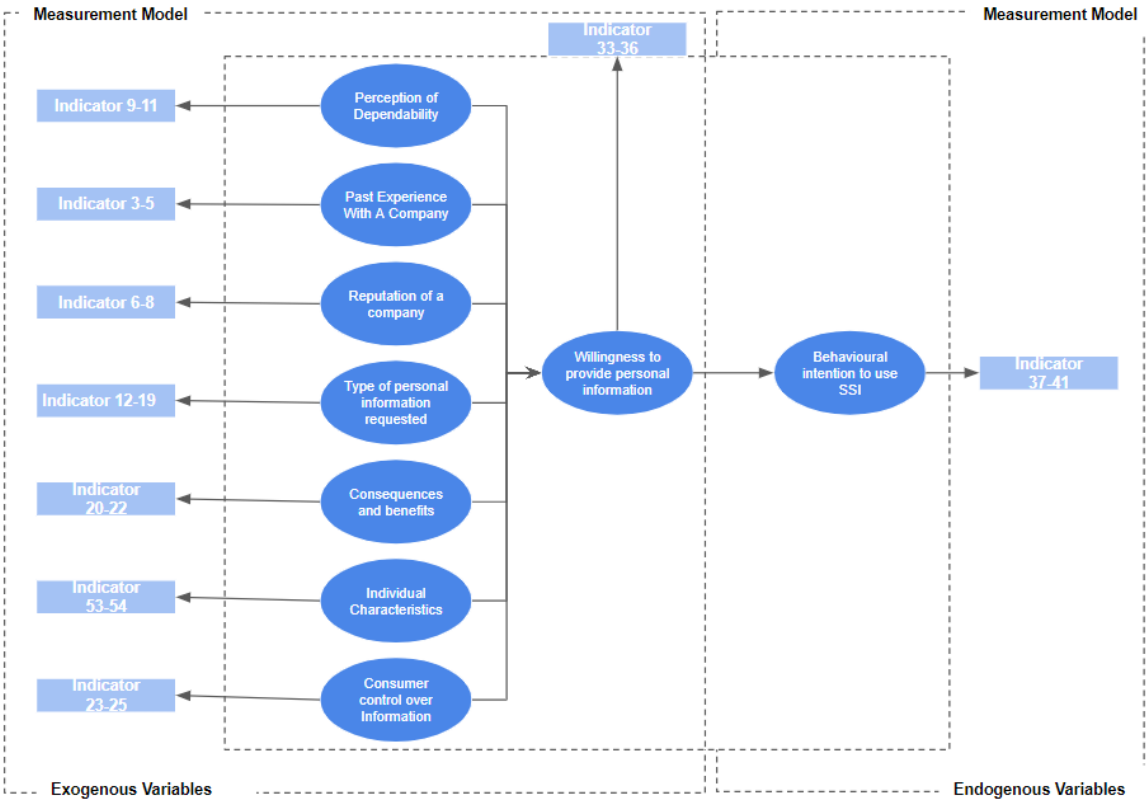

Figure 17. Path Model

3.9.2.2 Operationalisation

There are several ways to analyse the variance linked to partial least squares SEM. This study uses SmartPLS because it is freely accessible and the program has an active discussion forum which can assist researchers, if they require help with the modelling (Wong, 2013).

3.9.2.3 Measurement Model

There are two types of measurement scales: formative and reflective (Wong, 2013). Formative scales are described as follows: "*If the indicators cause the latent variable and are not interchangeable among themselves, they are formative"* Wong (2013:14). On the other hand, Wong (2013:15) describes reflective measurement scales as indicators which are: "*highly correlated and interchangeable, they are reflective and their reliability and validity should be thoroughly examined…*" In this study, a reflective measurement model was adopted as some of the variables have a high degree of correlation and interchangeability.

Reliability and validity must be examined when using a reflective measurement scale (Wong, 2013). Birks and Malhorta (2006) recommend the use of an index of fit or R-square to evaluate reliability and validity. The coefficient of determination measures the degree of association between two variables and their relative strength.(Birks and Malhorta, 2006). The R-squared value should at least be 0.25 for a marketing research study (Wong, 2013).

Internal consistency reliability is a measure of the "*...reliability of a summated scale where several items are summed to form a total score*" (Birks and Malhorta, 2006:314). As they explain, coefficient alpha is a valuable measure of internal consistency reliability. The value for coefficient alpha varies from 0 to 1, with a value below 0.6 indicates inadequate internal consistency validity (Birks and Malhorta, 2006). In line with Birks and Malhorta (2006), when using SmartPLS, Wong (2013) advocates for consistency reliability this is at least 0.6.

Birks and Malhorta (2006) explains validity as whether the phenomenon analysed signify certain features. Convergent validity is an important type of validity. "*Convergent validity is the extent to which the scale correlates positively with other measurements of the same construct*" and "*discriminant validity is the extent to which a measure does not correlate with other constructs from which it is supposed to differ*" (Birks and Malhorta, 2006:315).

These two measures of validity are used to enable confirmation of the validity of constructs included the model. Average variance extracted (hereafter referred to as AVE) allows for the analysis of convergent validity. AVE values should be greater than 0.5 according to Wong (2013). AVE describes how a single latent variable is able to decipher the indicator variables and can be used to operationalise convergent validity. This value should be at least 0.5 (Bagozzi and Yi, 1988).

Discriminant validity should also be used in SmartPLS as a requirement for construct validity. Birks and Malhorta (2006:315) define discriminant validity as "*a type of construct validity that*

assesses the extent to which a measure does not correlate with other constructs from which it is supposed to differ." Another way to measure discriminant validity is using the Fornell and Lacker criterion. It has been suggested by Fornell and Lacker (1981) that taking the square root of each AVE in each latent variable may be used as a measure of discriminant validity (Wong, 2013). More specifically, for each individual latent variable, the square root of AVE must be of a higher value than the latent variables that are measured (Wong, 2013). In the next section the operationalisation of the structural model is illuminated.

3.9.2.4 Structural Model

The next step after considering reliability and validity is an examination of the structural model should be conducted (Hair *et al*., 2014). There is considerable complexity in this study's structural model, due to the moderation construct which can be seen in Figure 19.

The inner or structural model shows the proposed hypotheses, which is assisted visually by arrows. This is relationship is indicative of the relationship between the trust and perceived risk with the willingness to disclose personal information, and ultimately the willingness to use SSI technology. SmartPLS software was used to verify these hypotheses. This software is useful and appropriate when examining PLSE-SEM (Wong, 2013; Hair *et al*., 2013).

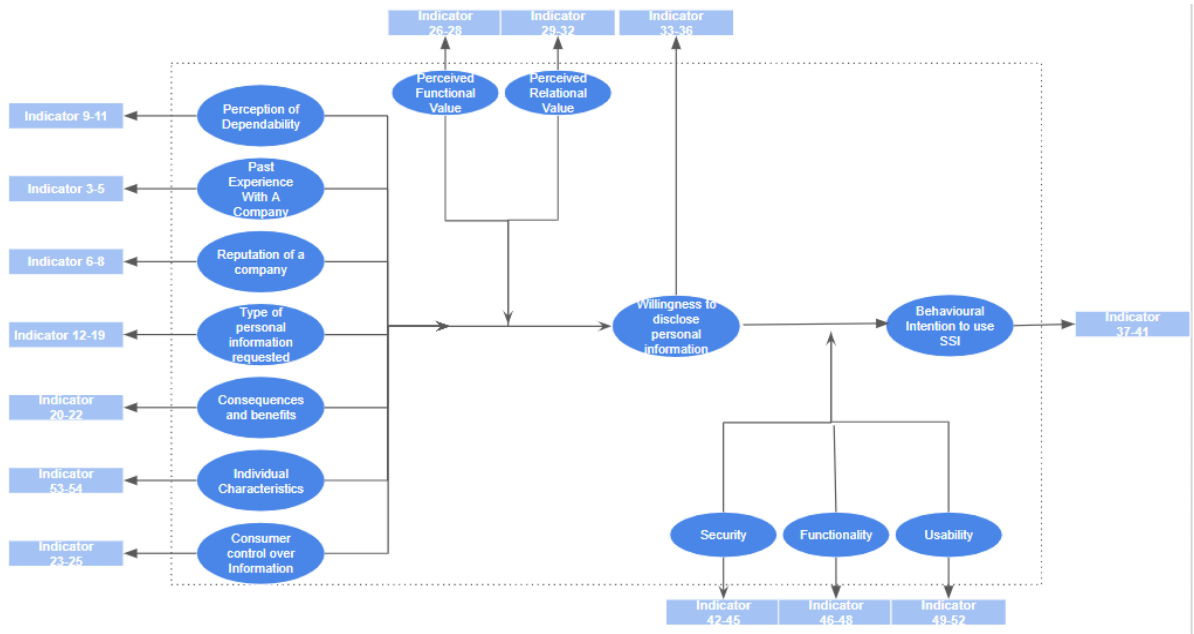

Figure 17. Structural Model

SmartPLS software provides the user with the coefficient of determination, t-test, p-values and beta coefficients. These variables were used to confirm the hypotheses. SmartPLS harnesses the coefficient of determination to indicate how well a model fits to data (Wong, 2013; Hair *et al*., 2013). This coefficient must have a value between 0 and 1. T-tests are important to confirm

hypotheses in a model (Hair *et al*., 2013). More specifically, a t-test measures whether a null hypothesis is supported (Birks and Malhorta, 2006). A null hypothesis is validated when a t-statistic, at a significance level of 0.05 gives a value lower than 1.96. An alternative hypothesis becomes valid, when a t-statistics is higher than 1.96 at a significance level of 0.05.

P-values also allow one to verify a hypothesis. P-values are probability based and range from 0 to 1. Generally, a smaller p-value is indicative that there is stronger support that you should dismiss the null hypothesis. For SmartPLS the p-value should not exceed 0.05 (Hair *et al*., 2013).

A hypothesis must be significant, for it to make sense to interpret the beta coefficient (Hirschfelder, 2015 citing Pallant, 2013). Furthermore, when interpreting the beta coefficient it is advisable to consider standardised values (Hirschfelder, 2015 citing Pallant, 2013). This led to the transformation of the beta coefficient to an equivalent scale to enable comparison.

3.9.2.5 Moderation Model

SmartPLS was not suitable for the volume of moderation paths that is required by the structural model in this study, to be tested at once. This meant every single model had to be separately tested. Fortunately, a macro called PROCESS that was developed by Hayes (2015) allows for the simplification of the confirmation of moderation. This study used PROCESS to test all the moderation paths for significance.

P-value is considered the most important to prove significant interaction, when analysing moderation models. In this case, the p-value will decipher whether moderation exists between the dependent and independent variables (Hirschfelder, 2015 citing Field, 2013). Generally, this p-value should not exceed 0.05 to prove moderation is present (Hirschfelder, 2015 citing Hayes, 2013).

The unstandardised beta coefficient can also be used to illuminate associations between the predictor and moderator variables, and their corresponding strength (Hirschfelder, 2015). Negative beta coefficients show a negative relationship, where an increase causes a decrease in the strength of the moderator (Hirschfelder, 2015 citing Field, 2013). The opposite is also true, a negative beta coefficient is indicative of a negative relationship between moderator and predictor. Specifically, this means an increase in the moderator leads to an increase of the predictor (Hirschfelder, 2015 citing Field, 2013).

3.10 Conclusion

This chapter described the methodology that is used in this study, and this included a description of the objectives and related hypotheses. It also included detail on the measurement and scaling, questionnaire design, sampling and data collection which is harnessed in this study. Finally, the statistical analysis was described in detail. The next chapter, shows the results that were obtained in this study which is based on the methodology that is described in this chapter.

CHAPTER FOUR: RESULTS

4.1 Introduction

Chapter Four reports on the statistical results of the data collected using the online survey. Before these statistical results are discussed, the relevant hypotheses and their relation to the aforementioned theoretical framework is restated. Thereafter, the procedure which was followed for fieldwork is described as well as the features of the sample and responses. Lastly, discussion and inferential statistics are presented, which includes a synopsis of the findings of this chapter.

4.2 Hypotheses and the Theoretical Framework

The hypotheses indicated below are discussed again. These hypotheses and the theoretical model are restated below. The various hypotheses are consolidated in this chapter to allow for discussion and reporting of the results.

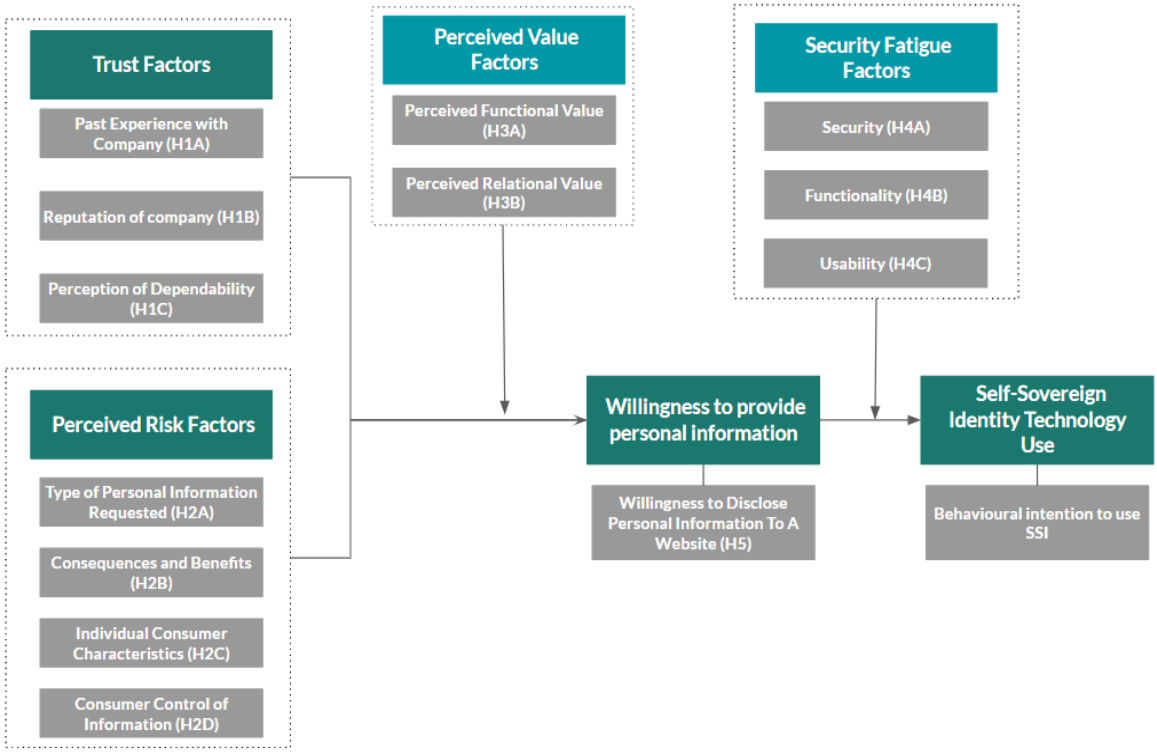

Figure 18. Theoretical Model

Hypothesis 1A:

There is a positive relationship between past experience with a company and the willingness of an online consumer to disclose personal information to a website.

Hypothesis 1B:

There is a positive relationship between the reputation of a company and the willingness of an online consumer to disclose personal information to a website.

Hypothesis 1C:

There is a positive relationship between perception of dependability of a company and the willingness of an online consumer to disclose personal information to a website.

Hypothesis 2A:

There is a positive relationship between the type of personal information requested and the willingness of an online consumer to provide personal information to a website.

Hypothesis 2B:

There is a positive relationship between benefits received and willingness of an online consumer to provide personal information to a website.

Hypothesis 2C:

A younger age has a positive relationship with the willingness of an online consumer to provide personal information to a website.

Hypothesis 2D:

Information control has a negative relationship with the willingness of an online consumer to provide personal information to a website.

Hypothesis 3A:

Perceived functional value moderates the relationship between:

i. Past experience with a company and the willingness of an online consumer to provide personal information on a website.
ii. Reputation of a company and the willingness of an online consumer to provide personal information on a website.
iii. Perception of dependability and the willingness of an online consumer to provide personal information on a website.
iv. Type of personal information requested and the willingness of an online consumer to provide personal information on a website.
v. Benefits received and the willingness of an online consumer to provide personal information on a website.

vi. Individual consumer characteristics and the willingness of an online consumer to provide personal information on a website.
vii. Consumer control over information and the willingness of an online consumer to provide personal information on a website.

Hypothesis 3B:

Perceived relational value moderates the relationship between:

i. Past experience with a company and the willingness of an online consumer to provide personal information on a website.
ii. Reputation of a company and the willingness of an online consumer to provide personal information on a website.
iii. Perception of dependability and the willingness of an online consumer to provide personal information on a website.
iv. Type of personal information requested and the willingness of an online consumer to provide personal information on a website.
v. Benefits received and the willingness of an online consumer to provide personal information on a website.
vi. Individual consumer characteristics and the willingness of an online consumer to provide personal information on a website.
vii. Consumer control over information and the willingness of an online consumer to provide personal information on a website.

Hypothesis 4A:

Security moderates the relationship between the behavioural intention to use SSI technology and the willingness of an online consumer to provide personal information.

Hypothesis 4B:

Functionality moderates the relationship between the behavioural intention to use SSI technology and the willingness of an online consumer to provide personal information

Hypothesis 4C:

Usability moderates the relationship between the behavioural intention to use SSI technology and the willingness of an online consumer to provide personal information

Hypothesis 5:

The willingness to provide personal information over the internet has a negative relationship with the behavioural intention to use SSI technology.

Firstly, the hypotheses grouped under trust in an organisation are discussed. This contains hypotheses 1A to 1C. Next, hypotheses falling with the perceived risk model are discussed, which contains hypotheses 2A to 2C. Following this, hypothesis 5 is discussed which relates to a key objective of this study, to investigate and prove a negative relationship between the behavioural intention to use SSI technology and the willingness to provide personal information.

As mentioned before, the hypothesised relationship between trust factors and the willingness to provide personal information was based primarily on the work of Schoenbachler and Gordon (2010). In the same vein, the hypothesised relationship between perceived risk and the willingness to provide personal information is derived primarily from the work of Phelps, Nowak and Ferrel (2000). To the researcher's knowledge hypothesis 5 is exploratory and not based on the work of any published authors. The hypothesis was created on the logic if a consumer will readily share information, using a technology that will allow a consumer to have more control over their information would be undesirable or unnecessary to these consumers

The discussion on the moderation model follows, which includes perceived value factors and hypotheses 3A and 3B and 4A to 4C. Tai (2011) was relied upon as a basis to propose perceived value as a moderator and Waite (2010) formed the basis of conceptualising security fatigue as a moderator. For a more detailed breakdown of prior work relating to each hypothesis, refer to the aforementioned literature review. The next section presents the fieldwork report; how the methodology was implemented; and an evaluation of the survey.

4.3 Fieldwork Report

Before the fieldwork was conducted, appropriate ethical approval was obtained. The approval is attached in Appendix A.

The data was collected online and an online survey was distributed to research participants. These research participants formed part of the researcher's personal and professional network. Specifically the survey was sent to respondents via WhatsApp, posted on Facebook and sent to colleagues at Nimble Group. The respondents were informed that all the data they provided would be treated confidentially, and that response was voluntary. Respondents were also

informed they could withdraw from the research at any point. The survey period (excluding the pilot) was from the 7th of June 2020 to the 28th of June 2020. For details on the contents of the survey refer to Appendix B. Results could be exported directly from Survey Monkey into Microsoft Excel. The results only needed to be formatted to be usable in the statistical programs SPSS and SmartPLS.

4.4 Sample Size

The sample size for analysis amounted to 572 respondents and 347 respondents were usable for statistical purposes. Of the 572 respondents, 3 did not consent to the research, 12 respondents did not consent to their responses being disseminated anonymously, 6 respondents did not fit the target group of living or having resided in South Africa, and 4 respondents were under the age of 18. In addition, 209 respondents only partially completed the survey. For the 347 usable responses, 116 (33%) of respondents identified as male, 223 (64%) respondents identified as female, 2 identified as neither male nor female and 7 respondents preferred not to answer. Table 6 provides a summary of the sampling results.

Table 6. Breakdown of Sampling Results

Total Sample Size	572
Did not consent to research	3
Did not consent to response being shared and disseminated anonymously	12
Incomplete Responses	209
Did not fit target group	10
Gender breakdown of 347 usable responses	33% (116) male 64% (221) female 0.58% (2) Other 2% (7) Prefer Not To Answer

The next section expands on descriptive and inferential statistics. Descriptive statistics allow a researcher to understand the sample set, or the 347 usable responses. Often a few summary values are provided to describe these responses meaningfully in descriptive statistics. On the

other hand inferential statistics involves making predictions on the entire population, from which the sample set was drawn. This means making predictions about the target group, South African residents, above the age of 18 years based on the 347 usable responses.

4.5 Descriptive Statistics

In this subsection, the descriptive statistics are organised into 6 sections. The first and second section discuss descriptive statistics for the *trust* and *perceived risk* factors. The third section focuses on *consumer characteristics* which was a special case that led to a descriptive analysis per age grouping. The willingness to provide *personal information* and the behavioural *intention to use SSI technology* are discussed in sections four and five. The sixth and seventh section focus on factors relating to *perceived value* and *security fatigue* which were proposed as moderators in this study.

The measurement of most of these factors was done using a 7-point Likert-type scale. The respondents indicated their agreement to statements, which were coded as follows: strongly disagree (1), disagree (2), somewhat disagree (3), neutral (4), somewhat agree (5), agree (6), strongly agree (7).

The exception was hypothesis 2B, which hypothesised a relationship between consumer characteristics and the willingness to provide personal information. Consumer characteristics consisted of a consumer indicating whether their age fell within a certain age group. This was coded as follows: Under 18 (1), 18-24 (2), 25-34 (3), 35-44 (4), 45-54 (5), 55-64 (6) , 65+ (7).

Likert-type scales are ordinal in nature. However, it is common to treat Likert-type scales as interval measurements (Blaikie, 2003). Ordinal scales do not allow differentiation between single items, whereas intervals allow for differentiation which allows for differences in rank and distance to be measurable. Mean and standard deviation are useful when interval scales are evaluated descriptively (Toutenburg & Heumann, 2009 as cited by Hirschfield, 2015). The mean and standard deviation were analysed using SPSS, and are included as part of the results in Appendix B.

4.5.1 Trust Factors

This subsection focuses on the trust factors: past experience with a company; reputation of a company; and perception of dependability. Past experience was polled with three items. The mean for past experience ranged from 4.15 to 4.78. Four (4) is indicative of a neutral response to the statement whereas 7 is indicative of strong agreement. The standard deviation was

between 1.67 and 1.71. This indicates that the majority of respondents felt that past experience with a website does have an effect on their willingness to disclose information, generally.

For reputation of a company, the mean was between 4.86 and 5.47 and the standard deviation was between 1.54 and 1.62. Compared to past experience, reputation shows an even stronger tendency towards positive agreement. Lastly, perception of dependability had a mean ranging from 4.91 to 5.12 and a standard deviation ranging from 1.45 to 1.53. This means perception of dependability had a strong tendency towards agreement.

Of all the trust factors, the question stating "I generally disclose my information to websites which have a reputation for respecting their customers wishes linked to privacy" had the highest tendency towards agreement. This may be indicative that a consumer who has had their privacy violated before, will be unlikely to disclose their personal information again.

4.5.2 Perceived Risk Factors

Similar to the section on trust factors, this subsection focuses on the following perceived risk factors: *type of personal information requested*; *consequences*; *benefits*; and *consumer control over information* and individual consumer characteristics.

Type of personal information requested was polled by the most questions in the survey. Eight (8) questions were asked in total. The results are graphically depicted in Figure 21. Questions related to a variety of information types. When the question related to highly sensitive information that could be used to identify the person directly, it was framed in the negative, or the respondent's willingness to not disclose that information type.

For information that could be used to identify a respondent directly, the mean varied from 5.6 to 6.49. This tendency towards strong agreement may mean personal identifier information is the least likely to be disclosed by South Africans over the age of 18. Identity number and biometric data had the highest relative mean values of all the information types, and the lowest standard deviations. This indicates a strong unwillingness to disclose these information types. On the other hand, information that would be difficult to use to identity a person such as age, qualification and favourite hobbies also had a mean above 5. This indicates a willingness for a consumer to disclose these less sensitive information types.

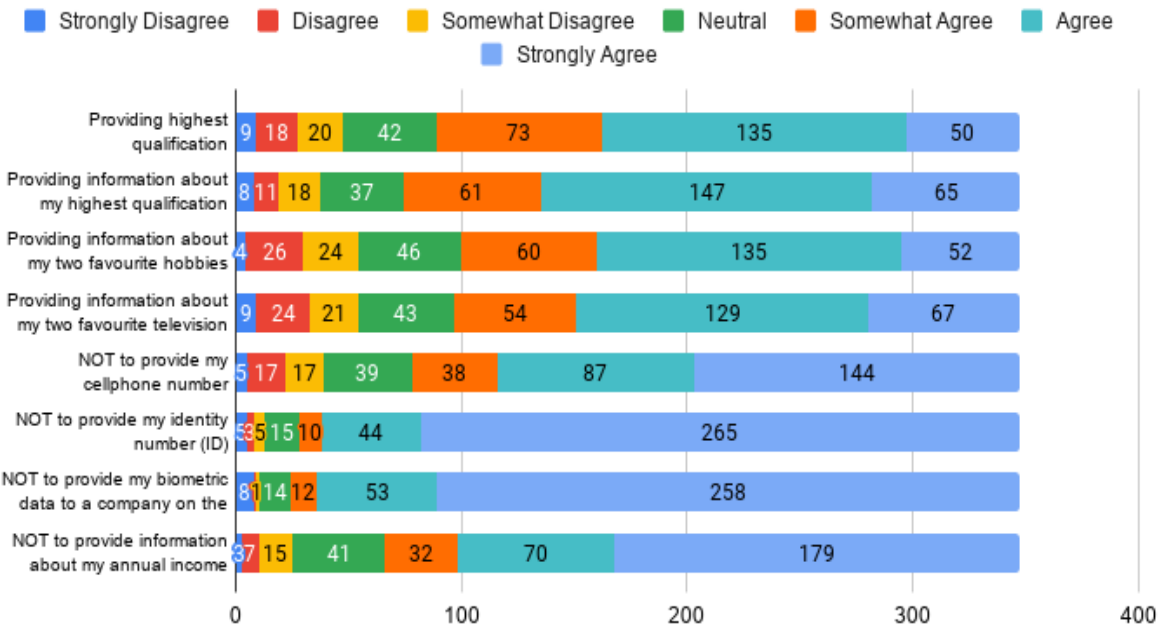

Figure 19. Willingness to Disclose or Not Disclose Different Information Types

For questions relating to consequences and benefits, the mean ranged from 3.71 to 3.9. These questions asked a respondent whether they would disclose personal information for a monetary benefit, saving or free goods. This indicates that most respondents did not believe an incentive could change their willingness to disclose information. However, 92% of respondents provided their email address, a form of personal information to be eligible for the monetary incentive to complete the survey. This may show misalignment between the actual behaviour of consumers, and their self-reported intention. The survey focused on disclosing information to an online website, whereas their email was provided for the purposes of winning a prize as part of an academic survey.

Consumer control over information had a mean ranging from 6.41 to 6.55 and relatively low standard deviation of 0.86 to 0.99. This variable showed the strongest agreement of all the

questions that were polled in the survey. This may show that almost all consumers desire stronger control over their personal information.

4.5.3 Willingness to Provide Personal Information

A respondent's willingness to disclose personal information was polled with 4 questions. Overall, respondents showed a tendency towards disagreeing that they were willing to disclose personal information to a website, and that their willingness to disclose personal information could be self-evaluated as high. Contrary to this, respondents showed a tendency to agree that they would disclose personal information if a website asked them to do so, and they were willing to fill in personal information to access a product or service. This may be indicative that consumers are used to disclosing information as a part of conducting activities over the web, and they tend to disclose information if asked to by a website, or if it is required to conduct activities on the web.

4.5.4 Behavioural intention to use SSI technology

Overall, the behavioural intention to use SSI technology showed a strong tendency towards agreement for the statements that were posed to respondents. If we exclude the question on using SSI technology to obtain a monetary benefit (question 41), the mean ranged from 5.1 to 5.55. This indicates that respondents may be highly likely to adopt SSI technology, if given the option to do so.

Question 41, had a mean of 4.37 showing a tendency towards disagreement and the highest standard deviation of all questions. This question asked a respondent to indicate their agreement to the following statement: "I would consider using the technology in the scenario to sell my personal information for my own monetary benefit, if the monetary benefit was high enough and it was safe to do so."

The high standard deviation may show the exchanging monetary benefits for personal information is highly desirable for some consumers and highly undesirable for others. Combined with the analysis on consequences and benefits and question 22, it seems that exchanging a monetary benefit for personal information may not be a desirable exchange for a consumer.

4.5.5 Consumer characteristics

This subsection focuses on the consumer characteristics of age group and its influence on the willingness to provide personal information. Figure 21 indicates the breakdown of the usable

sample. The sample size mainly consisted of respondents between the ages of 18-44, and most of the sample fall within the youngest age grouping of 18-24 years.

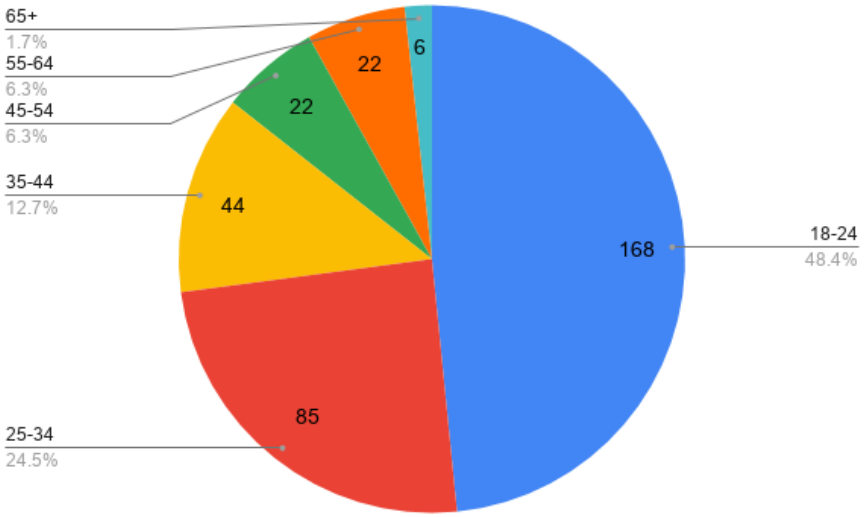

Figure 20. Age Breakdown of Usable Responses

The next step after understanding the breakdown of the sample size was to compare the responses for the questions polled per age group. This was done exclusively for the questions relating to a respondents willingness to disclose personal information. The age grouping 65+ was excluded due to the low volume of respondents from this age group.

When the data was analysed per age group, a trend emerged that younger respondents indicated a stronger tendency to agreement with the 3 of the 4 polled questions for the willingness to provide personal information. This means that younger respondents may be more willing to disclose personal information than older respondents, in South Africa. The exception was question 36 which asked a respondent to indicate their agreement to a statement where they self-evaluated their willingness to disclose personal information as high. For question 36, the age groupings 18-24 and 25-34 had similar means of 3.51. However, the 18-24 and 25-34 still showed a higher tendency towards agreement then the older counterparts whose aged ranged from 35-64.

4.5.6 Perceived Value

This subsection focuses on perceived functional value and perceived relational value. The 3 questions used to poll perceived functional value were all in positive agreement territory and the mean ranged from 4.98 to 5.51. Question 26 had the highest mean and lowest standard deviation of all the questions polled for perceived functional value. This may indicate that

quality of a good or service provided in exchange for personal information, is one of the most important functional value factors that consumers consider.

Perceived relational value was polled with 4 questions. 3 of the questions were in positive agreement territory, with means ranging from 4.46 to 4.92. One question was in negative agreement territory with a mean of 3.25, and a relatively high relative standard deviation of 1.60. This question related to the perceived comfort consumers experience when disclosing personal information. The reason for this disagreement may be because consumers experience an inherent discomfort when disclosing personal information regardless of the relationship they have with the website.

4.5.7 Security Fatigue

In this section, the security fatigue factors are focused upon. Comparatively, all the questions polled under security fatigue had a mean above 5, indicative of a strong tendency towards agreement. This may be indicative that security, functionality and usability are important considerations that a consumer will take into account before using a SSI technological solution.

The questions polled for security had a mean ranging from 5.53 to 5.98. The statement "I imagine myself using the technology in the scenario, if the security features allow me to effectively protect my privacy" had the highest mean and lowest standard deviation of all the questions polled for security. This means privacy protection afforded to consumers by SSI technology, may contribute decisively to whether a consumer uses the technology or not. This makes intrinsic sense as SSI technology is positioned as a privacy protection solution.

Questions polled for functionality also showed a high tendency towards to agreement. Controlling access to their personal data, seems to be an influential factor that affects a consumer's intention to use SSI technology. This had the highest mean (5.93) of all the functionality factors. This conclusion seems to agree with a consumer's tendency to desire more control over their personal information, which has already been discussed.

Lastly, questions polled for usability had a mean between 5.64 and 5.84. Whether a SSI technological solution is easy to use seems to be an important factor which influences a consumer's decision whether to use SSI technology. This is important in the context of SSI solutions. As mentioned before, Dunphy and Petitcolas (2018) analysed three popular identity management systems that use blockchain (*uPort, ShoCard* and *Sovrin*) and found usability to be a key area of improvement.

4.5.8 Conclusion

Descriptive results provide initial and important insight into the data. With exception of some questions, most of the polled questions show a tendency towards agreement. This shows some indication that *trust*, *perceived risk* and *perceived value* factors are important considerations when consumers decide to disclose personal information. The polled questions also show a tendency for respondents to adopt SSI technology.

4.7 Inferential Statistics

Inferential statistics involves making predictions on the entire population from which the sample set was drawn. This is done using theories relating which utilise probability. The conclusions drawn for inferential statistics allow the acceptance or rejection of the hypotheses.

This section begins with an analysis of the outer or measurement model which was illuminated in the methodology section and which involves analysing the reliability and validity of this measurement model, using structural equation modelling or SEM. This was done using the software, SmartPLS. After this is completed, the hypotheses posed in this paper are verified using structural model.

4.7.1 Measurement Model

Reflective measurement scales are indicators which are: "*highly correlated and interchangeable, they are reflective and their reliability and validity should be thoroughly examined…*" (Wong, 2013:15). Following the recommendations of Wong (2013), an analysis of internal consistency reliability and construct validity was done to verify the measurement or outer model.

4.7.2 Internal Consistency Reliability

Cronbach's Alpha is useful to analyse consistency reliability of the variables (Wong, 2013; Malhorta, 2010). Cronbach's alpha should be 0.7 or higher to be satisfactory (Wong, 2013; Malhorta, 2010). The requirement for composite reliability is relaxed if it is exploratory research design, and levels of 0.6 and higher are acceptable (Wong, 2013). As mentioned, this research follows a conclusive research design so this lower level was not applicable

PLS-SEM allows for the use of single item constructs. Single item constructs have been deployed frequently in PLS-SEM models (Ringle, Sarstedt and Straub, 2012). For obvious reasons, only one question on age was included in the survey. Age was also the only item which was used to measure consumer characteristics, which is a variable that forms a part of the

perceived risk factors. This led to a values of 1 for Cronbach's Alpha and Composite Reliability. This is because reliability measures how close the relationship between items are, and with only a single item, the Cronbach's Alpha and Composite reliability will always be 1.

Table 7. Results for Internal Consistency Reliability

	Cronbach's Alpha	Composite Reliability
Behavioural Intention to Use SSI	0.9	0.929
Consequences and Benefits	0.897	0.936
Consumer Characteristics	1	1
Consumer Control Over Information	0.872	0.921
Past Experience With Company	0.876	0.924
Perception of Dependability	0.859	0.915
Reputation of a company	0.867	0.918
Type of Personal Information Requested	0.46	0.047
Willingness To Provide Personal Information	0.85	0.899

Table 7 indicates all the values, except for the type of personal information requested, meet the 0.6 threshold for the internal consistency reliability. Eight questions were polled for the type of personal information requested. 4 of these questions can be described as relating to 'sensitive information' that could be used to identify a respondent directly. These 4 questions were framed in the negative. The other 4 questions related to information which would be difficult to use to identify a respondent and were framed positively. Furthermore, questions 16 to 19 were the only questions in the survey that were framed in the negative. These disparities likely lead to poor internal consistency reliability and questions 16-19 were removed. Cronbach's Alpha and the composite reliability significantly improved to 0.717 and 0.815 after this was done. The rest of the analysis improves reliability with these questions being excluded.

4.7.2 Validity

Validity was measured using convergent validity. As mentioned in the methodology, Convergent validity can be measured through the use of Average Variance Extract or AVE. AVE should be greater than 0.5 to confirm validity (Wong, 2013). Discriminant validity is another measure of validity which was used in this study. As mentioned before, this study uses Fornell and Lacker criteria to measure discriminant validity. This involves taking the square root of each AVE and comparing it to the latent variables. To meet the Fornell-Lacker criteria, the square root of each AVE must have higher values than the latent variables that are considered (Wong, 2013). Table 8 shows that the threshold for an adequate AVE is met, and

all the values are above 0.5. In the same vein, Table 9 indicates that Fornell-Lacker is met and the square root of each AVE has higher values than the latent variables.

Table 8. Results for Average Variance Extracted

	Average Variance Extracted
Behavioural Intention to Use SSI	0.729
Consequences and Benefits	0.830
Consumer Characteristics	1
Consumer Control Over Information	0.796
Past Experience With Company	0.803
Perception of Dependability	0.782
Reputation of a company	0.789
Type of Personal Information Requested	0.589
Willingness To Provide Personal Information	0.691

Table 9. Results using Fornell-Lacker Criteria

	BISSI	CB	CC	CCOI	PEWC	POD	ROC	TPIR	WTPPI
BISSI	**0.854**								
CB	0.298	**0.911**							
CC	-0.131	-0.209	**1**						
CCOI	0.004	-0.005	-0.083	**0.892**					
PEWC	0.361	0.341	-0.052	-0.037	**0.896**				
POD	0.376	0.367	-0.127	-0.045	0.591	**0.884**			
ROC	0.392	0.366	-0.234	0.006	0.594	0.772	**0.888**		
TPIR	0.358	0.327	-0.06	0.04	0.286	0.33	0.327	**0.767**	
WTPPI	0.414	0.549	-0.212	-0.127	0.514	0.547	0.575	0.418	**0.831**

Abbreviations Used
Behavioural Intention to Use SSI (BISSI)
Consequences and Benefits (CB)
Consumer Characteristics (CC)
Consumer Control Over Information (CCOI)
Past Experience With Company (PEWC)
Perception of Dependability (POD)
Reputation of a company (ROC)
Type of Personal Information Requested (TPIR)
Willingness To Provide Personal Information (WTPPI)

The sections on internal consistency reliability and validity have shown that the requirements set by Wong (2013) and Malhorta (2010) for reliability and validity have been met.

Specifically, it was shown that the measures for reliability, Composite Reliability exceeded the minimum level of 0.6. Similarly, the requirements for validity were also shown to have been exceeded. In the next section, the discussion focuses on the structural model, which considers the relevant hypotheses posed in this study.

4.7.2 Structural Model

The verification of the relationships which were hypothesised in this paper was done using the structural model. Verification of these relationships was done in two ways. Firstly, SEM or structural equation modelling was utilised. Specifically, the partial least squares software called SmartPLS was used to test the hypotheses relationships. Secondly, regression analysis was used to examine the moderating effect of the perceived value and security fatigue factors. These involved the utilisation of the macro called PROCESS which was developed by Hayes (2015). The macro PROCESS is utilised within the statistical software SPSS. This section begins with verification of hypotheses relating to the willingness to provide personal information and the behavioural intention to use SSI technology. This is followed by the confirmation or rejection of moderating effects. The important findings of the structural model is included at the end of this section.

4.7.2.1 Results for the structural model

The hypotheses were analysed and verified using the following statistics which are provided by the SmartPLS software: beta coefficient, coefficient of determination, t-values and p-values. This approach and use of these statistics to confirm the hypotheses in the structural model, was recommended by Wong (2013).

The coefficient of determination or R^2 ranges between 0 and 1. As mentioned in the methodology section, the coefficient of determination should be higher than 0.25 for marketing research (Wong, 2013). Results from SmartPLS indicate that the R^2 value is 0.534 for the relationship between the willingness to provide personal information and the perceived risk factors and trust factors. This indicates that the variation in the 7 latent variables moderately explains 53% of the variation in the willingness of a respondent to provide personal information.

The R^2 value of 0.172 for the relationship between the behavioural intention to use SSI and the willingness to provide personal information. This does not meet the minimum threshold. However, this is not necessarily problematic. Behavioural intention to use SSI only has a single predictor (the willingness to provide personal information), this means that the standardised

path coefficient or beta coefficient (0.414) is equal to the R^2 value. The lack of additional predictors, or multicollinearity affecting the model, means that for the single variable to explain the variance of the dependant variable, the effect would need to be exceptionally strong.

The t-values, along with the beta coefficients and coefficient of determination for the structural model are shown in Figure 24. The t-values can be used to either reject or accept a hypothesis. At a significance level of 0.05, and using two-tailed test, the path coefficient is significant if it is above 1.96 (Wong, 2013). The p-value is another important statistic to measure the likelihood that the null hypothesis is true, with a smaller value increasing the likelihood of rejecting the

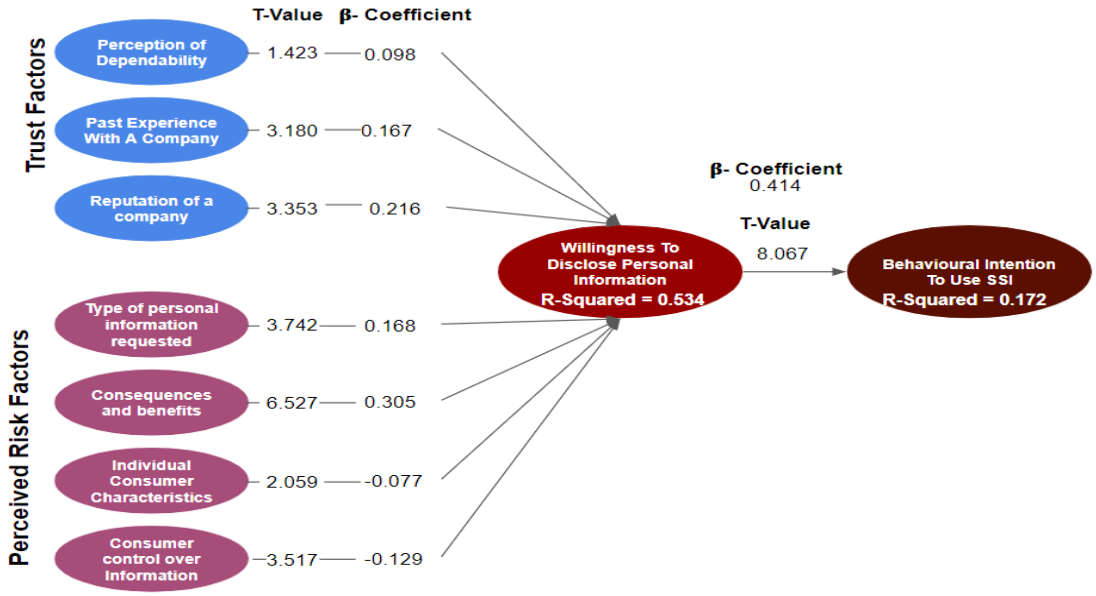

Figure 21. T-Value, Beta Coefficient and R-Squared Values, Bootstrapping Method, α=0.05, Two-Tailed Test

null hypothesis, and that the alternative hypothesis is true. In cases where the t-value is significant, the beta coefficient (β) can be used to enhance the interpretation of the results (Hirschfelder, 2015). The beta coefficient allows an interpretation of strength of the relationship between the independent/predictor variable and the dependent variable (Hirschfielder, 2015). The aforementioned statistics are summarised in Table 10, along with whether the hypothesis should be rejected or accepted. The discussion which follows uses the statistics in Table 8 to interpret the hypotheses that were suggested in this paper.

Table 10. Summary of Results from SmartPLS

Hypothesised Relationship	Beta Coefficient	T-Value	P-Value	Null Hypothesis
Trust Factors				
PEWC→WTPPI	0,167	3,18	0,001	Rejected
ROC→WTPPI	0,216	3,3353	0,001	Rejected
POD→WTPPI	0,098	1,423	0,155	Supported
Perceived Risk Factors				
TPIR→WTPPI	0,168	3,742	0	Rejected
CB→WTPPI	0,305	6,527	0	Rejected
CC→WTPPI	-0,077	2,059	0,04	Rejected
CCOI→WTPPI	-0,129	3,517	0	Rejected
SSI Interaction With WTPPI				
WTPPI→BISSI	0,414	8,067	0	Rejected

Abbreviations Used

Behavioural Intention to Use SSI (BISSI)
Consequences and Benefits (CB)
Consumer Characteristics (CC)
Consumer Control Over Information (CCOI)
Past Experience With Company (PEWC)
Perception of Dependability (POD)
Reputation of a company (ROC)
Type of Personal Information Requested (TPIR)
Willingness To Provide Personal Information (WTPPI)

Hypothesis 1A suggested a positive relationship between past experience with a company and the willingness of an online consumer to disclose personal information to a website. This relationship was supported and showed a t-value above 1.96, and the t-value was measured as 3.18 Secondly, the corresponding low p-value supported the rejection of this null hypothesis, and the acceptance of hypothesis 1A. Lastly, the beta coefficient was positive and comparatively high, showing that the relationship was strong and positive.

Hypothesis 1B suggested that there was a positive relationship between the reputation of a company and the willingness of an online consumer to disclose personal information to a website. This relationship was also supported, and the corresponding t-value measured 3.33. Again, the low p-value of 0.001 supports the acceptance of this relationship. The beta coefficient was positive and one of the highest of all the variables measured. This supports, a strong significant relationship between the willingness to disclose personal information to a website and the reputation of company. Of all the trust factors, this relationship was the most supported.

The last hypothesis, 1C, relating to the trust factors, suggested a positive relationship between perception of dependability of a company and the willingness of an online consumer to disclose personal information to a website. This relationship was not supported and the t-value measured 1.423. The p-value of 0.155 added to rejection of hypothesis 1C.

Hypothesis 2A hypothesised that a relationship exists between type of personal information requested and the willingness to provide personal information to a website. The questions which were analysed only related to information which could be characterised as non-evasive, and difficult to use to identify a respondent. For example, a respondents willing to disclose their favourite hobbies was an information type that was polled in the survey. This relationship was supported. The t-value for this relationship was 3.742 with a p-value close to zero. Comparatively, the beta coefficient indicated this relationship was a positive and relatively strong.

Hypothesis 2B, suggested a positive relationship between benefits received and willingness to provide personal information to a website. This relationship had a high relative t-value of 6.527. The beta coefficient indicated this relationship is positive, and the strongest of all the relationships that were measured.

The next hypothesis that falls within the perceived risk factors is hypothesis 2C. Hypothesis 2C proposed that younger consumers are less reluctant to disclose personal information, compared to older consumers. This hypothesis was polled with a single item, which asked a consumer their age. Younger ages were coded with lower scores. This means a negative relationship would support this hypothesis. The t-value measured for this hypothesis was measured as 2.059 and the corresponding p-value was measured as 0.004. Furthermore, the beta coefficient measured was -0.077 indicating a weak, but negative relationship. This means the hypothesis 2C is supported. However, it is notable that of all the variables that had their null hypotheses rejected, this hypothesis had the least favourable t-values and p-value.

The last hypothesis that falls within the perceived risk factors is 2D. It was hypothesised that information control would show a negative relationship with the willingness to provide personal information to a website. The hypothesis was supported because of the t-value of 3.517 and corresponding negative beta coefficient.

Lastly, it was hypothesised that the willingness to provide personal information over the internet would have a negative relationship with the behavioural intention to use SSI technology. This relationship was confirmed, and was the strongest of all the relationships

measured. The t-value was the highest of all the variables, and measured at 8.067. Comparatively, the beta value of 0.414 indicates a very strong, positive relationship between the two variables. This means that although the relationship is confirmed, it is positive and not negative, as it was predicted to be.

4.7.2.2 Moderation Model

As discussed in the section on methodology, the moderation model was analysed using SPSS and the macro PROCESS. The p-value was examined to determine whether sufficient moderation existed. The p-value showed whether moderation between the independent and dependent variables in the model. The p-value should be lower than 0.05 to confirm significant moderation, at a 95% significance level (Hirschfelder, 2015 citing Field, 2013). The specific moderation model used is indicated in Figure 25.

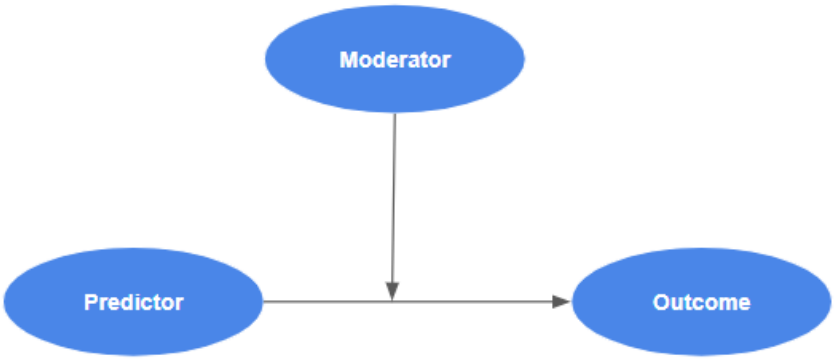

Figure 22. Moderation Model Used (adapted from Field 2013)

Using the moderation model presented in Figure 25, 17 models were tested. 7 of these models used perceived functional value as a moderator (see hypothesis 3A), and further 7 of these models used perceived relational value as a moderator (see hypothesis 3B). For these 14 models, the predictor or independent variables were the trust and perceived risk factors which were indicated in the theoretical model. For the remaining 3 models, security, functionality and usability were used as a moderator (see hypothesis 4A to 4C) and the predictor variable was the willingness to provide personal information. In this scenario the outcome variable was the behavioural intention to use SSI technology. A table indicating the results of the analysis using SPSS and the macro PROCESS are included in Table 11.

Table 11. SPSS PROCESS

Interaction Effect	Moderator	T-Value	P-Value	LLCI	ULCI	Null Hypothesis
Past Experience	Functional Value	1.247	0.213	0.149	0.520	Supported
Past Experience	Relational Value	-0.396	0.693	-0.024	0.016	Supported
Reputation Of A Company	Functional Value	1.459	0.145	-0.006	0.042	Supported
Reputation Of A Company	Relational Value	0.799	0.425	-0.013	0.031	Supported
Perception Of Dependability	Functional Value	-0.172	0.864	-0.030	0.025	Supported
Perception Of Dependability	Relational Value	-0.346	0.021	-0.030	0.021	Supported
Type of Personal Info.	Functional Value	1.114	0.266	-0.010	0.037	Supported
Type of Personal Info.	Relational Value	-0.800	0.424	-0.029	0.012	Supported
Consequences & Benefits	Functional Value	-1.551	0.122	-0.049	0.006	Supported
Consequences & Benefits	Relational Value	-0.695	0.488	-0.029	0.014	Supported
Consumer Characteristics	Functional Value	1.425	0.155	-0.029	0.179	Supported
Consumer Characteristics	Relational Value	2.642	0.009	0.032	0.219	Not Supported
Consumer Control	Functional Value	-0.142	0.887	-0.332	0.287	Supported
Consumer Control	Relational Value	-1.024	0.307	-0.111	-0.35	Supported
Willingness To Provide Personal Information	Security	1.768	0.078	-0.001	0.020	Supported
Willingness To Provide Personal Information	Functionality	0.200	0.81	-0.17	0.020	Supported
Willingness To Provide Personal Information	Usability	-0.100	0.921	-0.015	0.014	Supported

Various hypotheses in this paper suggested that perceived functional value and perceived relational value acted as a moderator between the trust factors as well as perceived risk factors and the willingness to disclose personal information to a website. The majority of these hypotheses were not supported, and had p-values greater than 0.05. This is indicative that moderation was not present, as was mentioned before.

The only hypothesis which was supported, was hypothesis 3B. This hypothesis suggested that consumer characteristics (measured by age) and its relationship with the willingness to provide personal information to a website, is moderated by perceived relational value. Furthermore, this relationship had an r-squared value of 0.193 and a b-value of 0.126. This means that a positive relationship is present and that an increase in perceived relational value leads to an increase in the impact of age on the willingness to provide personal information. It also means that age explains 19% of the variance of perceived relational value. Hypothesis 3B was examined more closely using the unstandardised coefficient (b) as well as the p-value. This is

advisable according to the work of Field (2013). Table 12 shows a deeper analysis of hypothesis 3B (VI).

Hypotheses 4A to 4C, related to the moderating effect of security fatigue factors on the relationship between the willingness to provide personal information and the behavioral intention to use SSI. None of these hypotheses were supported, as all had p-values above the threshold of 0.05.

Table 12. Deeper Analysis of H3B (VI) Taken From SPSS Results

Model	Age Value		b LLCI/ULCI	SE B	t-value	p-value
H3B (VI) Perceived relational value moderates the following relationship between individual consumer characteristics and the willingness to provide personal information	Low (-4.671)		-1.416 -2.054/-0.779	0.324	-4.369	0
	Mean Value (0)		-0.829 -1.209/-0.449	0.193	-4.291	0
	High (4.671)		-0.242 -0.756/0.272	0.261	-0.926	0.355

For H3B (VI) the results in the table can be interpreted as follows:

(1) For low perceived relational value there is a negative and highly significant relationship between age and the willingness to provide personal information to a website.
(2) For moderate perceived relational value there is a smaller but still negative significant relationship between age and the willingness to provide personal information to a website.
(3) For high perceived relational value there is the smallest negative relationship between age and the willingness to provide personal information to a website.

The above three points, were visualised with the help of SPSS and are presented in Figure 26.

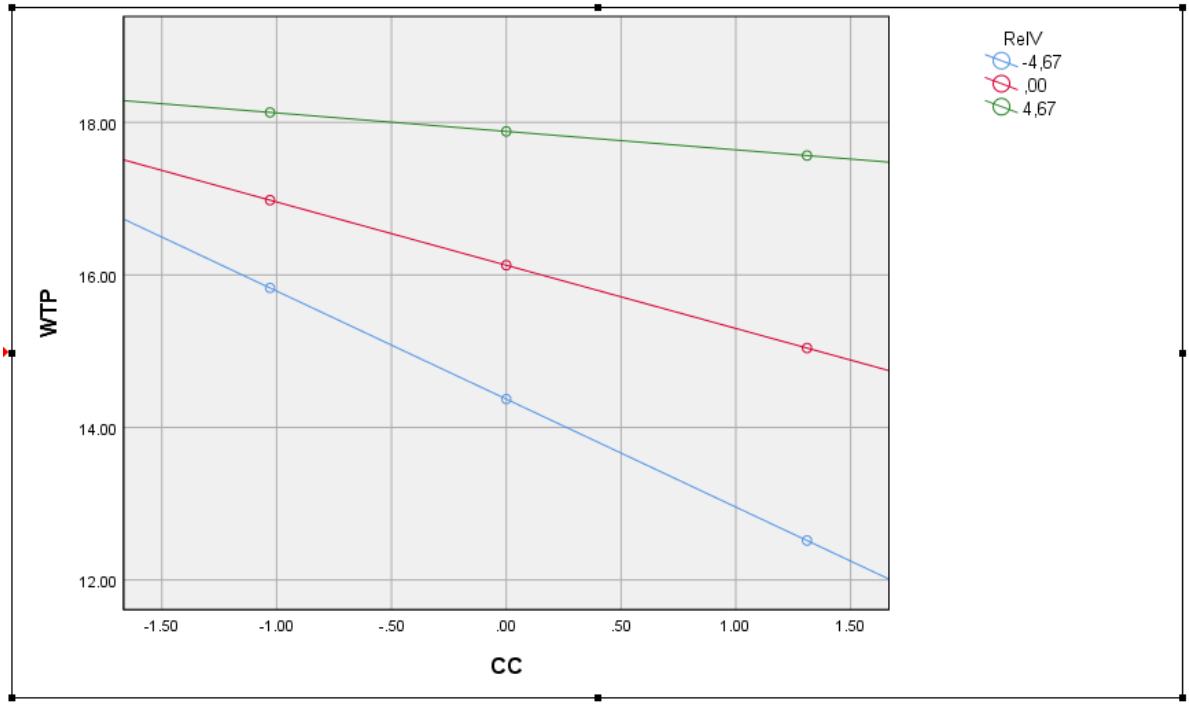

Figure 23. Visualisation of SPSS Results For H3B (VI)

4.8 Conclusion

This chapter began with the restatement of the hypotheses. What followed was a description of the fieldwork as well as the sampling utilised in this study. Using the methodology discussed in chapter 3, the results were presented. The results began with an analysis of the descriptive statistics, and ended with an analysis of the inferential statistics. This included a comment on validity and reliability of the measurement model, which was found to be robust, as well as an examination of the structural model and the relevant hypotheses. Excluding hypotheses related to the moderation model, the majority of the hypotheses suggested in this paper were supported. Notably, the hypothesised relationship between the perception of dependability and the willingness to disclose personal information was found to be not supported.

Similarly, the relationship between the use of SSI technology and the willingness to provide personal information, was found to have a strong, but positive relationship. Regarding moderation, all the hypotheses relating to the moderation models proposed for perceived value factors and security fatigue factors were not supported. The only exception was the moderating effect of perceived relational value on the relationship between consumer characteristic and the willingness of a respondent to disclose information to a website.

The next, and final chapter summarises the important results and outlines the limitations of this research. Recommendations for further research and the implications of this research for various stakeholders are also outlined in this final chapter.

CHAPTER FIVE: CONCLUSION AND RECOMMENDATION

5.1 Introduction

As mentioned before, privacy and the 'right to be let alone' more commonly known as the right to be left alone, was articulated more than 100 years ago by Warren and Brandeis (1890). Approximately 93 years later the internet was invented (Andrews, 2019). The rapid growth of the internet allowed the collection of consumer data at unparalleled speed and efficiency that was not possible before (Nam *et al.*, 2006). Arguably, this led to consumer concern in the early nineties relating to the information marketers had and the methods they used to collect this information (Nowak and Phelps, 1995). This concern may be valid as competitive forces faced by marketers have driven a greater use of technology to effectively collect and utilise personal information (Graeff & Harmon, 2002). This stems from an actual or perceived desire by consumers for personalised communication and attention (Graeff & Harmon, 2002).

Understanding the factors that drive a consumer to disclose their personal information is thus an important objective for two reasons. Firstly, for those who desire to protect consumers and their privacy, understanding what might drive a consumer to disclose personal information can inform how to protect a consumer more effectively. On the other hand, as marketers continue to depend on personal information to drive marketing performance and personalisation, understanding how they might increase the availability of a consumers personal information becomes a business imperative.

Further, this study incorporated SSI technology. SSI Technology is defined as system for identity management that permits a person to own and manage their electronic or digital identity. (Mühle *et al*., 2018). For further clarification, a digital identity can be described as digital data which relates to a person in a specific identity system (Chen, 2007). SSI technology aims to give consumers greater security, control and power over their own personal information. This technology, currently in its infancy has major implications for both marketers, and those who might want to use it to create better privacy protection for consumers. If it is adopted it may completely change the status quo of information collection and information sharing.

Chapter five aims is to interpret the findings of previous chapter and address the primary objectives of this research. The next section also provides a synopsis of the individual chapters

which were part of this research. This is followed by a discussion on the results; a reflection on the limitations of this study; and a conclusion for this chapter.

5.2 Synopsis of Research

This research aimed to explore the factors that contribute to a South African consumer's willingness to disclose personal information to a website. The willingness of an online consumer to disclose personal information is a fairly well researched area of academic research. However, there is limited research which is focused on a South African context and consumer.

Hoping to add a unique contribution, this study proposed a relationship between the willingness of an online consumer to disclose personal information and the behavioural intention to use SSI technology. Owing to its novelty, SSI has received little to no academic attention.

In the theoretical model proposed in this paper, perceived risk and trust factors were hypothesised to be influential factors that affected a consumer's willingness to disclose personal information. These factors were based on the work of Schoenbachler and Gordon (2002) and Phelps, Nowak and Ferrell (2000). Adding to this, a moderator of this relationship was proposed in the form of perceived value. This was inspired by work of Tai (2011) and his understanding of perceived value.

Focusing on the willingness to provide personal information, this research aimed to shed light on the relationship between the willingness to provide personal information to a website, and the behavioural intention to use SSI technology. A moderator was introduced for this relationship, in the form of security fatigue. This was based on the security triangle proposed in the work of Waite (2010).

Chapter Two provided the reader with insight into existing literature which was organised logically according to the theoretical model mentioned above. The work of Schoenbachler and Gordon (2002); Phelps, Nowak and Ferrel (2000); Tai (2011) and Waite (2010) are discussed in detail in this chapter. Other authors' work is also referenced and discussed to the extent that it relates to one of the 15 variables included as a part of this study. This work either supported, or sheds light on other perspectives of these variables and their relationship to a willingness to provide personal information. Existing research on SSI is described in this chapter which makes the reader aware of the limited research in the area and the need for further research. The section on SSI aimed to give a reader a conceptual understanding and some knowledge of

the history of the development of both SSI as the evolution of a digital identity, and its application into a feasible technology using the blockchain.

Chapter Three extensively outlines the methodology followed for this study. This is based on the work of Birks and Malhorta (2006) and their understanding of an effective market research process. In this chapter the creation, distribution, and testing of the survey used to collect data, is described. This survey utilised a 7-point Likert-Type scale and was created and distributed online to adult South African citizens as the intended target population. There is considerable coverage of the statistical approach used to analyse the data. PLS-SEM, guided by the work of Wong (2013), is used to analyse the measurement and structural models which are described in this chapter. The use of PLS-SEM is. The use of the macro, PROCESS and SPSS to test the moderation models are also described.

Following a detailed description of the methodology, Chapter 4 applies this methodology to the 347 usable responses that were collected in the online survey. Descriptive results are analysed as well as inferential results. Specifically, the measurement model is examined comprehensively for validity and reliability, and this is followed by an analysis of the structural model and the relevant hypotheses. The moderation model is the last aspect which is analysed. Linked to this, SPSS and the results derived from it using PROCESS are shared and discussed with the reader. Briefly, the results in Chapter 4 show that only one relationship was not supported by the results - the relationship between the perception of dependability and the willingness to disclose personal information over the internet. The hypothesised relationship between the willingness to provide personal information and the behavioural intention to use SSI was supported, but it was found to be a positive rather than a negative relationship. Perceived relational value's moderating effect on the relationship between consumer characteristics and willingness to provide personal information to a website was found to be supported by the data analysis. This was the only moderating relationship which was supported after the analysis of the data using the macro PROCESS and SPSS.

Now that a synopsis of each chapter has been provided, the next section discusses the findings of this research and comments on their implications. These implications apply to marketers and stakeholders such as privacy regulators who may have an interest in protecting the privacy of consumers.

5.3 Summary of Findings and Managerial Implications

Before the findings are discussed, the primary objective, theoretical model and relevant hypotheses are restated. The reason for this is because the findings are logically organised under four headings which relate to theoretical model: *perceived risk factors*, *trust factors*, *moderating factors*, and *information disclosure and SSI Technology.*

Primary Objective:

1. To determine the factors which affect a South African consumer's willingness to provide personal information over the internet to a website.

Secondary Objective:

2. To determine the relationship between the willingness to provide personal information on the internet and the use of Self-Sovereign Identity Technology, in South Africa.

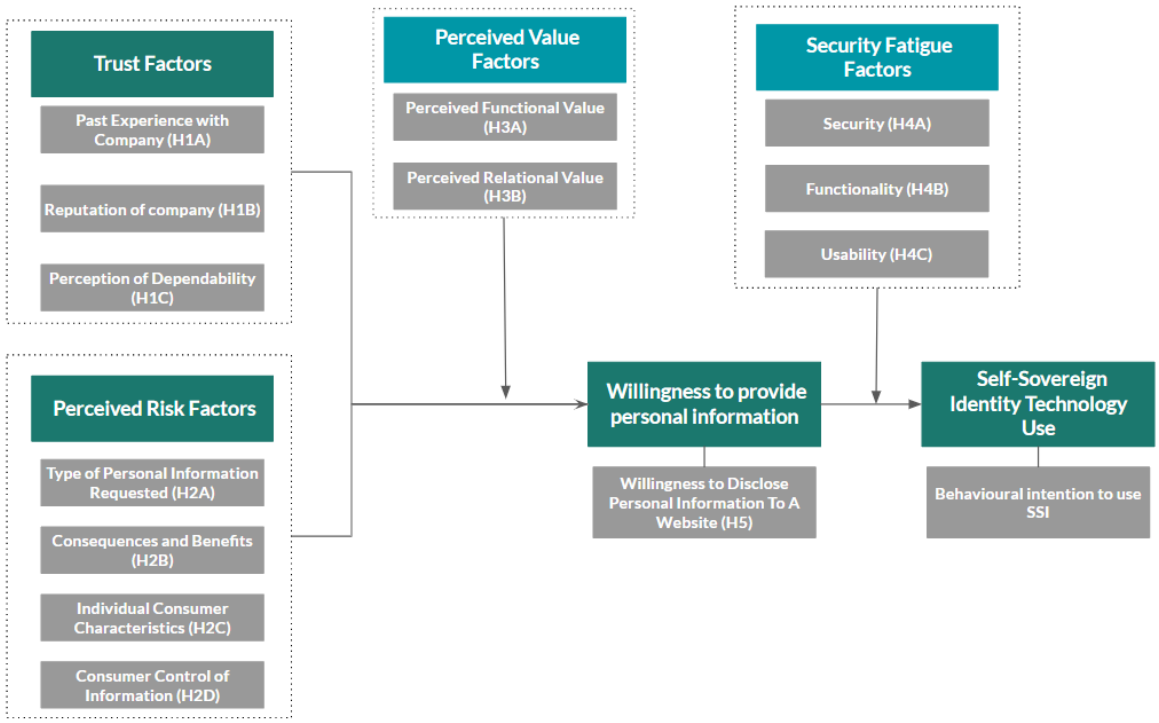

Figure 24. Combined Theoretical Model Proposed In This Paper

Hypothesis 1A:

There is a positive relationship between past experience with a company and the willingness of an online consumer to disclose personal information to a website.

Hypothesis 1B:

There is a positive relationship between the reputation of a company and the willingness of an online consumer to disclose personal information to a website.

Hypothesis 1C:

There is a positive relationship between perception of dependability of a company and the willingness of an online consumer to disclose personal information to a website.

Hypothesis 2A:

There is a positive relationship between the type of personal information requested and the willingness of an online consumer to provide personal information to a website.

Hypothesis 2B:

There is a positive relationship between benefits received and willingness of an online consumer to provide personal information to a website.

Hypothesis 2C:

A younger age has a positive relationship with the willingness of an online consumer to provide personal information to a website.

Hypothesis 2D:

Information control has a negative relationship with the willingness of an online consumer to provide personal information to a website.

Hypothesis 3A:

Perceived functional value moderates the relationship between:

i. Past experience with a company and the willingness of an online consumer to provide personal information on a website.
ii. Reputation of a company and the willingness of an online consumer to provide personal information on a website.
iii. Perception of dependability and the willingness of an online consumer to provide personal information on a website.
iv. Type of personal information requested and the willingness of an online consumer to provide personal information on a website.
v. Benefits received and the willingness of an online consumer to provide personal information on a website.

vi. Individual consumer characteristics and the willingness of an online consumer to provide personal information on a website.
vii. Consumer control over information and the willingness of an online consumer to provide personal information on a website.

Hypothesis 3B:

Perceived relational value moderates the relationship between:

i. Past experience with a company and the willingness of an online consumer to provide personal information on a website.
ii. Reputation of a company and the willingness of an online consumer to provide personal information on a website.
iii. Perception of dependability and the willingness of an online consumer to provide personal information on a website.
iv. Type of personal information requested and the willingness of an online consumer to provide personal information on a website.
v. Benefits received and the willingness of an online consumer to provide personal information on a website.
vi. Individual consumer characteristics and the willingness of an online consumer to provide personal information on a website.
vii. Consumer control over information and the willingness of an online consumer to provide personal information on a website.

Hypothesis 4A:

Security moderates the relationship between the behavioural intention to use SSI technology and the willingness of an online consumer to provide personal information.

Hypothesis 4B:

Functionality moderates the relationship between the behavioural intention to use SSI technology and the willingness of an online consumer to provide personal information

Hypothesis 4C:

Usability moderates the relationship between the behavioural intention to use SSI technology and the willingness of an online consumer to provide personal information

Hypothesis 5:

The willingness to provide personal information over the internet has a negative relationship with the behavioural intention to use SSI technology

5.3.1 Trust Factors

As can be seen in Figure 26, three trust factors were measured*: past experience with a company* (H1A), *reputation of a company* (H1B) and *perception of dependability* (H1C). The data analysis revealed that H1A and H1B were supported. Conversely, H1C was not supported. This related to the proposed relationship between the perception of dependability and a consumer's willingness to provide personal information.

Support for the proposed positive relationship proposed in hypothesis 1A and 1B, somewhat supports the earlier work of Schoenbachler and Gordon (2002) on past experience and the willingness of consumers to disclose personal information. Schoenbachler and Gordon (2002) found that past experience and reputation had a positive relationship with trust, and trust influenced the willingness of a consumer to disclose personal information. Additionally, findings for hypothesis 1A supports the work of Milne and Boza (1999). In the qualitative part of a study by Milne and Boza (1999), they found that the key reason which influenced why respondents trusted a company with their personal information, was the respondents' past experience with the company.

The relationship between perception and dependability and the willingness to disclose personal information was not supported. This finding is somewhat supported by the work of Moorman, Desphande and Zaltman (1993) who found that dependability was unrelated to trust. If dependability is unrelated to trust, it may be unable to indirectly affect the information disclosure intentions through a trust mechanism. Compared to past experience, reputation showed a stronger positive relationship with the willingness for a consumer to disclose personal information. This may suggest that consumers consider both their most recent experience with a website, as well as their overall experience and perception of the website when they asses their willingness to disclose personal information.

The questions polled for past experience did not refer to a positive 'privacy experience' but focused on a website meeting expectations, as well as feelings of happiness and positivity when a consumer recalls their past experience. Creating a feeling of happiness and positivity towards

a past experience may mean that improving factors such as customer service quality, could have an effect on increasing the disclosure intentions of a consumer. Long-term, this may also increase information disclosure intentions of a consumer via the creation of a more positive reputation.

Moreover, support for hypothesis 1A and 1B has implications for new businesses which have not yet had time to build or invest in building a positive reputation, and have yet to acquire customers who can easily recall positive past experiences. It is recommended that these businesses ask for the minimal amount of personal information possible, especially if it is required to engage or transact with the business. Regulators should be cognisant that a consumer may be less reluctant to disclose personal information to websites which create positive past experiences, and have a good reputation. This reputation may be created through high levels of service quality or other factors which are not related to ethical information practices. Related to this, regulators should be wary of bigger businesses with sufficient capital to inflate their reputation through marketing spend and who rely on personal information to drive their business models. These businesses may require closer regulatory scrutiny, as consumers may readily share information with these businesses.

5.3.2 Perceived Risk Factors

The perceived risk factors are related to hypotheses 2A to 2D. Specifically, the perceived risk factors are: *type of personal information requested*; *consequences and benefits*; *individual consumer characteristics*; and *consumer control over information*. Hypotheses 2A to 2D which relate to these variables were supported in the data analysis. The implications of these hypotheses are discussed below.

Consumers who were more willing to disclose non-sensitive information types to a website, were also more willing to disclose generally personal information. Non-sensitive information in this context is defined as information which cannot easily be used to identify an individual. The survey polled and analysed questions on the disclosure intentions of consumers for non-invasive information such as *favourite hobbies*, *highest qualification* and *age*.

Gupta, Iyer and Weisskirch (2009) analysed willingness to share personal information online. The authors measured geographical discrepancies of consumers in India as well as the, US to share different categories of data. It was found that consumers in both countries were less willing to disclose date of birth, home and work addresses as well as phone numbers, credit card details, medical history and financial history. This supports the findings of Phelps, Nowak

and Ferrel (2000) where consumers were more reluctant to disclose financial information, and less reluctant to disclose lifestyle and demographic information. South African consumers were polled questions that indicated their willingness to disclose lifestyle, financial and demographic information. The findings of this study are in agreement with Gupta, Iyer and Weisskirch (2009) and Phelps, Nowak and Ferrel (2000). Consumers showed more reluctance to disclose financial information, and information that could be used to directly identify them (Cellphone number and biometric information) and less reluctance to disclose lifestyle information like their favourite hobbies and television programmes.

Hypothesis 2B was supported in the data analysis. This hypothesis suggested a positive relationship between benefits received for disclosing information, and the willingness of a consumer to disclose information. The questions polled incorporated benefits relating to: *monetary rewards*; *savings;* and *free goods and services*. This suggests that consumers who are willing to exchange personal information for a reward, are more likely to generally disclose their personal information.

Phelps, Nowak and Ferrel (2000) as well as Ward, Bridges and Chitty (2005) found that benefits do not have an influence on consumer concerns relating to information disclosure. With these findings in-mind, it can be postulated that benefits do not reduce concern but function to offset the loss experienced by consumers. This is in line with the 'privacy calculus' perspective of Li, Sarathy and Xu (2010). This 'privacy calculus' is a cost-benefit trade-off that consumers experience when facing a decision to disclose personal information. Consumers who value benefits, and are more cognisant of the benefits received in return for information, may be more aware of these benefits generally, leading to a higher general intention to disclose personal information. These consumers may require additional protection from regulators, as benefits offered by companies could be used to influence their intention to disclose personal information to their detriment.

Hypothesis 2C was supported and proposed that younger consumers are more willing to disclose personal information than their older counterparts. The effect of age on privacy concern is not settled in the literature, with several authors finding different results (Hoofnagle *et al*., 2000; Lee, Wong and Chang, 2016; Zukowski and Brown, 2007).

Jordaan (2007) found that age influenced privacy concerns in South African consumers. Together, with the validation of Hypothesis 2C, this suggests a younger age may lead to less privacy concern and a corresponding increased intention to disclose personal information. A

possible reason for this may be that younger individuals are desensitised to privacy as they were born in an era where eCommerce and information disclosure is a typical part of participating in social media and the internet. For regulators, this means that younger individuals require specific consideration for privacy protection initiatives. Note that minors were not of interest to this study, so this conclusion cannot be extended to individuals younger than 18 years old.

Similar to the other hypotheses, hypothesis 2D was supported. This hypothesis suggested a negative relationship between information control and the willingness of a consumer to share personal information with a website. Practically, this means that consumers who highly value information control are less willing to share their personal information to websites. This makes intrinsic sense as a consumer who desires more information control, will not easily forgo control through the sharing of their personal information. This adds to the findings of Milne and Boza (1999) as well as Phleps, Nowak and Ferrel (2000) who found that perceived control decreased privacy concern. The confirmation of hypothesis 2D makes the 'control paradox' found by Brandimarte, Acquisiti and Loewenstein (2013) concerning for regulators. The 'control paradox' suggests that if the willingness to share personal information increases enough due to perceived control, a consumer will disclose information that leaves them at a greater risk. As discussed by these authors, this 'control paradox' is created because consumers place too much value on the control over and above the *release* of their information and the risk this represents. Equal or greater risk relates to *access and usage* of this personal information by other parties once the information has been *released.* This can lead to increased perceived control over the release of information leading to a greater risk for consumers, as they underestimate the risk posed by *access and usage*.

5.3.3 Information Disclosure and SSI Technology

Hypothesis 5 suggested that a negative relationship existed between the willingness to disclose personal information and the behavioural intention to use SSI technology. This relationship was confirmed, and was found to be the strongest of the relationships that were tested. However, the relationship was found to be positive and not negative.

Originally, it was hypothesised that consumers who were more willing to disclose personal information to a website, would not value or use a technology intended to protect their personal information and give them more control. However, this was not the case, and consumers who

were more willing to disclose their personal information showed a similarly high behavioural intention to use SSI technology.

This has two major implications. It may mean that consumers who self-evaluate their own willingness to disclose personal information as high, are more likely to use SSI technology, which is a technology aimed at protecting privacy. One reason for this may be that consumers want to minimise the risk they understand is present when they frequently disclose personal information to websites. On the other hand, consumers who self-evaluate their willingness to disclose personal information as low, show less willingness to use SSI technology. This makes some intrinsic sense as a consumer who infrequently discloses information has no need for a technology that would protect them from harms associated with information disclosure. However, some researchers have observed a privacy paradox where actual disclosure differs from what consumers perceived to be their willingness to disclose personal information (see Norberg, Horne & Horne, 2007; Sayre & Horne, 2000). Assuming that a privacy paradox exists, a consumer would misjudge their need for SSI technology and forgo protection they may actually need. If regulators choose to promote SSI technology as a privacy protection mechanism, they should be aware of the impact this privacy paradox may have on a consumer's intention to use the technology.

5.3.4 Moderators: Perceived Value Factors and Security Fatigue Factors

One hypothesis related to moderation was found to be valid in the data analysis. This was hypothesis 3B (VI). This hypothesis suggested that consumer characteristics (measured by age) and its relationship with the willingness to provide personal information to a website, is moderated by perceived relational value. Perceived relational value was defined in this paper as a belief that a relationship built with a provider of a good or service, will have benefits in the future (Tai, 2011)

The results showed that a positive relationship is present and that an increase in perceived relational value leads to an increase in the impact of age on the willingness to provide personal information. It has already been discussed that age has a negative relationship with the willingness to disclose personal information to a website. This effect is increased when perceived relational value is present. Adding to this, it may mean that younger adults regard relationships with eCommerce websites as influential and likely to cause them to increase their information disclosure intentions. Regulators should be aware of this, as sound information

management practices may be unrelated to the relational value that younger consumers perceive.

5.4 Addressing the Research Objectives

The primary objectives of this research were to:

1. To determine the factors that affect a South African consumer's willingness to provide personal information online.
2. To determine the relationship between a South African consumer's willingness to provide personal information online and their willingness to use SSI technology.

This study comprehensively met both of these primary objectives. Regarding the first objective, several factors were found to affect a South African consumer's willingness to provide personal information online. Based on the prior work of Schoenbachler and Gordon (2010) and Phelps, Nowak and Ferrel (2000) several perceived risk factors and trust factors were hypothesised to affect this willingness to provide personal information. The trust factors included: *past experience with a company, reputation of a company* and *perception of dependability*. The perceived risk factors included: *type of personal information requested, consequences and benefits, individual consumer characteristics* and *consumer control over information*. All of these factors were found to be significant except for the perception of dependability, which was not supported. Furthermore, perceived functional value was found to moderate the relationship between individual consumer characteristics and the willingness to provide personal information. The other relationships were not found to be moderated by perceived functional value or perceived relational value. Overall, this contextualised research on privacy in a South African context shed light on some of the factors which influence an adult South African consumer's willingness to share personal information, in an online setting.

Regarding the 2nd objective, a relationship was found to exist between the willingness to provide personal information online and the willingness to use SSI technology. This relationship was found to be strong, and negative. As mentioned before, this broadly adds to the under-researched area of SSI technology. It also adds to research focused on willingness of consumers to share information online, and provides evidence of a new relationship. To this author's knowledge, the relationship has not been suggested before and is therefore novel.

This study combined the theoretical frameworks of multiple authors in a novel way to build a comprehensive theoretical model to understand the willingness of an online consumer to share personal information. Furthermore, the combined theoretical framework helped to shed light

on the relationship of sharing personal information in an online environment with the usage of SSI technology. This theoretical framework adds to the existing literature on measuring a consumer's willingness to share personal information. Further, it provides a basis for further investigation into the relationship of personal information disclosure with the usage of SSI technology. As mentioned before, this is a novel extension of theoretical models proposed to measure the sharing of personal information.

5.5 Limitations of This Research

This section outlines limitations that impacted the findings mentioned in this study; and impacted the ability to meet the research objectives; as well as verify the related hypotheses.

As mentioned, age was a limiting factor. Respondents below the age of 18 were excluded and this had implications for the study. Attention should specifically be drawn to the conclusions on age and its relationship with the willingness to provide personal information. Similarly, this study was limited to consumers residing in, or having resided in South Africa. This geographical limitation should not be underestimated. Certain factors which affect a consumer's willingness to share personal information have already been found to differ geographically. As mentioned in the literature review, the work of Gupta, Iyer and Weisskirch (2009) found geographical differences in the willingness of consumers to share different types of personal information in India as compared to the US.

Another limitation was that this study used non-probability sampling. Convenience sampling was used, which is a form of non-probability sampling. This means that procurement of sampling units is based on what is most easily available to the researcher. This makes it difficult to make generalisations on the population. The relatively large sample size of 347, does still allow for meaningful conclusions on the dataset. Furthermore, limitations may result from the collection of data via an online survey. For example, there may be fraudulent respondents and also internet populations may not mirror the population of the country: these are some considerations to take into account when conducting a study using an online survey (Ilieva *et al*., 2002; Lefever, Dal and Matthiasdottir, 2007).

The focus of this research was on SSI technology. This means that the findings relate to SSI technology specifically, and do not relate to other technologies that may enable greater privacy protection. Furthermore, the understanding of SSI technology given to respondents was conceptual and based on the explanation of SSI technology provided in a video by the Sovrin Foundation. This may further limit the applicability of the findings to realistic implementations

of SSI technologies. The conceptual understanding of SSI technology in literature and may depart from the explanation given by the Sovrin foundation.

Lastly, the findings on the willingness to provide personal information are focused on an online environment, and the disclosure intentions to an online website, specifically. This means that these findings may have limited applicability to offline settings. Specifically, consumers who do not interact online may have difference preferences, behaviours and attitudes compared to their offline counterparts because of their usage of the internet may differ. This means this research is applicable to South African consumers who use the internet only, and should not be generalised and applied to offline South African consumers. This study limited applicability to the disclosure intentions of consumers in online environments that are not on websites, such as on online surveys.

5.6 Future Research

This study shed light on the factors that may affect a consumer's willingness to share personal information online. The willingness of consumers to share personal information online can be described as a globally well-researched area that is growing in interest to researchers. However, more research is needed that focuses on a South African setting. This is essential to guide policy decisions, and choices regarding privacy. As mentioned before, some researchers have found evidence of a privacy paradox, and a misalignment between intended behaviour and actual behaviour (see Norberg, Horne and Horne, 2007). Further research is required to understand the existence of this privacy paradox in a South African context. If the existence of a privacy paradox is proven, it will have an influential impact on research that follows in this area.

Furthermore, additional research exploring SSI technology is needed. SSI technology is a new technology that may allow consumers to have unparalleled privacy protection. If this technology is adopted successfully by consumers, it will have a profound effect on how business collect data, and how consumers share their data. In many ways it could completely change the status quo of data collection, data sharing and control. Understanding the potential and limitations of this technology, for marketers as well as regulators, will become more critical as the technology is refined and adoption of the technology increases. This will require extensive research as current research is severely limited and mainly focused on the technical aspects of the technology.

5.7 Conclusion

Chapter Five presented and discussed the findings of this research, and the extent to which the research met the objectives of this study. Several factors were found to have a significant impact on the willingness of a consumer to disclose information over the internet, and as a whole, the theoretical model successfully predicated many of the proposed relationships. Most notably, the theoretical model successfully showed that the following variables had a relationship with the willingness to provide personal information: *past experience with a company*; *reputation of a company; type of personal information requested*; *benefits offered; consumer characteristics* and *consumer control over personal information*. Adding to this, *perceived value* was shown to moderate the relationship between consumer characteristics and the willingness to provide personal information. This adds a significant contribution to the understanding of which variables affect an adult South African's decision to share personal information with a website, in an online setting.

Equally importantly, a strong, negative relationship was found between the willingness of a consumer to share personal information and the behavioural intent to use SSI technology. To the authors knowledge this is an original and significant contribution to the understanding of SSI technology and its relationship with the information disclosure intentions of consumers.

The importance of these findings for regulators and marketers were also discussed as well as the importance of further research in this area. As mentioned before, further research in this area is critical for both marketers who may find their information collection practices disrupted by SSI technology, and also regulators who seek to safeguard the privacy of consumers.

The 'right to be let alone' more commonly known as the right to be left alone, was articulated more than 100 years ago by Brandeis and Warren (1890). More than 100 years later, its importance should not be underestimated as technologies begin to allow the realisation of this right to become almost permanent reality.

Reference List

Acquisti, A., John, L.K. and Loewenstein, G., 2013. What is privacy worth? *The Journal of Legal Studies*, *42*(2), pp.249-274.

Al-Fedaghi, S. and Al-Azmi, A.A.R., 2012. Experimentation with personal identifiable information. *Intelligent Information Management*, *4*(04), p.123.

Alboaie, S. and Cosovan, D., 2017, June. Private data system enabling self-sovereign storage managed by executable choreographies. In *IFIP International Conference on Distributed Applications and Interoperable Systems* (pp. 83-98). Springer, Cham.

Allen, C. 2016. *The Path to Self-Sovereign Identity*. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (2019/06/17).

Bada, M., Sasse, A.M. and Nurse, J.R., 2019. Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.

Bagozzi, R.P. and Yi, Y., 1988. On the evaluation of structural equation models. *Journal of the academy of marketing science*, *16*(1), pp.74-94.

Bakre, A., Patil, N. and Gupta, S., 2017. Implementing decentralized digital identity using blockchain. *International Journal of Engineering Technology Science and Research*, *4*(10), pp.379-385.

Bansal, G. and Gefen, D., 2010. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision support systems*, *49*(2), pp.138-150.

Baron, R.M. and Kenny, D.A., 1986. The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of personality and social psychology*, *51*(6), p.1173.

Bart, Y., Shankar, V., Sultan, F. and Urban, G.L., 2005. Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. J*ournal of marketing, 69(*4), pp.133-152.

Bass, L. and John, B.E., 2003. Linking usability to software architecture patterns through general scenarios. *Journal of Systems and Software, 66*(3), pp.187-197.

Bazerman, M. H. 1994. Judgment in managerial decision making. New York: Wiley.

Bellman, S., Johnson, E.J., Kobrin, S.J. and Lohse, G.L., 2004. International differences in information privacy concerns: A global survey of consumers. *The Information Society, 2*0(5), pp.313-324.

Bernardo, M., Marimon, F. and del Mar Alonso-Almeida, M., 2012. Functional quality and hedonic quality: A study of the dimensions of e-service quality in online travel agencies. Information & Management, 49(7-8), pp.342-347.

Birks, D.F. and Malhotra, N.K., 2006. *Marketing Research: an applied approach*. Pearson Education UK.

Black, E 2019. *How Facebook makes money by targeting ads directly to you*. Available: https://www.cnbc.com/2019/04/02/how-facebook-instagram-whatsapp-and-messenger-make-money.html (19/01/2020).

Blank, G., Bolsover, G. and Dubois, E., 2014, August. A new privacy paradox: Young people and privacy on social network sites. In *Prepared for the Annual Meeting of the American Sociological Association (*Vol. 17).

Blockchain Bundesverband. 2018. *Self-sovereign Identity - A position dissertation on blockchain enabled identity and the road ahead.* Available: https://www.bundesblock.de/wp-content/uploads/2018/10/ssi-dissertation.pdf (2019/06/17)

Brandimarte, L., Acquisti, A. and Loewenstein, G., 2013. Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), pp.340-347.

Brandeis, L. and Warren, S., 1890. The right to privacy. *Harvard law review, 4*(5), pp.193-220.

Calisir, F., Elvan Bayraktaroğlu, A., Altin Gumussoy, C., İlker Topcu, Y. and Mutlu, T., 2010. The relative importance of usability and functionality factors for online auction and shopping web sites. *Online Information Review, 34*(3), pp.420-439.

Cameron, K., 2008. A User-Centric Identity Metasystem. Microsoft Corp.

Casaló, L.V., Flavián, C. and Guinalíu, M., 2007. The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review, 31*(5), pp.583-603.

Chen, Y.H., Chien, S.H., Wu, J.J. and Tsai, P.Y., 2010. Impact of signals and experience on trust and trusting behavior. *Cyberpsychology, Behavior, and Social Networking, 1*3(5), pp.539-546.

Chen, Z., 2007, May. A scenario for identity management in Daidalos. In *Fifth Annual Conference on Communication Networks and Services Research (CNSR'07)* (pp. 176-183). IEEE.

Chiu, C.M., Hsu, M.H. and Wang, E.T., 2006. Understanding knowledge sharing in virtual communities: An integration of social capital and social cognitive theories. *Decision support systems, 42(*3), pp.1872-1888.

Choi, H., Park, J. and Jung, Y., 2018. The role of privacy fatigue in online privacy behaviour. *Computers in Human Behaviour, 81*, pp.42-51.

Coopamootoo, K.P., Groß, T. and Pratama, M.F.R., 2017. An Empirical Investigation of Security Fatigue: The Case of Password Choice after Solving a {CAPTCHA}. In *The {LASER} Workshop: Learning from Authoritative Security Experiment Results ({LASER} 2017)* (pp. 39-48).

Crain, M., 2018. The limits of transparency: Data brokers and commodification. *New Media & Society, 20*(1), pp.88-104.

Cropanzano, R., Rupp, D.E. and Byrne, Z.S., 2003. The relationship of emotional exhaustion to work attitudes, job performance, and organisational citizenship behaviours. J*ournal of Applied psychology, 88(*1), p.160.

Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V., 2016. Blockchain technology: Beyond bitcoin. *Applied Innovation, 2*(6-10), p.71.

Culnan, M.J. and Armstrong, P.K., 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organisation science, 10*(1), pp.104-115.

Culnan, M.J. and Bies, R.J., 2003. Consumer privacy: Balancing economic and justice considerations. *Journal of social issues, 59*(2), pp.323-342.

Curran, D. 2018. *Are you ready? Here is all the data Facebook and Google have on you*. Available: https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy (07/08/2019)

Diebold, Z., 2017. Self-Sovereign Identity using Smart Contracts on the Ethereum Blockchain (Doctoral dissertation, Dissertation, University of Dublin, Trinity College).

Doney, P.M. and Cannon, J.P., 1997. An examination of the nature of trust in buyer–seller relationships. *Journal of marketing*, *61*(2), pp.35-51.

Dunphy, P. and Petitcolas, F.A., 2018. A first look at identity management schemes on the blockchain. *IEEE Security & Privacy*, *16*(4), pp.20-29.

Eastlick, M.A., Lotz, S.L. and Warrington, P., 2006. Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research, 59(*8), pp.877-886.

European Commission (n.d.) *What personal data is considered sensitive?* Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en (07/08/2019).

Fishbein, M. and Ajzen, I., 1980. Understanding attitudes and predicting social behavior.

Fisher, J., Burstein, F., Lynch, K. and Lazarenko, K., 2008. "Usability+ usefulness= trust": an exploratory study of Australian health web sites. *Internet Research, 1*8(5), pp.477-498.

Fornell, C., & Larcker, D.F., 1981. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research,* 18 (1), 39-50.

Foxman, E.R. and Kilcoyne, P., 1993. Information technology, marketing practice, and consumer privacy: Ethical issues. *Journal of Public Policy & Marketing*, *12*(1), pp.106-119.

Fung, R. and Lee, M., 1999. EC-trust (trust in electronic commerce): exploring the antecedent factors. *AMCIS 1999 Proceedings*, p.179.

Furnell, S. and Thomson, K.L., 2009. Recognising and addressing 'security fatigue'. C*omputer Fraud & Security*, *2009*(11), pp.7-11.

Furnell, S., 2010. Usability versus complexity–striking the balance in end-user security. *Network Security, 2010*(12), pp.13-17.

Ganesan, S. and Hess, R., 1997. Dimensions and levels of trust: implications for commitment to a relationship. *Marketing letters, 8*(4), pp.439-448.

Giffin, K. 1967. The contribution of studies of source credibility to a theory of interpersonal trust in the communication department. *Psychological Bulletin, 68:* 104-120

Goodwin, N.C., 1987. Functionality and usability. *Communications of the ACM, 30*(3), pp.229-234.

Graeff, T.R. and Harmon, S., 2002. Collecting and using personal data: consumers' awareness and concerns. *Journal of consumer marketing*.

Gupta, B., Iyer, L.S. and Weisskirch, R.S., 2009. Willingness to Disclose Personal Information Online and its Effect on Ensuring and Protecting Privacy: A Two Country Study. *AMCIS 2009 Proceedings*, p.172.

Ha, H.Y., 2004. Factors influencing consumer perceptions of brand trust online. *Journal of product & brand management, 13*(5), pp.329-342.

Hair, J. F., Hult, G. T. M. and Ringle, C. M. and Sarstedt, M. 2013. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). London: Sage.

Hayes, A. F. 2015. PROCESS. [Online]. Available from: http://www.processmacro.org [Accessed: 22 March 2020].

Henseler, J. and Sarstedt, M., 2013. Goodness-of-fit indices for partial least squares path modeling. *Computational Statistics*, *28*(2), pp.565-580.

Hoadley, C.M., Xu, H., Lee, J.J. and Rosson, M.B., 2010. Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic commerce research and applications, 9*(1), pp.50-60

Hirschfelder, B., 2015. *Effects of content marketing on attitude formation in the South African energy drink market* (Doctoral dissertation, University of Cape Town).

Hoffman, D.L., Novak, T.P. and Peralta, M., 1999. Building consumer trust online. *Communications of the ACM, 42*(4), pp.80-85.

Hon, L.C. and Grunig, J.E., 1999. Guidelines for measuring relationships in public relations.

Hoofnagle, C.J., King, J., Li, S. and Turow, J., 2010. How different are young adults from older adults when it comes to information privacy attitudes and policies? Available at SSRN 1589864.

Hox, J.J. and Bechger, T.M., 1998. An introduction to structural equation modelling.

INFOSEC. 2018. *CIA triad.* Accessed at https://resources.infosecinstitute.com/cia-triad/#gref (2019/09/11)

Irwin, L. 2019. *GDPR: How the definition of personal data has changed*. Retrieved from https://www.itgovernance.co.uk/blog/gdpr-how-the-definition-of-personal-data-will-change (07/08/2019).

Jacobovitz, O., 2016. Blockchain for identity management. *The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva, Israel.*

Jarvenpaa, S.L., Tractinsky, N. and Saarinen, L., 1999. Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication, 5*(2), p.JCMC526.

Jiang, P., Jones, D.B. and Javie, S., 2008. How third-party certification programs relate to consumer trust in online transactions: An exploratory study. *Psychology & Marketing, 25(*9), pp.839-858.

Jordaan, Y., 2007. Information privacy concerns of different South African socio-demographic groups. *Southern African Business Review, 11*(2), pp.19-38.

Kahneman, D and Tversky A., 1979. 'Prospect Theory: An Analysis of Decision under Risk,' *Econometrica, 47* (2), 263-291.

Katsabas, D., Furnell, S.M. and Dowland, P.S., 2005. Using human computer interaction principles to promote usable security. In *Proceedings of the Fifth International Network Conference (INC 2005), Samos, Greece* (pp. 235-242).

Keith, M.J., Maynes, C., Lowry, P.B. and Babb, J., 2014, December. Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. In *International Conference on Information Systems (ICIS 2014), Auckland, New Zealand, December* (pp. 14-17).

Korhan, O. and Ersoy, M., 2016. Usability and functionality factors of the social network site application users from the perspective of uses and gratification theory. *Quality & Quantity, 50*(4), pp.1799-1816.

Krishnamurthy, B. and Wills, C.E., 2009, August. On the leakage of personally identifiable information via online social networks. In *Proceedings of the 2nd ACM workshop on Online social networks* (pp. 7-12). ACM.

Kröger, J. B., Meyer, I. and Hirschfelder, B. 2019. A win-win-win solution: The potential benefits of blockchain technology in digital advertising for users, marketers and society. (unpublished).

Kwon, J. and Johnson, M.E., 2015, June. The Market Effect of Healthcare Security: Do Patients Care about Data Breaches? In *WEIS*.

Lee, H., Wong, S.F. and Chang, Y., 2016. Confirming the effect of demographic characteristics on information privacy concerns.

Leon, P.G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., Bauer, L., Christodorescu, M. and Cranor, L.F., 2013, July. What matters to users? factors that affect users' willingness to share information with online advertisers. In *Proceedings of the ninth symposium on usable privacy and security* (p. 7). ACM.

Li, H., Sarathy, R. and Xu, H., 2010. Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems, 51*(1), pp.62-71.

Li, Y., 2014. The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision support systems*, *57*, pp.343-354.

Lo, J., 2010, August. Privacy Concern, Locus of Control, and Salience in a Trust-Risk Model of Information Disclosure on Social Networking Sites. In *AMCIS* (p. 110).

Lund, A.M., 2001. Measuring usability with the use questionnaire. *Usability interface*, *8*(2), pp.3-6.

Lu, Y. and Yang, D., 2011. Information exchange in virtual communities under extreme disaster conditions. *Decision Support Systems, 50*(2), pp.529-538.

Macintosh, G., 2002. Building trust and satisfaction in travel counsellor/client relationships. *Journal of Travel & Tourism Marketing, 12*(4), pp.59-74.

Malhotra, N.K., Kim, S.S. and Agarwal, J., 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, *15*(4), pp.336-355.

Martin, K.D. and Murphy, P.E., 2017. The role of data privacy in marketing. Journal of the *Academy of Marketing Science*, *45*(2), pp.135-155.

Marr, B. 2015. *Big Data: 20 Mind-Boggling Facts Everyone Must Read.* Available: https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#191ab97b17b1 (07/08/2019)

Mathwick, C., Malhotra, N.K. and Rigdon, E., 2002. The effect of dynamic retail experiences on experiential perceptions of value: an Internet and catalogue comparison. *Journal of retailing*, *78*(1), pp.51-60.

Metzger, M.J., 2004. Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of computer-mediated communication*, 9(4), p.JCMC942.

Milgrom, P., & Roberts, J. 1992. Economics, Organisation and management. Englewood Cliffs, NJ: Prentice Hall.

Milne, G.R. and Boza, M.E., 1999. Trust and concern in consumers' perceptions of marketing information management practices. *Journal of interactive Marketing*, *13*(1), pp.5-24.

Moon, Y., 2000. Intimate exchanges: Using computers to elicit self-disclosure from consumers. Journal of consumer research, 26(4), pp.323-339.

Moorman, C., Deshpande, R. and Zaltman, G., 1993. Factors affecting trust in market research relationships. *Journal of marketing*, *57*(1), pp.81-101.

Mott, N. 2014. *The FTC condemns the data brokerage industry's collection practices*. Available at: https://pando.com/2014/05/27/the-ftc-condemns-the-data-brokerageindustrys-collection-practices/ (07/08/2019).

Mothersbaugh, D.L., Foxx, W.K., Beatty, S.E. and Wang, S., 2012. Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of service research*, *15*(1), pp.76-98.

Mühle, A., Grüner, A., Gayvoronskaya, T. and Meinel, C., 2018. A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, pp.80-86

Myerscough, S., Lowe, B. and Alpert, F., 2008. Willingness to provide personal information online: The role of perceived privacy risk, privacy statements and brand strength. *Journal of Website Promotion, 2*(1-2), pp.115-140.

Nahapiet, J. and Ghoshal, S., 1998. Social capital, intellectual capital, and the Organisational advantage. *Academy of management review, 23*(2), pp.242-266.

Nam, C., Song, C., Park, E.L. and Ik, C., 2006. Consumers' privacy concerns and willingness to provide marketing-related personal information online. *ACR North American Advances.*

Norberg, P.A., Horne, D.R. and Horne, D.A., 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs, 41*(1), pp.100-126.

Nowak, G.J. and Phelps, J., 1995. Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Direct Marketing, 9*(3), pp.46-60.

O'Neil, D., 2001. Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review, 19*(1), pp.17-31.

Pallant, J. 2013. *The SPSS survival manual*. 5. London: Open University Press.

Phelps, J., Nowak, G. and Ferrell, E., 2000. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), pp.27-41.

Phelps, J.E., D'Souza, G. and Nowak, G.J., 2001. Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing, 15*(4), pp.2-17.

Pirson, M. and Malhotra, D., 2011. Foundations of Organisational trust: What matters to different stakeholders?. *Organisation Science, 22*(4), pp.1087-1104.

Protection of Personal Information Act, No. 4 of 2013. 2013. Available: http://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf (07/08/2019).

Rempel, J.K., Holmes, J.G. and Zanna, M.P., 1985. Trust in close relationships. *Journal of personality and social psychology, 49*(1), p.95.

Rousseau, D.M., Sitkin, S.B., Burt, R.S. and Camerer, C., 1998. Not so different after all: A cross-discipline view of trust. *Academy of management review, 23*(3), pp.393-404.

Ruparelia, N., White, L. and Hughes, K., 2010. Drivers of brand trust in internet retailing. *Journal of Product & Brand Management, 19*(4), pp.250-260.

Rust, R.T., Kannan, P.K. and Peng, N., 2002. The customer economics of Internet privacy. *Journal of the Academy of Marketing Science, 30*(4), pp.455-464.

Sanchez, J., Callarisa, L., Rodriguez, R.M. and Moliner, M.A., 2006. Perceived value of the purchase of a tourism product. *Tourism management, 27*(3), pp.394-409.

Sasse, M.A., Steves, M., Krol, K. and Chisnell, D., 2014, June. The great authentication fatigue–and how to overcome it. In *International Conference on Cross-Cultural Design* (pp. 228-239). Springer, Cham.

Schaufeli, W. and Enzmann, D., 1998. The burnout companion to study and practice: A critical analysis. CRC press.

Schermer, B.W., Custers, B. and van der Hof, S., 2014. The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology, 16*(2), pp.171-182.

Schoenbachler, D.D. and Gordon, G.L., 2002. Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of interactive marketing, 16*(3), pp.2-16

Seppänen, R., Blomqvist, K. and Sundqvist, S., 2007. Measuring inter-Organisational trust—a critical review of the empirical research in 1990–2003. *Industrial marketing management, 36*(2), pp.249-265.

Shankar, V., Urban, G.L. and Sultan, F., 2002. Online trust: a stakeholder perspective, concepts, implications, and future directions. *The Journal of strategic information systems, 11*(3-4), pp.325-344.

Sheehan, K.B. and Hoy, M.G., 2000. Dimensions of privacy concern among online consumers. *Journal of public policy & marketing, 19*(1), pp.62-73.

Sheehan, K.B., 2002. Toward a typology of Internet users and online privacy concerns. *The Information Society, 18(*1), pp.21-32.

Siyavooshi, M., Sanayei, A. and Fathi, S., 2013. SMS Advertising and Consumer Privacy: Analysis of Factors Affecting Consumer Willingness to send and Receive Information in Permission and Data based SMS advertising. *New Marketing Research Journal.*

Slade, E.L., Dwivedi, Y.K., Piercy, N.C. and Williams, M.D., 2015. Modeling consumers' adoption intentions of remote mobile payments in the United Kingdom: extending UTAUT with innovativeness, risk, and trust. *Psychology & Marketing, 32*(8), pp.860-873.

Sridhar Balasubramanian, V.M., 2001. The economic leverage of the virtual community. *International journal of electronic commerce, 5*(3), pp.103-138.

Stanton, B., Theofanos, M.F., Prettyman, S.S. and Furman, S., 2016. Security fatigue. *IT Professional, 18*(5), pp.26-32.

Steenkamp, J.B.E. and Baumgartner, H., 2000. On the use of structural equation models for marketing modeling. *International journal of research in marketing*, *17*(2-3), pp.195-202

Stokkink, Q. and Pouwelse, J., 2018, July. Deployment of a blockchain-based self-sovereign identity. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 1336-1342). IEEE.

Streitfeld, E. 2018. *How calls for privacy may upend business for Facebook and Google*. Available:https://www.nytimes.com/2018/03/24/technology/google-facebook-data-privacy.html (2020/07/20).

Sullivan, C. and Burger, E., 2017. E-residency and blockchain. *Computer law & security review*, *33(*4), pp.470-481.

Sultan, F. and Mooraj, H.A., 2001. Designing a trust-based e-business strategy. M*arketing Management, 10(*4), pp.40-45.

Swan, J.E., Trawick Jr, I.F., Rink, D.R. and Roberts, J.J., 1988. Measuring dimensions of purchaser trust of industrial salespeople. *Journal of Personal Selling & Sales Management, 8(*1), pp.1-10.

Tai, Y.M., 2011. Perceived value for customers in information sharing services. *Industrial Management & Data Systems*, *111(*4), pp.551-569.

Tan, X., Qin, L., Kim, Y. and Hsu, J., 2012. Impact of privacy concern in social networking web sites. *Internet Research, 22(*2), pp.211-233.

Tandon, U., Kiran, R. and Sah, A.N., 2016. Customer satisfaction using website functionality, perceived usability and perceived usefulness towards online shopping in India. *Information development, 32(*5), pp.1657-1673.

Taylor, R. G. 1989. The role of trust in labor-management relations. *Organisation Development Journal*, 7: 85-89.

Thompson, D.V., Hamilton, R.W. and Rust, R.T., 2005. Feature fatigue: When product capabilities become too much of a good thing. *Journal of marketing research, 42*(4), pp.431-442.

Tobin, A. and Reed, D., 2016. *The inevitable rise of self-sovereign identity.* The Sovrin Foundation, 29.

Topaloglu, H., Gumussoy, C.A., Bayraktaroglu, A.E. and Calisir, F., 2013. The relative importance of usability and functionality factors for e-health web sites. *Human Factors and Ergonomics in Manufacturing & Service Industries, 23*(4), pp.336-345.

Toth, K.C. and Anderson-Priddy, A., 2018. Architecture for self-sovereign digital identity. In *Proc. 31st Int. Conf. Computer Applications for Industry and Engineering (CAINE)*.

Trochim, W. n.d. Descriptive Statistics. Available: https://socialresearchmethods.net/kb/descriptive-statistics/ (03/03/2020).

Tsesis, A., 2014. The right to erasure: Privacy, data brokers, and the indefinite retention of data. *Wake Forest L. Rev., 49*, p.433.

Urban, G.L., Sultan, F. and Qualls, W.J., 2000. Placing trust at the center of your Internet strategy. *Sloan Management Review, 42*(1), pp.39-48.

Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D., 2003. User acceptance of information technology: Toward a unified view. *MIS quarterly*, pp.425-478.

Venkatesh, V., Thong, J.Y. and Xu, X., 2012. Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly, 36*(1), pp.157-178.

Vergura, S., Acciani, G., Amoruso, V., Patrono, G.E. and Vacca, F., 2008. Descriptive and inferential statistics for supervising and monitoring the operation of PV plants. *IEEE Transactions on Industrial Electronics*, *56*(11), pp.4456-4464.

Von der Trenck, A., Emamjome, F., Neben, T. and Heinzl, A., 2015, January. What's in it for me? Conceptualizing the perceived value of knowledge sharing. In *2015 48th Hawaii International Conference on System Sciences* (pp. 3920-3928). IEEE.

Waite, A, 2016. *InfoSec Triads: Security/Functionality/Ease-of-use*. Available: https://blog.infosanity.co.uk/2010/06/12/infosec-triads-securityfunctionalityease-of-use/

(2019/06/17)

Wang, T., Duong, T.D. and Chen, C.C., 2016. Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*(4), pp.531-542.

Wang, H., Lee, M.K. and Wang, C., 1998. Consumer privacy concerns about Internet marketing. *Communications of the ACM*, *41*(3), pp.63-70.

Wang, Y.D. and Emurian, H.H., 2005. An overview of online trust: Concepts, elements, and implications. *Computers in human behavior*, *21*(1), pp.105-125.

Ward, S., Bridges, K. and Chitty, B., 2005. Do incentives matter? An examination of on-line privacy concerns and willingness to provide personal and financial information. J*ournal of Marketing Communications*, *11*(1), pp.21-40.

Wasko, M.M. and Faraj, S., 2000. "It is what one does": why people participate and help others in electronic communities of practice. *The journal of strategic information systems*, *9*(2-3), pp.155-173.

Weitzner, D.J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J. and Sussman, G.J., 2008. Information accountability. *Communications of the ACM*, *5*1(6), p.82.

White, T.B., 2004. Consumer disclosure and disclosure avoidance: A motivational framework. *Journal of Consumer Psychology*, *14*(1-2), pp.41-5

Williams, M., Rana, N., Dwivedi, Y. and Lal, B., 2011. Is UTAUT really used or just cited for the sake of it? A systematic review of citations of UTAUT's originating article.

Windley, P. 2018. *How blockchain makes self-sovereign identities possibl*e. Available: https://www.computerworld.com/article/3244128/how-blockchain-makes-self-sovereign-identities-possible.html (20200620)

Wong, K.K.K., 2013. Partial least squares structural equation modeling (PLS-SEM) techniques using s. *Marketing Bulletin*, *24*(1), pp.1-32.

Wong, K.K.K., 2016. Mediation analysis, categorical moderation analysis, and higher-order constructs modeling in Partial Least Squares Structural Equation Modeling (PLS-SEM): A B2B Example using SmartPLS. *Marketing Bulletin*, 26.

Xie, E., Teo, H.H. and Wan, W., 2006. Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. *Marketing letters*, *17*(1), pp.61-74.

Xu, H., Dinev, T., Smith, J. and Hart, P., 2011. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), p.1.

Yoon, A., 2014. End users' trust in data repositories: Definition and influences on trust development. *Archival Science*, *1*4(1), pp.17-34.

Young, L.C. and Wilkinson, I.F., 1989. The role of trust and co-operation in marketing channels: a preliminary study. *European journal of marketing*, *23*(2), pp.109-122

Zukowski, T. and Brown, I., 2007, October. Examining the influence of demographic factors on internet users' information privacy concerns. In *Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries (*pp. 197-204). ACM.

Appendix A: Ethics Clearance

Faculty of Commerce

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

04/02/2020

Matthew Hendricks

School of Management Studies

University of Cape Town

REF: REC 2020/02/004

Privacy, Self-Sovereign Identity Technology and The Willingness

To Provide Personal Information

We are pleased to inform you that your ethics application has been approved. Unless otherwise specified this ethical clearance is valid until 28 February 2021 .

Your clearance may be renewed upon application.

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

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

We wish you well for your research.

Signature Removed
2020.02.04
23:24:35 +02'00'

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

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

Appendix B: Questionnaire

Question Number	Construct	Question	Answers
Dear Respondent, *To stand a chance to win the R1000 Takealot voucher, please provide me with your email in the last question. This email will not be shared and be kept confidential. I am a Masters student in the Faculty of Commerce at the University of Cape Town. I am conducting a study on privacy and self-sovereign identity technology. You are invited to participate in this research. Your participation in this research is voluntary. You can choose to withdraw from the research at any time. Your answers will be helpful to illustrate the willingness of consumers to share personal information online. Your response will also help to determine the willingness of a consumer to use a blockchain related privacy technology (self-sovereign identity technology). This research has been approved by the Commerce Faculty Ethics in Research Committee. Please understand that you do not have to participate. The choice to participate is yours alone. If you choose not to participate, there will be no negative consequence. If you choose to participate, but later decide you want to withdraw, you are free to do so at any time, without negative consequence. However, I would be grateful if you would assist me by answering this survey. The online survey should take 10 minutes to complete. The survey can be completed by selecting the extent to which you agree with a statement from a 7-point scale ranging from strong disagree to strongly agree. Should you have any questions regarding the research please feel free to contact the researcher: Matthew Hendricks Email: HNDMAT008@myuct.ac.za Supervisor: Dr. Benedikt Hirschfelder Email: benedikt.hirschfelder@gmx.de			
1	N/A	Do you consent to this research?	Yes/No
2		Do you consent to your responses being disseminated and shared anonymously?	Yes/No
3	Past Experience With A Company	If I was happy with an online website during my last interaction, I would consider disclosing my personal information to that website.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
4		If an online website fulfilled my expectations during my last interaction, I would consider disclosing my personal information to that website.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
5		A positive past experience with an online website, helps me to trust a website with my personal information	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
6	Reputation Of A Company	I generally disclose my personal information to websites with a good reputation	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
7		I generally disclose my information to websites with a reputation for offering a good product or great service to their consumers.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
8		I generally disclose my information to websites which have a reputation for respecting their customers wishes linked to privacy.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
9	Perception of Dependability	I generally disclose my personal information to websites that can be counted on to do what they promised to do.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree

10		I generally disclose my personal information to websites I feel can be depended upon.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
11		I generally disclose my personal information to websites which I believe would resolve any issues I had with their product or service.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
12	Type of Personal Information Requested	I would consider providing information about my highest qualification to a company on the internet	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
13		I would consider providing information about my age to a company on the internet	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
14		I would consider providing information about my two favourite hobbies to a company on the internet	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
15		I would consider providing information about my two favourite television programs to a company on the internet	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
16		I would prefer NOT to provide my cellphone number to a company on the internet	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
17		I would prefer NOT to provide my identity number (ID) to a company on the internet	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
18		I would prefer NOT to provide my biometric data (data on human characteristics like fingerprints and eye colour) to a company on the internet	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
19		I would prefer NOT to provide information about my annual income to a company on the internet	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
20	Consequences and Benefits	I would consider exchanging my personal information for a discount or to save money at an online store	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
21		I would consider exchanging my personal information for a chance to win a free good or service	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
22		I would consider exchanging my personal information for a monetary reward	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
23	Consumer Control Over Information	I would like to have more control over what companies do with the my personal information.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
24		I would like to be able to control how companies distribute my personal information	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
25		I would like to be able to control which companies are able to access and use my personal information	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
26	Perceived Functional Value	When I disclose personal information to a website, the quality of the good or service the website provides is of a high standard or quality.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
27		The online websites I disclose personal information to fulfill my technical expectations. For example, loading times and how the website works.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
28		The online websites I disclose personal information to fulfill my privacy expectations	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree

29	Perceived Relational Value	I feel comfortable when I disclose personal information to a website	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
30		When I disclose information to a website, the website can be counted on to keep the promises it has made to me regarding the protection of my information	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
31		When I disclose information to a website, the website can be counted on to do what is right.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
32		I believe it is valuable to maintain a relationship with the websites I disclose personal information to	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
33	Willingness To Provide Personal Information	I am likely to disclose my personal information to an online website	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
34		I am likely to fill in or create a user profile containing personal information, to access a product or service offered by an online website.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
35		I am likely to provide an online website with information, if I am asked to do so.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
36		I would rate my willingness to disclose personal information to an online website as high	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree

Scenario: Imagine a new technology exists called Self-Sovereign Identity Technology. This technology allows your "identity" to exist online. This identity would be fully controlled by you.

When using this new technology:

Firstly, you control what exists online about you. For example, you could choose for your digital identity to not have your surname linked to it. You could also choose for your identity to contain any number of things like your eye colour, what foods you enjoy or your annual income. You can also alter what data exists about you at any time and remove or add data as you wish, to this digital identity.

Secondly, you can control who has access to and can distribute the data you make available. For example, an advertiser might want to know your address to send you a discount. You choose whether to grant the advertiser access to your address.

Lastly, You can't fake your personal information. The personal information which exists is verified by a trusted third party. For example, the bank will confirm the income that you disclose to 3rd parties.

If you would are interested in learning more, you can view a basic video explaining self-sovereign identity technology below.

The Sovrin Network- Making Self-Sovereign Identity a Reality

37	Behavioural Intention To Use SSI Technology	If the technology in the scenario existed, I would use it.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
38		I would try to incorporate the technology in the scenario in my daily life and activities on the web.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
39		I would use the technology in the scenario frequently.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
40		I would use the technology in the scenario on my phone or computer	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree

41		I would consider using the technology in the scenario to sell my personal information for my own monetary benefit, if the monetary benefit was high enough and it was safe to do so.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
42	Security	I imagine myself using the technology as it will make my internet experience, safer and more secure.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
43		I imagine myself using the technology in the scenario, if the technology is highly secure and will guarantee the information stored on it, is safe.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
44		I imagine myself using the technology in the scenario, if the security features allow me to effectively protect my privacy	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
45		I imagine myself using the technology in scenario because the security measures would allow me to feel safe when browsing the internet	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
46	Functionality	I imagine myself using this technology, if the solution or software is designed well.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
47		I imagine myself using this technology, as this technology has functionality that allows me to protect what information is shared online	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
48		I imagine myself using the technology in the scenario, as controlling the access to my personal data is important	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
49	Usability	I imagine myself using the technology in the scenario, assuming the technology does not interfere with my navigation of websites on the internet.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
50		I imagine myself using the technology in the scenario, if it is simple to use.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
51		I imagine myself using the technology in the scenario, if it is easy to learn to use it.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
52		I imagine myself using the technology in the scenario, if it works the way I want it to work.	Strongly Disagree, Somewhat Disagree, Neutral, Somewhat Agree, Agree Strongly Agree
53	Individual Consumer Characteristics	What gender do you identify as?	Male, Female, Other, Prefer Not To Answer
54		Which age group do you fall within?	Under 18, 18-24, 25-34, 35-44, 45-54, 55-64,65+
55	N/A	Do you currently live, or have you lived in South Africa?	Yes/No
56	N/A	Please provide your email address if you would like to be included for the R1000 Takealot Voucher	Free Text Response

Appendix C: Certification of editing

CERTIFICATION

This certifies that Gabi de Bie has edited Matthew Hendricks' dissertation.

A comprehensive edit involves editing the text for:

Language and Grammar;

Coherence and Flow;

Consistency;

Clarity which often requires necessary Overwriting;

Formatting (light)

Signed:

Signature Removed

BSc; BSc(Hons); MSc; PhD (Education)