Research Report

Sherwin Govender: 15008030

Supervisor: Sally Fisher

Research Methodology (RESM8419)

Bachelor of Commerce Honours in Management

TITLE:

A qualitative study exploring customers' reactions towards companies that are negligent with their personal data.

DECLARATION:

I hereby declare that the Research Report submitted for the Bachelors of Commerce Honours in Management degree to The Independent Institute of Education is my own work and has not previously been submitted to another University or Higher Education Institution for degree purposes.

WORD COUNT:

12 831 Words

ABSTRACT:

With the increase of the amount of personal information stored by organisations, privacy and data breaches are becoming more common. These breaches can result in financial loss, lost records, leading to identity theft and related crimes. In this study, the researcher explores consumers reactions towards privacy flaws and private information data breaches caused by the negligence of a company.

This research study found that consumers react negatively to companies that are negligent with their personal data. Furthermore, the study found that all participants had lost their trust and loyalty towards a company that exposed their personal data.

Data was collected using a semi-structured interview approach as it enabled the researcher to explore the views, experiences and beliefs of the participants on specific matters thus providing the researcher with a deeper understanding of the phenomenon.

Recommendations were made for future researchers to increase the sample size so more rigorous data could be generated. It was also recommended that customers reactions towards companies that do not safeguard their customers' personal data is explored across the country of South Africa.

TABLE OF CONTENTS

Presentation of Findings

Conclusion

References List

Annexures

INTRODUCTION:

Contextualisation:

The collection of personal information from consumers is an unavoidable element of electronic commerce (Hui, Teo & Lee, 2008). For consumers, Hui et al (2008) state that such information collection has both benefits and risk implications. In terms of benefits, it is now possible for consumers to access more convenient services and save transaction time and search costs (Hui et al, 2008). In terms of risk, unlike conventional retailing, consumers cannot remain anonymous in Internet transactions, and hence they face a new spectrum of risks of information misuse, such as transfer of their data to third parties or use of their data in unintended ways (Ponemon Institute LLC, 2017).

Today, individuals and organisations rely heavily on technology: high speed mobile devices and constant access to the Internet (Korzaan, Brooks & Greer, 2008). Therefore, this reliance has led to an increase in the amount of personal data that organisations capture, store, exchange, and use in order to conduct their operations. The disclosure of personal information by organisations, whether intentional or unintentional, is currently a very sensitive issue and illegal in some countries (Korzaan et al, 2008). Korzaan et al (2008) indicates that some organisations are so leery of disclosing personal information that they won't disclose the information to the individual themselves when the information could be very beneficial. For example, Anderson (2004) as cited by Korzaan et al (2008) mentioned a situation that arose during the "mad cow" scare in 2004 where large supermarket chains chose not to notify customers that may have purchased tainted meat in 2004. This would have alerted the customer as to how much personal information the company had stored. Organisations involved were very concerned as to how customers might react (Korzaan et al, 2008).

Data breaches are in the headlines and on the minds of both businesses and consumers (Ackerman, 2014). While much of the dialog has been driven by companies that experienced a data breach, this research study will explore consumers' sentiments about

data breaches (Ackerman, 2014). This research study aims to explore customers' reactions to companies that do not safeguard their customers' personal data and therefore leave their customers' personal data susceptible to data breaches.

Rationale:

Personal data is released and/or stored with every Instagram post, twitter status update, Facebook check-in, and when purchasing products and services (Ablon, 2016). Customer's personal data is beneficial to companies for product planning and it could also be profitable to companies, as they sell this personal data of clients to third parties (Schlesinger, 2017). Personal data of consumers could also be breached either by cyberattacks or hacking (Wallace, 2014).

As per Ponemon Institute LLC (2017) consumers are very apprehensive and concerned with data privacy. The personal data that companies obtain from customers are sold to third parties without their authorization (Schlesinger, 2017). Their personal data is also spread across the Internet, databases, computers, documents and email accounts and are therefore susceptible to cyber-attacks, hacking and data privacy breaches (Gemalto, 2017). Consequently, consumers appreciate companies that protect their personal data and shield them from personal data privacy breaches (Wallace, 2014).

By shielding customer's personal data, it helps to augment loyalty and trust; ultimately this would yield greater market share and profits for companies (Schlesinger, 2017). However, if weak data security methods are employed and the customers' personal data is not protected, this would have an impact on the relationship between the company and client (Wallace, 2014). Bennet (2017) as cited by Schlesinger (2017) states that a company's relationship with their customer is only as strong as the weakest link in the chain.

Therefore, data security is a very relevant issue in the 21st century as it impacts our day-to-day lives and most importantly the privacy of individuals (Ponemon Institute LLC, 2017). Regardless of their size, all businesses are involved in providing either services, goods or both to their customers (Schlesinger, 2017). Businesses of all types and sizes work with many different kinds of data such as information regarding the company's

employees, products, services or customers (Schlesinger, 2017). The potential risks of data security definitely outweigh the costs needed to implement extra data security (Schlesinger, 2017).

Problem Statement:

To gain an in-depth understanding of customers' reactions towards companies that do not safeguard their customers' personal data. As the amount of personal data stored and processed by organisations increases, so too does the complexity of the information systems required for its safe-keeping. Such data trends are correlated with an increase in the number of privacy incidents. A privacy incident can be broadly defined as an event involving misuse of individuals' personal information. This misuse can consist of illegal sale, or usage, or lack of protection. It can be criminal, commercial, or ultimately innocuous. It can be intentional or unintentional. Therefore, protecting customers' personal data will help businesses to build trust and loyalty, ultimately increasing market share and wallet share. Furthermore, data security is of paramount importance to businesses and by gaining customers views on this phenomenon, it will aid businesses in reviewing their data security methods to reduce personal data security breaches and invariably heighten profits. It might also assist in strengthening company-customer relationships.

Purpose Statement:

The purpose of this study is to explore customers' reactions towards companies that are negligent with their customers' personal data, using a cross-sectional design. The results will be a discussion of themes and patterns. Data security will be defined generally as protective digital privacy measures that are applied to prevent unauthorized access to information, databases and websites (O'Byrne, 2013).

Research Question:

What impact do companies, that employ weak data security methods, have on their customers?

Sub-question:

Is data security of paramount importance to a consumer?

Research objective:

To understand how the negligence of companies towards their customers' personal data impacts the relationship between company and client.

Theoretical foundation:

The "Hierarchy of needs" published by Maslow (1943) as cited by Kaur (2013) probably provided the field of human behavior and management with a new way of looking at individual's attitudes or behaviors in understanding how individuals are motivated.
Smit et al (2013) states that the best-known conceptualization of human needs has been proposed by this theory. Abraham Maslow was a clinical psychologist who introduced his theory based on personal judgement, which was generally known as the need hierarchy theory (Kaur, 2013). According to Maslow (1943) as cited by Kaur (2013) if people grew in an environment in which their needs are not met, they will be unlikely to function as healthy individuals or well-adjusted individuals. Specifically, Maslow (1943) theorized that people have five types of needs and that these are activated in a hierarchical manner, namely; Physiological, safety, love/belonging, esteem and self-actualization needs (Smit et al, 2013). This means that these needs are aroused in a specific order from lowest to highest, such that the lowest-order need must be fulfilled before the next order need is triggered and the process continues (Kaur, 2013). Safety is the only need that will be explored for the purposes of this research study.

Safety-security needs, as Maslow (1943) cited by Kaur (2013) explained, are also basic to human beings. To define the safety-security needs, it is necessary to identify the types of threats that could reduce the safety-security response and the conditions that satisfy these needs. Maslow (1943) as cited by Kaur (2013) stated that because this level of need is conceptually higher than the previous level, the terms used as threats to safety refer to both concrete and abstract things, such as wild animals, criminal assault, disease, war, anarchy, social chaos, natural catastrophes, and, in more peaceful times, the lack of such things as job security, financial security, medical insurance, and retirement security.

Maslow (1943) did not make mention of data security breaches such as hacking and cyberattacks because these issues were not prevalent at the time the theory was devised, but nevertheless, data security will fall under the umbrella of safety needs in the 21st century as it is a prominent safety-security issue.

Smit et al (2013) state that safety is one of human's most fundamental needs. They go on to state that majority of human actions and decisions emanate from protecting ourselves and our well-being. Humans are driven by the need for safety, for themselves, and that of their families and friends (Pichère, Cadiat & Probert, 2015). This need for security is also present in consumer behavior (Pichère et al, 2015). Therefore, products and services that are purchased must offer protection to the customers who have purchased it (Pichère et al, 2015). Specific measures must be put into place to protect and shield the consumer. Maslow (1943) as cited by Smit et al (2013) acknowledged safety as a basic human need in his hierarchy of needs theory. Therefore, Maslow's (1943) hierarchy of needs will be the best theory to use in relation to personal data security breaches as this is regarded as an infringement to an individual's safety.

Taormina and Gao (2013) state that Maslow's (1943, 1987) theory of human motivation has generated a great deal of interest, based on the number of citations it has garnered, but it has always been a controversial theory, because the literature includes both criticism and support. A key criticism directed at Maslow's (1943) proposition is regarding deprivation/ domination. This proposition states that a greater or increased deprivation would lead to a greater or increased strength in a need. With this proposition in mind, there is an implicit claim that deficient needs will have dominance as long as they have not been satiated (Rajagopal & Abraham 2009). However, many reviewers of this proposition could not find evidence of it. b and Syed (2018) showed that the deprivation/dominance concept either only enjoys partial support or no support when applied to the other needs of security, social or esteem. Taormina and Gao (2013) believe that this theory has made a significant contribution in the field of human behavior and management especially in the area of human motivation and remains attractive to researchers. Therefore, the incorporation of the need's theory into the current security environment helped to enhance the researcher's understanding of personal data security

breaches from a consumer's perspective. This theory essentially aided the researcher in exploring this phenomenon.

LITERATURE REVIEW:

Smith et al (1996) as cited by Li (2011) states that with the development of e-commerce, individuals' information privacy, referring to the ability of individuals to personally control information about themselves, is becoming critically important to individuals, organisations, industries, governments, and the global community. MacMillan (2010) reported the concerns of the United States congress about social network giant Facebooks practices of sharing the private information of its users without their consent. Similar concerns were expressed in other major media (Li, 2011).

Li (2011) postulated that although organisations, industries, and governments play important roles in protecting consumers' information privacy and consumers may take protective actions to reduce the risks, a full protection of privacy has not been achieved in the e-commerce environment. More studies are needed to understand consumers' privacy concerns and the factors that influence the concerns (Li, 2011). Scholars from multiple disciplines, especially the Information Systems (IS) field, have conducted extensive research on individuals' information privacy based on constructs such as perceived information privacy and information privacy concerns (Smith, Milberg & Burke, 1996). The former is a direct measure of an individual's perception of his/her information privacy, and the latter captures the worries about privacy control (Li, 2011).

Although these are two opposing constructs, they share many antecedents and consequences with reverse relationships and have been used interchangeably across studies (Cases, 2010). To develop a comprehensive view and understanding on customer's reactions towards companies that are negligent with their customer's personal data, this study considers both while emphasizing the privacy concern construct.

Themes discussed in the review include:

Information privacy, cybercrime, informed consent and concerns for information privacy (CFIP). Based on the review, an integrative framework is developed to illustrate the relationships between the themes.

Information privacy:

Information privacy can be defined as the privacy of personal information and usually relates to personal data stored on computer systems (Gemalto, 2017). The need to maintain information privacy is applicable to collected personal information, such as personal data, medical records, financial data, criminal records, political records, business related information or website data (Ponemon Institute LLC, 2017).

This literature review deals directly with information privacy as opposed to physical privacy as information privacy links directly to data security. The latter concerns physical access to an individual and/or the individual's surroundings and private space; the former concerns access to individually identifiable personal information (Korzaan et al, 2008). Historically, the concept of physical privacy was explicated first (Smith, Dinev & Xu, 2011). Later, as it became apparent that information about individuals and groups (especially families and organisational teams) was gathering saliency, information privacy was subsumed under the larger umbrella of general privacy (Smith et al, 2011).

General privacy as a philosophical, psychological, sociological, and legal concept has been researched for more than 100 years in almost all spheres of the social sciences (Smith et al, 2011). And yet, it is widely recognized that, as a concept, privacy is in disarray and nobody can articulate what it means (Smith et al, 2011). Solove (2006) as cited by Smith et al (2011) states that numerous attempts have been made by social and legal scholars to bring together the different perspectives found in different fields. However, the picture that emerges is fragmented with concepts, definitions, and relationships that are inconsistent and neither fully developed nor empirically validated (Smith et al, 2011).

Smith et al (1996) as cited by Martin et al (2015) shows that early research on privacy concerns in the Internet age proposed that personal information privacy was primarily the

responsibility of individuals. This was based on a long-held view of privacy as the right to be left alone, and that it is the individual's responsibility to maintain that right (Martin et al, 2015). However, privacy in the modern digital age is now a more complex concept that involves trade-offs between concerns about the collection of personal information and disclosure of such information for some gain (Smith et al, 2011). Privacy is therefore a context-driven concept that is characterised by complex dynamic relationships that must be balanced with the benefits of information sharing (Smith et al, 2011).

Recognising this need for balance, Westin (1970) as cited by Martin et al (2015) advocated privacy as the right to define for oneself when, how and to what extent information is released. Thus, from Westin's (1970) viewpoint, personal information privacy may be said to relate to identifying the information that an individual wants to keep private (Martin et al, 2015). Westin (1970) does not address how that information is managed (e.g. who may collect, store and manage that data and for what purpose) nor does he consider the context in which privacy trade-offs are made (Martin et al, 2015).

The current state of privacy research fails to capture the full range and richness of issues that are important to people when they make decisions about personal privacy (Martin et al, 2015). Kumaraguru and Cranor (2005) as cited by Martin et al (2015) states that Westin's (1970) metrics, although good and valid for their intended purpose, are relatively one-dimensional, and typically consist of only three or four self-response items. Given the complexity of peoples' privacy beliefs, this raises the question about whether a single, one-dimensional scale, such as that proposed by Westin (1970), is capable of capturing a complete picture of personal information privacy (Martin et al, 2015). To address this question, it is necessary to develop a new means of operationalizing and measuring personal information privacy, that captures the full range of privacy beliefs and how those beliefs are prioritized, and compares the results obtained by those measurements with Westin's (1970) theory of personal information privacy (Martin et al, 2015).

A number of limitations in Westin's (1970) research are recognized for further research, summarized as follows:

Westin (1970) completed most of his research and refined his theories in the years before widespread surveillance; collection and data mining of personal information became

common. In other words, the global context of personal information privacy has changed dramatically in recent years, and this has changed peoples' beliefs and attitudes with respect to personal information privacy (Martin et al, 2015). This alone would necessitate the revisiting of Westin's (1970) theory, in light of the new global information context.

Cybercrime:

Cybercrime can be defined as crimes committed on the Internet using the computer as either a tool or a targeted victim (Riek & Bohme, 2009). Cybercrime links directly with data security as it may cause an infringement of one's safety-security by exposing their personal information and details. Riek and Bohme (2009) state that online services provide extensive individual, social, and economic benefits for modern society. Online banking has introduced a convenient yet inexpensive and effective way of remotely handling financial transactions (Lee, 2009); ecommerce has increased product availability while decreasing trading costs (Li & Huang, 2009); and online social networks have deepened personal relationships worldwide (Li & Huang, 2009).

Unfortunately, the growing online space also provides ground for malicious behavior (Riek & Bohme, 2009). Utilizing the characteristics of the Internet, such as scalability, anonymity, and global reach, cybercrime emerged as a new form of crime and evolved into a serious industry in which specialized attackers operate globally to gain financial profit (Moore et al, 2009). Consumer-oriented cybercrime, which includes identity theft, credit card fraud, and phishing, increases the risk of using online services for all Internet users (Hunton, 2009). To avoid uncertain and risky situations, many Internet users remain reluctant to use online services (Riek & Bohme, 2009).

The information revolution, coupled with the strategic leveraging of the Internet, has exposed a number of relatively open societies to the dangers of cybercriminal acts, especially in commercial business transactions (Riek & Bohme, 2009). With the development of e-commerce, this commercial dark side has taken on many forms that affect the perceptions of the way consumers shop online (Hunton, 2009). Riek & Bohme (2009) states that corporations should realize that these threats to their online businesses have strategic implications to their business future and take proper measures to ensure

that these threats are eliminated or significantly reduced so that consumer confidence in the Internet as an alternative means of shopping is maintained.

These counter measures, coined as cybersecurity, have been developed to ensure the safety of consumer privacy and information and allow for a carefree shopping experience (Moore et al, 2009). There is need for the development of models that will allow corporations to study the effects of cybercrime on online consumer confidence and to counter through leveraging the benefits associated with the latest developments in cybersecurity (Riek & Bohme, 2009). With these two facets of e-commerce impacting the online consumer, corporations must ensure that the security measures taken will ultimately prevail to assure that consumers will continue to use the Internet to satisfy their shopping needs (Riek & Bohme, 2009).

From the above review of past literature pertaining to cybercrime the following limitation can be ascertained:

Work on the social effects of cybercrime is still rare, as most studies focus on cybercriminal motives and attacks, or provide technical, organisational, and regulatory measures to prevent cybercrime (Riek & Bohme, 2009). To fill this research gap, this research study must gain an in-depth understanding of the social impact of cybercrime and consumers reactions towards cybercrime by showing how it generates perceived risk and how this risk impacts the consumers.

Informed consent:

Consumers rarely read terms and conditions at all and as a result the signing-without-reading problem or, in the online environment, the clicking-without-reading problem is a well-documented phenomenon (Arnold, Hillebrand & Waldburger, 2014). Consumers agree to terms and conditions in all sorts of situations that may or may not have an impact on who can access their personal data, analyse it and potentially use it for action that consumers may feel uncomfortable about (Arnold et al, 2014). In fact, consumer surveys consistently show that consumers do say they worry about their personal data and what happens with it (Bakos, Marotta-Wurgler & Trossen, 2014). However, in practice, they show very little if any interest in engaging with terms and conditions or even more

specifically privacy policies (Arnold et al, 2014). Bakos et al (2014) find that only about 0.05% of agreements are actually accessed by consumers before they consent to them. It was found that access does not necessarily translate into consumers actually having read the terms and conditions as the average time spent viewing the content of the agreements was significantly below one minute (Bakos et al, 2014). Understandably, this is not enough to grasp the meaning of the respective agreement (Arnold et al, 2014).

Time is also the reason commonly identified in the literature for why consumers do not engage in reading terms and conditions (Bakos et al, 2014). As these texts are usually difficult and cumbersome to read, consumers rarely bother. In fact, if one was to read all the terms and conditions of the websites one visits throughout a year, this would take up several weeks assuming a full 40 hours of reading time each week (Bakos et al, 2014).

Given that the vast majority of website visits last no longer than 15 seconds, consumers' low rate of engagement is not surprising although it does contradict how strongly consumers usually say they feel about protecting their personal data, which is reported in various surveys (Arnold et al, 2014).

Based on the research conducted by Arnold et al (2014), it should be noted that the online environment facilitates the clicking-without-reading phenomenon compared to the offline signing-without-reading phenomenon to some extent. For instance, there is no one there to point the consumer to the important parts of the terms and conditions (Arnold et al, 2014). There is also no physical signature involved, which may present a stronger barrier than a simple click of a button (Arnold et al, 2014). Arnold et al (2014) further maintains that setting the default option to agree may further facilitate consumers' signing-without-reading for online privacy policies as humans tend to stick to the default option. Furthermore, consumers are strikingly unaware of what happens with their personal data (Bakos et al, 2014). For instance, they are commonly surprised to learn that their browsing history is analysed and used for targeted advertising (Bakos et al, 2014). So, they may also believe that there is no harm in not reading privacy policies (Bakos et al, 2014). Finally, browse-wrap contracts (i.e. agreeing to terms simply by using a website) may even impede the consumer from becoming aware of agreeing to a contract completely (Arnold et al, 2014).

Cadogan (2004) as cited by Arnold et al (2014) postulated that the length of terms and conditions and the legalistic jargon are blamed for consumers not being able to understand them. Cadogan (2004) further maintains that even law students were found to have significant problems understanding them. Studies investigating the readability of terms and conditions consistently find that at least university-level reading skills are needed to understand the terms and conditions (Arnold et al, 2014). However, Bansal (2014) argues that the problem may start even at an earlier stage. Several studies highlight that consumers already have great difficulty understanding the term “privacy policy” as it misleads them to believe that there is a policy in place to protect their privacy. Thus, it is not surprising that the mere presence of a privacy policy inclines consumers to disclose more personal information (Bansal, 2014). Privacy labels or seals or other graphical representations are likely to increase this effect, in particular when one’s involvement with privacy issues is low (Bansal, 2014).

Based on the research of Arnold et al (2014), it was found that there is a fundamental dissonance between the assumptions and requirements for informed consent as stipulated in law and actual consumer behaviour in practice. Whereas privacy law rests on the assumption that consumers give informed consent, which means that they have read and understood the agreement they enter, in practice consumers commonly do not read terms and conditions, and they are also not able to understand the concepts, contents and consequences (Arnold et al, 2014). These points are not disputed in the literature. Bansal (2014) as well as Arnold (2014) argues that the literature on the inadequacy of privacy policies is well-documented, and conclusive enough that it does not need to be continued.

From the above review of past literature pertaining to informed consent the following limitation can be ascertained:

It is critical to gain deeper insight into privacy issues from countries other than the United States of America. In addition to culture and regulatory structures, Li (2011) stipulates that other factors such as privacy disposition, information sensitivity and social norms may also show significant distinctions across countries and should be studied more thoroughly.

Concern for Information Privacy (CFIP)

The issue of data privacy, accuracy, and accessibility were first presented by Mason (1986) as cited by Korzaan et al (2008), the same decade that personal computers emerged at the forefront of office automation and innovation. Interestingly enough, recent research has shown that privacy is the most significant of the issues presented by Mason as cited by Korzaan et al (2008). Smith et al (1996) as cited by Korzaan et al (2008) presented a conceptual model that identified four underlying factors of information privacy concerns exhibited by individuals. The study showed that privacy is a complex construct with underlying factors pertaining to the collection, unauthorized secondary use (internal), unauthorized secondary use (external), and errors of personal information and data (Korzaan et al, 2008). Korzaan et al (2008) extended Smith et al (1996) by empirically validating the concern for information privacy (CFIP) construct and found that privacy concerns served as a mediator between computer anxiety and behavioral intentions.

An individual's CFIP refers to an individual's subjective views of fairness within the context of information privacy (Chen et al, 2008). Chen et al (2008) postulated that an individual's CFIP will be influenced by external conditions including industry sectors, cultures, and regulatory laws. Chen et al (2008) further maintain that an individual's perceptions of such external conditions will also vary with personal characteristics and past experiences. Therefore, people often have different opinions about how an organisation collects and uses of their personal information (Korzaan et al, 2008).

Concern for information privacy (CFIP) was first empirically introduced and examined by Smith et al (1996) as cited by Korzaan et al (2008). In their original conceptualization of the construct, four different categories were recognized to reference information privacy practices in organisations: collection, unauthorized secondary use (internal), unauthorized secondary use (external), and errors data (Korzaan et al, 2008). These four categories exemplify areas in which the individual exhibits concern about the use of their personal information and data (Korzaan et al, 2008).

The category of collection includes the general perceptions of the individual regarding the quantity or amount of data captured by the organisation (Li, 2011). Unauthorized secondary use, both internal and external, refers to exploiting collected data for

alternative (secondary) uses without the consent of the individual from whom the data was originally gathered (Li, 2011). External unauthorized secondary use specifically focuses on data being used by a party other than the organisation that originally collected the data such as a third party (Li, 2011). The final category, errors, highlights the view that the data will be captured incorrectly or that the data will be modified to where it is no longer accurate (Li, 2011).

The following limitation in literature regarding CFIP is recognized for further research:

The conceptualizations of the CFIP construct should be deepened to capture its evolving nature in a changing social-cultural, technological, and legislative environment (Li, 2011).

This review has implications for both researchers who are looking for theories that explain the importance of understanding personal information privacy concerns with technology and commercial companies who may look to address some of the concerns identified in this research study as these relate to the way in which they collect, manage and use consumer's personal information (Korzaan et al, 2008). Cybercrime is a pervasive threat for today's information driven society (Riek & Bohme, 2009). While the real extent and economic impact is hard to quantify, scientists and researchers agree that cybercrime is a huge and still growing problem (Riek & Bohme, 2009). Besides confirming the inadequacy of privacy policies, this literature review finds that even if consumers read and understand privacy policies, they would still have very little scope to evade the exposure of their personal data (Arnold et al, 2014). This review of past literature provides a comprehensive outlook of the empirical studies regarding CFIP from the individual behavior perspective, building a holistic picture of the privacy concern construct and its association with multiple antecedent and consequence factors (Li, 2011).

RESEARCH DESIGN AND METHODOLOGY:

Tradition:

An interpretivist approach was used as the research is of a qualitative nature. Goodsell (2013) states that Interpretivism is a tradition within social science, composed of efforts to understand, to construct meaning and to tap into the subjective experiences that people

have. An interpretivist approach is used to comprehend and give a description of meaningful social actions and experiences (du Plooy-Cilliers, Davis & Bezuidenhout, 2014, p.27). The aim of this research study was to explore companies that are negligent with the personal data of their customers and the impact it has on the customer. Therefore, this paradigm complimented this research study, as it assisted the researcher in understanding and describing this phenomenon by gaining an in-depth understanding of it (du Plooy-Cilliers et al, 2014, p.27).

Schwandt (2000) as cited by Ponterotto (2014) states that the interpretivist position espouses a hermeneutical approach, which maintains that meaning is hidden and must be brought to the surface through deep reflection. This reflection can be stimulated by the interactive researcher–participant dialogue (Ponterotto, 2014). Thus, a distinguishing characteristic of interpretivism is the centrality of the interaction between the investigator and the object of investigation (Ponterotto, 2014). Only through this interaction can deeper meaning be uncovered (Ponterotto, 2014). The researcher and his participants jointly create findings from their interactive dialogue and interpretation (Goodsell, 2013). Therefore, a semi-structured interview was used to co-construct findings and bring meaning to the surface to gain an understanding of the phenomenon (Goodsell, 2013).

Hui, Teo & Lee (2008) states that existing data privacy research lacks in-depth understanding of consumers' behavioral responses towards privacy breaches that were experienced in a real setting. Past privacy studies have mostly employed surveys, wherein consumers were asked to respond to hypothetical scenarios (Hui, Teo & Lee, 2008). Hui et al (2008) postulated that there are two weaknesses to such approaches. First, directly prompting consumers with questions about privacy may lead to biased responses because people may inflate their concerns and emphasize protective measures if they are asked to provide cheap opinions. Thus, these opinions may not reflect their true attitude toward data privacy (Hui et al, 2008). Second, survey responses may not be indicative of final choices (Hui et al, 2008). When evaluating privacy assurances, it is important to gain an in-depth understanding of consumer reactions (Hui et al, 2008). Since such in-depth explorations are missing from extant literature, this research study represents a first step in this direction.

Epistemology: This research study focused on knowledge that had an empathetic understanding (Bonjour, 2010). Empathy, which is understood as a non-inferential and non-theoretical method of grasping the content of other minds became closely associated with the concept of understanding (Stueber, 2013). This is a concept that was championed by the hermeneutic tradition of philosophy concerned with explicating the methods used in grasping the meaning and significance of texts, works of arts, and actions (Stueber, 2013). Hermeneutic thinkers insisted that the method used in understanding the significance of a text or a historical event has to be fundamentally distinguished from the method used in explaining an event within the context of the natural sciences (Bonjour, 2010). This methodological dualism is famously expressed by Stueber (2013) in saying that historical research does not want to explain; that is, derive in a form of an inferential argument, rather it wants to understand (Stueber, 2013). Stueber (2013) further states that "we explain nature but understand the life of the soul".

Ontology: Bryman (2008) postulates that ontology is the study of 'being' and is concerned with 'what is', i.e., the nature of existence and structure of reality as such or what it is possible to know about the world. Snape and Spencer (2003) define ontology as "a concept concerned with the existence of, and relationship between, different aspects of society such as social actors, cultural norms and social structures". Therefore, this research study favored knowledge that had multiple, socially constructed realities (Creswell et al, 2016, pg.60-61).

Axiology: Creswell et al (2016) states that axiology refers to the ethical issues that need to be considered when planning a research proposal. It considers the philosophical approach to making decisions of value or the right decisions (Kivunja & Kuyini, 2017). It involves defining, evaluating and understanding concepts of right and wrong behaviour relating to the research (Kivunja & Kuyini, 2017). It considers what value we shall attribute to the different aspects of our research, the participants, the data and the audience to which we shall report the results of our research (Kivunja & Kuyini, 2017). Therefore, the researcher focused on a study that is non-judgmental, ethical, moral and fair by considering the ethical issues surrounding this research study (Creswell et al, 2016, pg.60-61).

Research design:

A qualitative research design was used for this study as the aim of this research study was to explore companies that are negligent with customer's personal data and what impact it will have on their customers. This method is used extensively by scientists and researchers studying human behavior, opinions, themes and motivations (du Plooy-Cilliers, Davis & Bezuidenhout, 2014, p.229). While qualitative methods are sometimes assumed to be easier or less rigorous than quantitative ones, the fact is that information of this kind can provide a depth of understanding about phenomena that cannot be achieved in other ways (du Plooy-Cilliers, Davis & Bezuidenhout, 2014, p.229). Rahman (2017) postulates that qualitative data is concerned with the features, attributes and characteristics of phenomenon that can be interpreted thematically. For example, a claim that pilots demonstrate intelligence that is visual-spatial in nature rather than verbal (Rahman, 2017). The design of qualitative research is probably the most flexible of the various experimental techniques, encompassing a variety of accepted methods and structures (Rahman, 2017). Though there is no standardized structure, this type of study still needs to be carefully constructed and designed (Rahman, 2017). Researchers need to continually ensure they are conducting bias-free, open-ended technique and staying alert to potential sources of error (Rahman, 2017). This usually involves awareness of bias and deep sensitivity to the phenomenon in question (Rahman, 2017).

Qualitative techniques are extremely useful when a subject is too complex be encapsulated by a simple yes or no hypothesis (du Plooy-Cilliers, Davis & Bezuidenhout, 2014, p.229). While quantitative data reveals simple linear relationships between discrete variables, qualitative techniques yield data that is richer and more insightful into underlying reasons and patterns within phenomena (du Plooy-Cilliers, Davis & Bezuidenhout, 2014, p.229). Qualitative research is often more practicable when budgets are small and sample sizes are restricted (Rahman, 2017). If a large number of participants cannot be secured for a quantitative study, the few available participants can be better understood with in-depth interviews (Rahman, 2017).

While the flexibility of a qualitative research design offers a number of advantages, there are two challenges that researchers face when employing a qualitative research design

(Rahman, 2017). Qualitative research experiments can be time and resource consuming compared to quantitative experiments (Rahman, 2017). A researcher may need to conduct hour-long interviews, whereas a quantitative study using a questionnaire can be completed in an afternoon (Rahman, 2017). Qualitative methods also require plenty of careful thought and planning throughout the study (du Plooy-Cilliers, Davis & Bezuidenhout, 2014, p.229). Researchers have to be far more sensitive to ethical issues, bias and the philosophical underpinnings of their research question than those undertaking quantitative studies (du Plooy-Cilliers, Davis & Bezuidenhout, 2014, p.229).

Line of reasoning:

An inductive theorising approach was selected for this study. The reason this approach was selected is because it enabled the researcher to analyse specific customers' stories and views to then generalise the findings from the specific themes (du Plooy-Cilliers et al, 2014). Frequently, qualitative research methods are used for inductive theorizing because they support the inductive mode of reasoning in which the researcher starts with collecting and analyzing raw data and then subsequently discovers or generates emerging theory (Glaser & Strauss, 1967). This is done in the behavioral sciences by coding data, classifying into concepts and densifying into categories, and then making the connections between the concepts and categories clear (Gregory & Muntermann, 2011). Gregory and Muntermann (2011) further state that this approach to theorizing is viewed as 'bottom-up' because abstraction and generalizable theory stands at the end of the process, rather than the beginning.

Type of study:

This type of study is an exploratory study because this research study explored the research questions and did not offer final and conclusive solutions to existing problems (Shuttleworth, 2017). This type of research is usually conducted to study a problem that has not been clearly defined yet. Exploratory research is conducted in order to determine the nature of the problem, exploratory research is not intended to provide conclusive evidence, but helps the researcher to have a better understanding of the problem (Saunders, Lewis & Thornhill, 2012). When conducting exploratory research, the

researcher ought to be willing to change his/her direction as a result of revelation of new data and new insights. This enabled the researcher to gain a better understanding of the problem and it was very suitable to the research study (Saunders et al, 2012).

Type of approach:

A case study approach was chosen for this research study. A case study approach is an empirical inquiry about a contemporary phenomenon set within a real-world context (Creswell et al, 2016, pg.81). An exploratory case study approach is commonly used to explore those situations in which the intervention being evaluated has no clear, single set of outcomes (Creswell et al, 2016, pg.81). Therefore, it was appropriate for this research study, as the researcher selected a limited number of individuals as subjects of the study (Dudovskiy, 2016). This approach was advantageous to the researcher as there was close collaboration between the researcher and the participant, which enabled the participant to share their views and stories of how they felt towards the phenomenon (Creswell et al, 2016, pg.82).

Time-dimension:

A cross-sectional design was used to collect information for this research study, because the information was collected from the participants on a single occasion (Creswell et al, 2016). Thus, data was only collected once from the respondents and there were no repeats (du Plooy-Cilliers et al, 2014, pg.149). Therefore, this was the best design to use for this research study because it was the first and last time the researcher collected data from the respondents (du Plooy-Cilliers et al, 2014, pg.149).

Population

The population can be defined as the total group of people or entities from whom information is required (du Plooy-Cilliers et al, 2014, p.132). Therefore, the population of this research study can be defined as: A group of individuals whose personal data was negligently exposed by a company.

A target population is an entire population or group of individuals to whom a researcher wants to generalise findings (Pascoe, 2014). The target population for this research study consisted of individuals whose personal data was negligently exposed by a company.

Since it is usually impossible to obtain access to the target population due to its broad size and nature, an accessible population was used (Pascoe, 2014).

An accessible population can be defined as a population that enables the researcher to apply conclusions to (Shuttleworth, 2017). This population is known as the study population (Shuttleworth, 2017). Therefore, the population parameters for this study was individuals whose personal data was negligently exposed by a company in Durban, KwaZulu-Natal and surrounding areas.

Sampling

Non- probability sampling was used in this research study; this method is used when it is nearly or not possible to determine who the entire population is or when it is hard to gain access to the whole population (Creswell et al, 2016, pg.197). Non-probability techniques will make it possible to take a sample of population where the elements are infinite in number (Alvi, 2016). Non-probability sampling is well suited for exploratory research intended to generate new ideas that will be systematically tested later (Alvi, 2016). Therefore, non-probability sampling was suitable for this research study due to time limitations and limited financial resources (Alvi, 2016). Purposive Sampling was used in this research study. This method of sampling is used in special situations where the sampling is done with a specific purpose in mind, for example the research is about the attitude of non-married women between the ages of 20-25 years towards abortion (Sharma, 2017). This sampling method reflects a group of sampling techniques that rely on the judgement of the researcher when it comes to selecting the units such as people, case/organisations, events, pieces of data that are to be studied (Sharma, 2017). These purposive sampling techniques includes homogeneous sampling (Sharma, 2017).

Purposive sampling is advantageous because it can provide researchers with the justification to make generalisations from the sample that is being studied, whether such generalisations are theoretical, analytic and logical in nature (Creswell et al, 2016, pg.198). However, purposive samples, irrespective of the type of purposive sampling used, can be highly prone to researcher bias (Sharma, 2017). The idea that a purposive sample has been created based on the judgement of the researcher is not a good defence when it comes to alleviating possible researcher biases, especially when compared with

probability sampling techniques that are designed to reduce such biases (Sharma, 2017). However, this judgemental subjective component of purpose sampling is only a major disadvantage when such judgements are ill-conceived or poorly considered; that is, where judgements have not been based on clear criteria, whether a theoretical framework, expert elicitation or some other accepted criteria (Sharma, 2017). Homogenous samples were used in this research study and they consist of individuals with similar characteristics that were chosen to give a comprehensive picture of the phenomenon (Holloway & Wheeler, 2002). Therefore, the sample consisted of 2 participants whose personal data was negligently exposed by a company. Ethical concerns were taken into consideration and the sample selected were considered feasible both in terms of time and money (Creswell et al, 2016).

Data collection methods:

The researcher was the research instrument as this study was a qualitative study. As the research is of a qualitative nature, the data collection method of a semi-structured in-depth interview was chosen. An interview involves a two-way communication between the researcher and the participant, where data can be collected (du Plooy-Cilliers et al, 2014). Semi-structured in-depth interviews present questions to participants with the aim of learning more about their views, opinions and beliefs about a specific phenomenon (Creswell et al, 2016, pg.93). Blandford (2013) postulates that a semi-structured interview is more like a conversation, albeit one with a particular focus and purpose. Semi-structured interviews are more flexible than structured interviews (Creswell et al, 2016, pg.93). An interview question guide, usually including both closed-ended and open-ended questions, is prepared; but in the course of the interview, the interviewer has a certain amount of room to adjust the sequence of the questions to be asked and to add questions based on the context of the participants' responses (Briggs, 2000).

Briggs (2000) postulates that while the flexibility of semi-structured interviews offers a number of advantages, there are three main challenges that researchers face when using semi-structured interviews as a data collection method. The first challenge is that this method requires a significant amount of time to collect the needed information (Patton, 2002), especially when the researcher first enters the field and knows little about the

setting. It takes time to gain trust, develop rapport, and gain access to interviewees. Because each interview is highly individualized, the length of each interview session may be very long (Arksey & Knight, 1999).

The second challenge for researchers is to exert the right amount and type of control over the direction and pace of the conversation (Briggs, 2000). It is difficult to control the degree of directiveness of the questions and statements proposed during the conversation. Also, when a new topic emerges in the discussion, it is difficult for the researcher to know whether to follow it and risk losing continuity, or to stay on the major theme and risk missing additional useful information (Patton, 2002). Furthermore, when the interviewee moves the conversation/interview in a direction that is not useful, the interviewer will need to decide when and how to interrupt the conversation gracefully, to return it to a topic of interest for the purposes of the research (Patton,2002). Researchers agree that, to develop skills in sensitively controlling semi-structured interviews, both training and experience is very important (Briggs, 2000).

The third challenge is analyzing the data gathered by semi-structured interviews (Briggs, 2000). The questions asked in each interview were somewhat dependent on the context of the interview and so can vary across multiple interviews (Briggs, 2000). Different questions will generate different responses so that a great deal of effort has to be made to analyze the data systematically, to find the patterns within it (Patton, 2002).

Semi-structured interviews are most useful when the researcher wants to gain an in-depth understanding of a particular phenomenon within a particular cultural context (Briggs, 2000). In addition, they are most appropriate when the researcher is working within an interpretive research paradigm, in which the reality is socially constructed by the participants in the setting of interest (Briggs, 2000). The researcher will want to understand the phenomenon of interest from the individual perspectives of those who are involved with it (Briggs, 2000). Therefore, this data collection method was relevant to this study as it obtained views, opinions and beliefs of the phenomenon from the participants (Creswell et al, 2016, pg.93).

The interviews were done face-to-face with 2 participants in the month of August, and lasted between 25 and 30 minutes. Both interviews were audio-taped and were carried

out and fully transcribed by the researcher. The resulting data body comprises approximately 17 pages of interview transcripts.

The interview questions comprised of 15 open and close ended questions and the interviews followed the logic of the semi-structured interview: the pre-determined questions served as a general guideline, but the question wording and sequence could be handled flexibly by the interviewer. Additional questions could be asked as necessary. More generally, the interviewer had a leeway to add or reformulate questions, or drop questions if an answer had already been provided spontaneously, for instance. Overall the interviewer mostly respected the general structure of the interview questions guide.

Data analysis methods

Thematic analysis was used to analyze the data obtained in the semi-structured interviews. Through its theoretical freedom, thematic analysis provides a highly flexible approach that can be modified for the needs of many studies, providing a rich and detailed, yet complex account of data (Braun & Clarke, 2006).However, while thematic analysis is flexible, this flexibility can lead to inconsistency and a lack of coherence when developing themes derived from the research data (Holloway & Todres, 2003). Consistency and cohesion can be promoted by applying and making explicit an epistemological position that can coherently underpin the study's empirical claims (Holloway & Todres, 2003).

As thematic analysis does not require the detailed theoretical and technological knowledge of other qualitative approaches, it offers a more accessible form of analysis (Braun & Clarke, 2006). Thematic analysis is perceived to be very easy to use and has been proven to be very useful to beginner researchers (Saldaña, 2011). Thematic analysis is believed to be one of the most common forms of qualitative research. It is a method that is used for identifying, analyzing and reporting patterns within data (du Plooy-Cilliers et al, 2014, p.241). A further advantage, particularly from the perspective of learning and teaching, is that it is a method rather than a methodology (Braun & Clarke 2006; Clarke & Braun, 2013). This means that, unlike many qualitative methodologies, it is not tied to a particular epistemological or theoretical perspective (Clarke & Braun, 2013). This makes it a very flexible method, a considerable advantage given the diversity

of work in learning and teaching (Alholjailan, 2012). Therefore, this data-analysis method was relevant as the result of this research will be a discussion of themes and patterns.

Braun and Clarke (2006) devised a six-step method in which the researched carried out thematic analysis. They were the following:

1.The researcher was required to familiarise themselves with the data: This step provided the basis for the analysis and the researcher was required to be actively involved as well as fully immersed in the data (Braun and Clarke, 2006).

2.Generate initial codes: these are features of the data that is relevant, which needed to be established by the researcher (Braun and Clarke, 2006).

3.Searching for themes: a theme is a logical and meaningful pattern in the data pertinent to the research question (Braun and Clarke, 2006).

4.Reviewing themes: this involved the researcher examining the themes to ensure that they worked in relation to the coded extracts and the full data set (Braun and Clarke, 2006).

5.Defining and naming themes: this involved the researcher conducting and writing a detailed analysis of each theme (Braun and Clarke, 2006).

6.Producing the Report: The researcher was required to convert his analysis into an interpretable piece of writing by making use of vivid and compelling extract examples that relate to the themes and research questions and further contextualise it in relation to the existing literature (Braun and Clarke, 2006).

FINDINGS AND INTERPRETATION OF FINDINGS:

Presentation of findings

This research study comprised of two participants (one female and one male) from Durban, South Africa. Both participants wanted to remain anonymous during the interviews and have therefore been given pseudonyms. The Company's mentioned in the interviews were also given pseudonyms, namely Company A and Company B.

Sarah trusted approximately seven companies with her personal data. Out of those seven companies, two companies exposed her personal data. The most recent incident occurred in 2017 where an unauthorized party gained access to the personal details of her bank account due to Company A's weak online security system. This unauthorized access led to a fraudulent withdrawal from Sarah's bank account. Existing literature by Schlesinger (2017) states that cybercrime links directly with data security as it may cause an infringement of one's safety-security by exposing their personal information and details. Furthermore, existing literature postulates that online banking has introduced a convenient yet inexpensive and effective way of remotely handling financial transactions but leaves consumers prone to data-security threats and this was evident in Sarah's case (Lee, 2009).

Edward trusted approximately 5-6 companies with his personal data. Out of those five to six companies, one company exposed his personal data. Edward's personal data was exposed in mid-December 2017. Company A negligently exposed his personal data by sending his personal details to the wrong e-mail address. This personal information included his name, identity number, banking details and home address. Existing literature suggests that consumers are very apprehensive and concerned with data privacy (Wallace, 2014). Furthermore, Wallace (2014) states that their personal data is also spread across the Internet, databases, computers, documents and email accounts and are therefore susceptible to data-security threats. In this case, Edward's was spread across to the wrong email account and this left him susceptible to data-security threats.

Four themes emerged from the data inductively, namely: Weak data security methods negative effect on company's reputation, change in customer/company relationship, broken trust/loss of loyalty and data security's importance to a consumer and data security's importance to a consumer.

Theme 1: Weak data security methods negative effect on a company's reputation

A prominent pattern that arose from the research among both participants was that they brought the company's name into disrepute after their incidents with the company. Existing literature by Schlesinger (2017) suggests that customers who have had their personal information stolen are also likely to spread the word about their negative experience. About 85 percent of retail-breach victims said they tell others about the incident; 34 percent complain on social media and 20 percent comment directly on the retailer's website (Schlesinger, 2017).

Therefore, since measures were not put in place to protect both participants, they brought the company's name into disrepute. Sarah and Edward discouraged friends and family to conduct business with the respective companies. Regarding whether they would recommend the company to any person after the incident occurred, the participants answered the following:

> *Sarah: "I would never recommend a company like that to anyone because I don't want them to go through the same problems that I had. Company A's quality had deteriorated over the years and they are now a terrible company. By recommending Company A to someone would be very terrible of me!... I would never promote a company that has lackluster staff in their helpline division and terrible online security. They did not help me in my time of need and it was their wrongdoing so yeah, I would never recommend them to anyone, if anything I would tell everyone about this awful experience and encourage them to not deal with Company A".*

Sarah also stated that she would never recommend the company to her friends, family or anyone after the company negligently exposed her personal data.

Edward: "No. I wouldn't recommend Company A to anyone; their service is very poor and they're regressing as a company. As a matter of fact, I actually encouraged a co-worker to cancel her policies with Company A as well … and she took out new policies at Company B afterwards".

Sarah and Edward stopped doing business with the respective companies and terminated policies after the incident occurred. Existing literature suggests that Consumers have an impact on an organization's reputation and brand following a breach (Ackerman, 2014). A company will lose money in the short term and their stock prices will go down in almost all cases (Ackerman, 2014). Therefore, the incidents of Sarah and Edward would have a negative effect on the reputation of the companies.

When asked whether they are still with Company A or if they have moved to a new company after the incident occurred, the participants answered the following:

Sarah: "I closed my account with Company and moved to another company. I could not remain with Company A knowing that my money wasn't safe with them and I feared this incident happening again".

Edward: "I cancelled most of my policies with Company A but I still kept my life policy with Company A since I've been paying premiums for quite a long time now and you'll never know what will happen so just to be on the safe side I kept my life policy only. I cancelled my hospital, insurance and foundational policies which were very important policies but I had to move to another Company".

It is evident from the information gained from the participants that the weak data security methods employed by the respective companies had a negative effect on the company's reputation. This links directly with a recent Ponemon Institute study set out to examine the attitudes and perspectives of three key stakeholder populations inside a business environment: Marketing practitioners, IT practitioners and consumers (Ackerman, 2014). A key objective of the study was to understand the impact of a data breach on a company's customers, stock price and overall brand reputation (Ackerman, 2014). Among the survey's key findings: A data breach now outranks a scandal involving the CEO in terms of adverse impact on a company's reputation. Data-security breaches ranked in the

top three most negative events, following shoddy customer service and an environmental incident (Ackerman, 2014). Therefore, companies will lose existing customers and will find it difficult to attract new customers after negligently exposing the personal data of their customers.

Theme 2: Change in customer/company relationship

A prominent pattern that arose from the research among both participants was the change in their relationships after the incidents with the respective companies. Existing literature suggests that if weak data security methods are employed and the customers' personal data is not protected, it would have an impact on the relationship between the company and client (Wallace, 2014). Bennet (2017) as cited by Schlesinger (2017) states that a company's relationship with their customer is only as strong as the weakest link in the chain. Both participants relationships with the companies changed after the respective personal data breaches occurred.

When asked to describe their relationship with Company A before their personal data was exposed, the participants answered the following:

> *Sarah: "My relationship with Company A was very good prior to this incident. I never really had a major problem with them or their staff for that matter. Although I had a few minor issues with my online personal details being updated by Company A a few months ago, this matter was resolved timeously by a very diligent staff member of Company A. He assisted me with all my issues in a timely and orderly manner. I was very happy with his service and Company A at that point".*
>
> Edward: *"Honestly, I cannot give you a definite answer, I'd say my relationship with Company was somewhere between good and bad".*

This clearly shows that there was a good relationship between Sarah and the company prior to the data exposure incident and Edward had a borderline relationship with the company prior to his data exposure incident. However, when asked to describe their

relationship with Company A after their personal data was exposed, the participants answered the following:

> *Sarah: "After the incident had occurred my whole view of Company A changed. My relationship with Company A was very poor after the incident and the trust in our relationship was definitely broken. I phoned Company A and explained the situation to them but they did not offer me any assistance nor did they give me an answer as to how my cellphone banking account was accessed by a third party. They were very rude and not helpful at all! I wanted to close my account immediately because the arrogance and attitude will never have me as a client ever again, and I did not trust Company A with my money anymore because my cellphone banking account was accessed by a third party".*
>
> *Edward: "After the incident had occurred my already bad relationship with Company A just got worse. I do not have any respect for Company A, they never put the needs of their customer first. Company A make's promises to get you to sign a contract with them and then as soon as you claim they come up with all kinds of excuses. Furthermore, they let out my personal information so easily to God knows who. I do not feel very comfortable knowing that a random person has my personal details, especially in this day and age. I could not believe that Company A was so irresponsible! They sent an e-mail containing my personal details to the incorrect person, I mean if that doesn't make a customer angry, what will?"*

Therefore, it is evident from the information gained that the participants relationships clearly changed towards their respective companies after the incidents occurred. There was a clear negative impact on the relationships between the customers and the companies. Both Sarah and Edward replied *"No"* when asked whether they would ever conduct business with Company A again. Therefore, the responses of both participants concurs with a study conducted by Ponemon institute which found that 31 percent of consumers discontinue their relationship with a company that had a data breach and never return to the company afterwards (Ponemon Institute LLC, 2017).

Theme 3: Customers broken trust and loss of loyalty

A conspicuous theme that arose from the research among both participants was the change in their trust and loyalty after the incidents with the respective companies. Existing literature suggests that by shielding customer's personal data, it helps companies to augment loyalty and trust; and ultimately this would yield greater market share and profits for companies (Schlesinger, 2017). However, if weak data security methods are employed and the customers' personal data is not protected, this would have an impact on the trust and loyalty of the customer (Schlesinger, 2017).

When asked if they trust Company A after their personal data was exposed, the participants answered the following:

> *Sarah: "No!"*
>
> *Edward: "No, I do not trust Company A after that incident and their customer service is terrible".*

This clearly shows that both Sarah and Edward do not trust their respective company anymore. Furthermore, when asked if they would ever do business with Company A again, the participants answered the following:

> *Sarah: "No! No! No! I will never trust them with my money ever again. Furthermore, Company A didn't even reimburse me with the money that was fraudulently withdrawn from my account nor did they give me any compensation, not even a sorry. I don't think Company A's online security is up to scratch so I will definitely not be their client in the future because I do not feel safe with them".*
>
> *Edward: "No. I will never take out another policy with Company A or deal with them in any business. They've lost my trust and it will be very hard for them to regain my trust. Company A's customer service, security and methods are very poor so I don't think I would ever deal with Company A in the near future".*

Sarah also stated that she closed her account with the company and moved to a new company because she could not remain with a company knowing that her money wasn't safe and she feared the incident would happen again. Edward also cancelled most of his policies with the company and moved to a new company because of trust issues. Therefore, it is evident that the respective personal data breach incidents broke the trust and lost the loyalty of Sarah and Edward as they have both stated that they've lost their trust and loyalty towards the respective companies that negligently exposed their personal data.

These responses concur with a study conducted by Gemalto (2017) which found that 64 percent of consumers are unlikely to do business with a company where their financial or sensitive data was stolen (Gemalto, 2017). Existing literature suggests that organisations with a poor security posture were more likely to lose customers (Ponemon Institute LLC, 2017). In contrast, a strong security posture supports customer loyalty and trust (Ponemon Institute LLC, 2017). Therefore, it is evident from the information gained that the participants trust and loyalty towards the respective companies were negatively affected because of their poor security posture. Furthermore, both Sarah and Edward started dealing with new companies after the incident occurred and this clearly shows the loss of loyalty.

Theme 4: Data security's importance to a consumer

Sarah and Edward stated that data security is an important element of business nowadays and this is consistent with existing literature by Ablon (2016) which suggests that data security is of paramount importance to consumers. Personal data protection has quickly risen to the top of consumers' priority lists, as people around the world continue to witness or experience data breaches of increasing magnitude (Schlesinger, 2017). Customers care about data security and data protection more than ever (Schlesinger, 2017). According to Ablon (2016) consumers are more concerned about the security of their private information and personal data than their physical well-being. In other words, cybercriminals scare citizens more than actual thieves. The biggest worry in cyberspace involves individuals' bank accounts, while retailer hacks, medical record breaches and malware infections also keep consumers awake at night (Ablon, 2016).

When asked whether data security is an important element of business nowadays, the participants answered the following:

> *Sarah: "Yes! Most definitely. I believe that now more than ever after the experience I've had with Company A and I'm sure every other consumer feels the same way. I think it's one of the most important elements of business because if a customer does not trust the company they're dealing with then their relationship would be very poor".*
>
> *Edward: "I also think that protecting your customers personal data is very important as were living in a technological age. Since technology is at the forefront of all businesses nowadays I agree with those customers that proclaim data security is an important element of business. I wouldn't have been in this position if Company A protected my data, so I'd have to agree with that statement".*

These responses are consistent with the literature presented by Ablon (2016). Therefore, it is evident from the information gained that the participants perceive data security as an important element of business nowadays. Furthermore, both Sarah and Edward started appreciating companies that protect their personal data as opposed to companies that don't.

Trustworthiness and reliability

Trustworthiness is an essential framework for evaluating qualitative research and is made up of four dimensions, namely: credibility; transferability; confirmability and dependability (Du Plooy-Cilliers et al, 2014).

Shenton (2004) postulates that credibility is the first aspect or criterion that must be established and is one of the most important factors in establishing trustworthiness. Credibility refers to the accuracy with which the researcher interpreted the data that was provided by participants (Du Plooy-Cilliers et al, 2014). Du Plooy-Cilliers et al (2014) further maintains that credibility is increased when the researcher spends long periods of time with the participants in order to understand them better and gain insight into their lives. It must be acknowledged that the researcher attempted as best as possible to accurately interpret the data presented. Furthermore, it must also be acknowledged that the researcher spent a limited amount of time with the participants due to time constraints.

Although this study was conducted by means of thematic analysis and the researcher's time with the participants was limited, the trustworthiness of this particular study was enhanced as the researcher ensured that a substantial amount of time was used to accurately interpret the data from the participants' perspective (Du Plooy-Cilliers et al, 2014).

The ability of the findings to be applied to a similar situation, delivering similar results is known as Transferability (Shenton, 2004). Transferability is the degree to which results and analysis can be applied beyond a specific research project as it allows for generalization within an approach that does not lend itself to generalisation (Shenton, 2004). Other researchers conducting similar studies on data security will be able to make use of the findings of this particular study and this will increase the transferability of this study (Shenton, 2004). It should be noted that the value of this transferability is minimal due to the sample size.

Confirmability is the degree of neutrality in the research study's findings. According to Shenton (2004) it refers to how well the data collected supports the findings and interpretation of the researcher. In order to ensure confirmability, the researcher will not

base his findings in a biased manner or for the researchers' self-gain. It is important to acknowledge that the findings of this study drew similar conclusions to that of another researcher conducting this study or that of a reader who interprets the study (Shenton, 2004).

Dependability is an evaluation of the quality of the integrated process of data collection, data analysis and theory generation (Shenton, 2004). In order to ensure the dependability of the study the researcher will identify the specific data collection and analysis methods that will be used in order to gather data from the participants.

Rigour in qualitative research is linked with being open to the data, and thoroughness in collecting data (Du Plooy-Cilliers et al, 2014). For this study, the researcher used inductive reasoning and was open to the data and collected the data by using thematic analysis.

CONCLUSION:

Summary of Findings

Although the interpretation and presentation of findings provided some answers to the research question and sub question, this section aims to draw together key aspects from the interpretation and presentation of findings in order to answer the research question and the sub-question in a more comprehensive manner.

The research questions were examined through a qualitative approach in the form of semi-structured interviews. The use of semi-structured interviews allowed for more in-depth insight into the personal experiences of how customers react to companies that are negligent with their personal data. A review of the literature was presented corresponding to the research topic on customers' reactions towards companies that are negligent with their personal data. Finally, an interpretation of the findings obtained was provided, along with why the findings were relevant to the research with comparisons to other research carried out to date.

The research question was: What impact do companies, that employ weak data security methods, have on their customers? Themes 1,2 and 3 answered this research question.

Broken trust and the loss of loyalty was seen to be a critical factor for the participants to leave the company that was negligent with their personal data. The literature surrounding these themes also supported this notion. The participants also reacted negatively by holding the company's name in disrepute. Furthermore, there was a change in customer/ company relationship after the incidents occurred from good/mediocre to bad. Therefore, the research objective to understand how the negligence of companies towards their customers' personal data impacts the relationship has been met.

The sub-question was: Is data security of paramount importance to a consumer?
Theme 4 answered this sub question. It is evident from the findings that the participants had a strong belief that data security is very important. Both participants expressed that after the incident they perceive data security as a very important element of business in the 21st century. Existing literature by Schlesinger (2017), Ablon (2016) and Ponemon Institute LLC (2017) also supported these findings as it states that customers care about data security and data protection more than ever in the 21st century. It is important to acknowledge that this research study was small-scale so findings therefore cannot be generalised. Therefore, the research question and sub-question was answered successfully. Furthermore, the objective to understand how the negligence of companies towards their customers' personal data impacts the relationship between company and client has therefore been satisfied.

Recommendations for Future Research:

This research study was very limited due to the sample size used. Although the researcher asked the participants about their experiences, rigorous data was not generated. Therefore, it is recommended that future researchers use a larger sample size, as it will enable the researcher to generate more rigorous data, thus making a significant contribution to the existing body of knowledge surrounding this topic. Furthermore, although this study represents a start for developing a larger body of research on customers reactions towards companies that are negligent with their personal data, further research is necessary. Therefore, it is recommended that this topic

should be looked at in other parts of South Africa and across a variety of countries because most of the data surrounding this topic was gathered from studies conducted in the United States of America.

Heuristic value:

This study is academically important as there is very little qualitative research for customers reactions towards companies that are negligent with their personal data. Furthermore, most of the existing research has been driven by companies that experienced a data breach, this research study explored consumers' sentiments about data breaches. Therefore, this research study aimed to build the overall existing body of knowledge around consumers' reactions towards companies that are negligent with their personal data. However, it must be acknowledged that while this number of in-depth interviews provides a generous data source, it does not permit generalization to the larger population. This research study will aid businesses in reviewing their data security methods to reduce personal data security breaches and invariably heighten profits and also assist in strengthening company-customer relationships. Furthermore, the study also aimed to provide insight into the mindset of customers' who have been a victim to a personal data security breach.

Ethical considerations:

Participants of the research remained anonymous for the full duration of the research and they were given pseudonyms, at their own will. This guaranteed that the participants privacy is not infringed (Roberts, 2010). Informed consent was required from the participants before the interview was conducted. Therefore, the participants were fully aware of the underlying facts, implications and consequences of their actions during the interview (Roberts, 2010). The participants were able to retract from the research study at any given time without any consequences whatsoever (De Chesnay, 2014). The researcher at all times was unbiased towards the participants and the researcher did not persuade or draw the participants into answers (De Chesnay, 2014). The companies that were mentioned in the interviews by the participants and interviewer remained anonymous throughout the research study. For example, the companies will be referred

to as Company A or Company B instead of their actual names. Both interviews were tape recorded, granted that the interviewee gave his/her consent to do so (Bernard & Gravlee, 2005). The consent document stated clearly and explicitly that an audio recording was required and the participants granted their permission for recording to take place (Bernard & Gravlee, 2005).

Limitations:

The sample for this study comprised of 2 participants. This sample is only a very small proportion of the entire population. Therefore, research studies with much larger sample size would be required to ensure appropriate generalization of the findings of the study (Julius, 2009).

The data collection was confined to only the city of Durban since time and money constraints were encountered during the collection of data. Julius (2009) states that the replication of the study at different regions of the world would enable better generalizability of the findings of the study.

The findings cannot be extended to wider populations with the same degree of certainty that quantitative analyses can (Julius, 2009). This is because the findings of the research are not tested to discover whether they are statistically significant or due to chance (Julius, 2009).

Ambiguities, which are inherent in human language, could be a limitation to this study (Julius, 2009). For example, the word "red" could be used in a corpus to signify the color red, or as a political categorization e.g. socialism or communism (Julius, 2009). Julius (2009) postulates that in a qualitative analysis both senses of red in the phrase "the red flag" could be recognized.

REFERENCE LIST:

Ablon, L. 2016. *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, RAND Corporation, Santa Monica, Calif.

Ackerman, L. 2014. *The Aftermath of a Data Breach: Consumer Sentiment*. 1st ed. [ebook] New York: Ponemon Institute LLC, pp.1-23. Available at: https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf [Accessed 14 Apr. 2018].

Alholjailan, M.I. 2012. Thematic Analysis: A critical review of its process and evaluation. West East Journal of Social Sciences, 1(1), pp. 39-47.

Alvi, M. 2016. *A Manual for Selecting Sampling Techniques in Research*. 1st ed. [ebook] Karachi: University of Karachi, pp.13-14. Available at: https://mpra.ub.uni-muenchen.de/70218/1/MPRA_paper_70218.pdf [Accessed 22 May 2018].

Arksey, H, & Knight, P. 1999. Interviewing for social scientists: An introductory resource with examples. Thousand Oaks: SAGE Publications *(PDF) Use of Semi-Structured Interviews to Investigate Teacher Perceptions of Student Collaboration*. Available from: https://www.researchgate.net/publication/271138816_Use_of_Semi-Structured_Interviews_to_Investigate_Teacher_Perceptions_of_Student_Collaboration [Accessed July 25 2018].

Arnold, R., Hillebrand, A. and Waldburger, M. 2014. Personal Data and Privacy. *WIK-Consult GmbH*, 3(1), pp.1-70.

Bakos, Y, Marotta-Wurgler, F, and Trossen, D. 2014. Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts. The Journal of Legal Studies, 43(1), pp.1-35.

Bansal, G. 2015. *Efficacy of Privacy Assurance Mechanisms in the Context of Disclosing Health Information Online*. 1st ed. Milwaukee: University of Wisconsin, p.178.

Bernard, H, and Gravlee, C. 2005. *Skin Color, Culture, and Blood Pressure in Southeastern Puerto Rico*. 1st ed. [ebook] Arroyo: US National library of medicine, pp.5-6. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1449506/ [Accessed 27 Feb. 2018].

Blandford, A. 2013. *Semi-structured qualitative studies*. 2nd ed. [ebook] Aarhus: The Interaction Design Foundation, pp.23-24. Available at: http://discovery.ucl.ac.uk/1436174/2/semi-structured_qualitative_studies.pdf [Accessed 22 May 2018].

Bonjour, L. 2010. The myth of knowledge. Philosophical persepctives, [online] (24), p.1. Available at: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1520-8583.2010.00185.x [Accessed 19 Sep. 2018].

Braun, V, and Clarke, V. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, pp.77-101.

Briggs, C. 2000. Interview. *Journal of Linguistic Anthropology, 9*(1), pp.137-140.

Bryman, A. 2008. Social research methods. *Research Methods in Education*. London: Routledge.

Cases, A.S. 2010. Web Site Spill Over to Email Campaigns: The Role of Privacy, Trust and Shoppers Attitudes, *Journal of Business Research* (63)9–10, pp. 993–999.

Clarke, V, and Braun, V. 2013. Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. The Psychologist, 26(2), pp. 120-123.

Creswell, J, Ebersohn, L, Ferreira, R, Ivankova, N, Jansen, J, and Nieuwenhuis, J. 2016. *First steps in Research*. 2nd ed. Pretoria: Van Shaik Publishers.

Chen, K, Hwang, H, Sher, M, and Lin, E. 2008. *An Empirical Study of Concern for Privacy on Providing Health Information in the EMR Context*. 1st ed. Chung Cheng: National Chung Cheng University, pp.678-682.

De Chesnay, M. 2014. *Nursing Research Using Phenomenology: Qualitative Designs and Methods in Nursing*, New York: Springer Publishing Company, eBook Collection (EBSCOhost), EBSCO*host*, viewed 9 March 2018.

du Plooy-Cilliers, F, Davis, C, and Bezuidenhout, R. 2014. *Research Matters*. 1st ed. Cape Town: Juta and Company Ltd.

Dudovskiy, J. 2016.Interpretivism (interpretivist) Research Philosophy - Research Methodology. [online] Research Methodology. Available at: http://research-methodology.net/research- philosophy/interpretivism/ [Accessed 22 May 2018].

Fallatah, R. and Syed, J. 2018. Employee Motivation in Saudi Arabia. Journal of Management Sciences, [online] 3(2), pp.1-42. Available at: https://www.researchgate.net/publication/321395915_A_Critical_Review_of_Maslow's_Hierarchy_of_Needs [Accessed 25 Aug. 2018].

Gemalto.2017. 1st ed. [ebook] New York: Gemalto, pp.1-20. Available at: https://safenet.gemalto.com/resources/data-protection/data-breaches-customer-loyalty-report-2017/ [Accessed 7 April. 2018].

Glaser, B, and Strauss, A. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago: Aldine Publishing Company.

Goodsell, T. 2013. The Interpretive Tradition in Social Science. 1st ed. [ebook] Utah: University of Utah, pp.3-4. Available at: https://www.ncfr.org/sites/default/files/2017-01/interpretive_tradition_in_the_social_sciences_goodsell.pdf [Accessed 4 April. 2018].

Gregory, R. and Muntermann, J. 2011. *Theorizing in Design Science Research: Inductive versus Deductive Approaches*. 1st ed. [pdf] Shanghai: University of Göttingen, pp.1-17.

Available at: https://pdfs.semanticscholar.org/71b0/785b6da7f1f3f502bae744dfa0385461a5ab.pdf [Accessed 23 May 2018].

Holloway, I. and Todres, L. 2003. The Status of Method: Flexibility, Consistency and Coherence. Sage Journals, [online] 3(3), pp.345-357. Available at: http://journals.sagepub.com/doi/10.1177/1468794103033004 [Accessed 8 Aug. 2018].

Holloway, I. and Wheeler, S.2002. Qualitative research in nursing, 2nd ed. Oxford: Blackwell.

Hui, K, Teo, H, and Lee, S. 2008. The value of privacy assurance: an exploratory field experiment. *MIS Quarterly*, 31(1), pp.19-33.

Hunton, P. 2009. The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model. *Computer Law Security Review*. 25(6) 528-535.

Julius, M. 2009. An analysis of the strengths and limitation of qualitative and quantitative research paradigms. *Problems of education in the 21st century*, [online] 13(13), pp.1-6. Available at: http://www.scientiasocialis.lt/pec/files/pdf/Atieno_Vol.13.pdf [Accessed 22 May 2018].

Kaur, A. 2013. Maslow's Need Hierarchy Theory: Applications and Criticisms. Global *Journal of Management and Business Studies*, 3(10), pp.1061-1064.

Kivunja, C. and Kuyini, A. 2017. Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of Higher Education*, [online] 6(5), p.28. Available at: https://files.eric.ed.gov/fulltext/EJ1154775.pdf [Accessed 27 May 2018].

Korzaan, M, Brooks, N, and Greer, T. 2008. Demystifying personality and privacy: an empirical investigation into antecedents of concerns for information privacy. *Journal of Behavioral Studies in Business*, 1(2), pp.2-3.

Lee, Y. 2009. Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems* (2009), 18(2), pp.177-187.

Li, Y. 2011. Empirical studies on online information privacy concerns. *Communications of the Association for Information Systems*, 28(28), pp.454-492.

Li, Y, and Huang,J. 2009. Applying theory of perceived risk and technology acceptance model in the online shopping channel. *World Academy of Science, Engineering and Technology* 53(4) pp.816-822.

MacMillan, D. 2010. Facebook's Washington Problem, *Businessweek*, May 17–May 23, pp. 33–34.

Martin, G, Gupta, H, Wingreen, S, and Mills, A. 2015. An Analysis of Personal Information Privacy Concerns using Q-Methodology*. MIS Quarterly*, 24(3), pp.59-76.

Moore, T, Clayton, R, and Anderson, R. 2009. The economics of online crime. *Journal of Economic Perspectives*. 23(3) 3-20.

O'Byrne, S. 2013. *Data Security, Data Mining, And Data Management: Technologies and Challenges*, Hauppauge, New York: Nova Science Publishers, Inc, eBook Collection (EBSCOhost), EBSCO*host*, viewed 10 March 2018.

Pascoe, G. 2014. *Research Matters*, Chapter 11: Sampling. 1st Edition. Juta & Company Ltd. Cape Town, pp. 131-146.

Patton, M. 2002. wo Decades of Developments in Qualitative Inquiry A Personal, Experiential Perspective. Sage Journals, [online] 1(3), pp.261-283. Available at: http://journals.sagepub.com/doi/10.1177/1473325002001003636 [Accessed 24 Aug. 2018].

Pichère, P, Cadiat, A, and Probert, C. 2015, Maslow's Hierarchy of Needs: Gain Vital Insights into How to Motivate People, Namur: 50Minutes.com, eBook Collection (EBSCOhost), EBSCOhost, viewed 11 April 2018.

Ponemon Institute LLC. 2017. The impact of data breaches on reputation & share value.1st ed. [pdf], pp.1-26. Available at: https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf [Accessed 7 April. 2018].

Ponterotto, J. 2014. Qualitative Research in Counseling Psychology: A Primer on Research Paradigms and Philosophy of Science. *Journal of Counseling Psychology,* 52(2), pp.126-136.

Rahman, S. 2017. The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language “Testing and Assessment” Research: A Literature Review. *Journal of Education and Learning*, 6(1), pp.1-11.

Rajagopal, N, and Abraham, S. 2009. Prominence of Higher Order Needs: An Indian IT Sector Experience. Vilakshan: The XIMB. *Journal of Management*, 6(2), 15–28.

Riek, M, and Bohme, R.2009. Understanding the influence of cybercrime risk on the e-service adoption of European Internet users. 1st ed. Munich: University of Munster, pp.1-35.

Roberts, C.M. 2010. *The Dissertation Journey: A Practical and Comprehensive Guide to Planning, Writing, And Defending Your Dissertation*, Thousand Oaks, Calif: Corwin, eBook Collection (EBSCOhost), EBSCO*host*, viewed 12 March 2018.

Saldaña, J. 2011. *Fundamentals of Qualitative Research*, New York: Oxford University Press, eBook Collection (EBSCOhost), EBSCO*host*, viewed 12 March 2018.

Saunders, M, Lewis, P, and Thornhill, A. 2012. *Research Methods for Business Students.* 6th ed. London: Pearson Education Limited.

Schlesinger, S. 2017. *Digital Dilemma: Turning Data Security and Privacy Concerns into Opportunities* [online] Harvard Business Review. Available at: https://hbr.org/sponsored/2017/11/digital-dilemma-turning-data-security-and-privacy-concerns-into-opportunities [Accessed 3 Mar. 2018].

Sharma, G. 2017. Pros and cons of different sampling techniques. *International Journal of Applied Research*, 3(7), pp.749-752.

Shenton, A. 2004. Strategies for ensuring trustworthiness in qualitative research projects. Education for Information, 22(2), pp.63-75.

Shuttleworth, M. 2017. Qualitative Research Design. Explorable. [Online]. Available at: https://explorable.com/qualitative-research-design [Accessed: 20 April 2018]

Smit, P, Cronje, G, Brevis, T, and Vrba, M. 2013. *Management Principles*. 5th ed. Cape Town: Juta & Company Ltd.

Smith, H.J, S.J. Milberg, and S.J. Burke.1996. Information Privacy: Measuring Individuals' Concerns About Organizational Practices, *MIS Quarterly* (20)2, pp. 167–196.

Smith, J, Dinev, T, and Xu, H. 2011. Information Privacy Research: An Interdisciplinary Review*. MIS Quarterly*, 35(4), pp.989-1015.

Snape, D, and Spencer, L. 2003. The foundations of qualitative research In J. Richie & J. Lewis, *Qualitative Research Practice* (pp. 1-23). Los Angeles: Sage.

Stueber, K. 2013. Empathy as the Unique Method of the Human Sciences. In: *Stanford Encyclopedia of Philosophy*, 2nd ed. Stanford: Stanford University, pp.1-20.

Taormina, R, and Gao, J. 2013. Maslow and the Motivation Hierarchy: Measuring Satisfaction of the Needs. *American Journal of Psychology*, 126(2), pp.155-177.

Wallace, L. 2014. *Hidden Hazards of Online Advertising: An Investigation of Consumer Security and Data Privacy Protection*, New York: Nova Science Publishers, Inc., eBook Collection (EBSCOhost), EBSCO*host*, viewed 10 March 2018.

ANNEXURE A

CONSENT FORM TO PARTICIPATE IN A RESEARCH STUDY

RESEARCHER'S NAME: Sherwin Govender

PROJECT TITLE: A qualitative study exploring customers' reactions towards companies that are negligent with their personal data.

To whom it may concern,

My name is Sherwin Govender (the researcher) and I am a student at Varsity College Durban North. The researcher is currently conducting research about customers' reactions towards companies that are negligent with their personal data. The researcher hopes that this research will enhance the understanding of the field of data security. The researcher will be clearly explaining to you exactly what participation in my research study will involve. These are listed below in the forms of questions that the researcher will try to fully answer. If you have any questions that you feel are not addressed or explained fully in this information sheet, please do not hesitate to ask the researcher for more information. Once you have read and understood all the information contained in this sheet, please complete and sign the consent form below.

This consent may contain words that you do not understand. Please ask the researcher to explain any words or information that you do not clearly understand.

You are being asked to participate in a research study. When you are invited to participate in research, you have the right to be informed about the study procedures so that you can decide whether you want to consent to participation.

You have the right to know what you will be asked to do so that you can decide whether or not to be in the study. Your participation is voluntary. You do not have to be in the study if you do not want to. You may refuse to be in the study and nothing will happen.

If you do not want to continue to be in the study, you may stop at any time without penalty or loss of benefits to which you are otherwise entitled.

WHY IS THIS STUDY BEING DONE?

The purpose of this research is to understand how the negligence of companies towards their customers' personal data impacts the relationship between company and client.

WHAT AM I BEING ASKED TO DO?

You will be asked to answer a set of questions regarding a company's negligence towards your personal data.

HOW LONG WILL I BE IN THE STUDY?

This study will take approximately 30 minutes to 45 minutes to complete. You can stop participating at any time without penalty.

ARE THERE ANY RISKS OR DISCOMFORTS?

There are no known risks associated with this research.

ARE THERE ANY POTENTIAL BENEFITS?

There are no known benefits to you that would result from your participation in this research.

PROTECTION OF CONFIDENTIALITY

The researcher will do everything in his power to protect your privacy. Your identity will not be revealed in any publication resulting from this study. In addition, if photographs, audiotapes or videotapes were taken during the study that could identify you, then you must give special written permission for their use. In that case, you will be given the opportunity to view or listen, as applicable, to the photographs, audiotapes or videotapes before you give your permission for their use if you so request.

This study involves the audio recording of your interview with the researcher. Neither your name nor any other identifying information will be associated with the audio recording or the transcript. Only the research team will be able to listen to the recordings. The tapes will be transcribed by the researcher and erased once the transcriptions are checked for

accuracy. Transcripts of your interview may be reproduced in whole or in part for use in presentations or written products that result from this study. Neither your name nor any other identifying information (such as your voice) will be used in presentations or in written products resulting from the study.

IS PARTICIPATION VOLUNTARY?

Your participation in this research study is voluntary. You may choose not to participate and you may withdraw your consent to participate at any time. You will not be penalized in any way should you decide not to participate or to withdraw from this study.

WHOM DO I CALL IF I HAVE QUESTIONS OR PROBLEMS?

If you have any questions regarding your rights as a participant in this research and/or concerns about the study, you may contact Sherwin Govender at [redacted] or [redacted]. You may ask more questions about the study at any time. For questions about the study or a research-related injury, contact Sherwin Govender at [redacted]. A copy of this Informed Consent form will be given to you before you participate in the research.

SIGNATURE

I have read this consent form and my questions have been answered. My signature below means that I do want to be in the study and I am allowing the researcher to audio tape me as part of this research. I know that I can remove myself from the study at any time without any problems.

_____ _____

Participants signature Date

ANNEXURE B:

Interview Questions

1. Can you provide the number of companies that hold your personal data? 1.1. Has your personal data been exposed by any of these companies?
1.2. How many companies exposed your personal data?
1.3. Can we focus on the most recent Company that exposed your personal data?

2. How was your personal data exposed by Company A?

3. Can you describe how you first became aware of Company A's negligence with your personal data?

4. Can you describe your relationship with Company A before your personal data was exposed?

5. Can you describe your relationship with Company A after your personal data was exposed?

6. Are you still with Company A or did you move to a new Company after the exposure of your personal data? 6.1. Why did you take that action?
6.2. If you moved to a new company – would you ever do business with Company A ever again?

7. I've heard many consumers say that data security is an important element of business nowadays. What do you think about this after your experience with Company A?

8. How will this experience with Company A affect your future choices of who you'd do business with?

9. Would you ever recommend Company A to any person after your experience with Company A?

9.1. What is the reasoning behind your answer?