# THE VALUE REQUIRED TO NEGATE CONSUMER PRIVACY CONCERNS AROUND LOCATION

Dale Rosenberg

10665375

A research project submitted to the Gordon Institute of Business Science, University of Pretoria, in partial fulfilment of the requirements for the degree of Master of Business Administration.

9 November 2011

# ABSTRACT

Privacy has been discussed throughout the ages as the world has developed and changed however privacy concerns have been reignited by the development of technology. One of these technologies, Location Based Services (LBS), together with how organisations are using these technologies is pushing the consumers' privacy boundaries. In order for this technology to become widely adopted these privacy concerns need to be understood and addressed. It is therefore the purpose of this research to examine whether consumers' privacy concern can be negated through consumers receiving a benefit which caused them to forego this concern.

The research used scenarios to evaluate consumers' comfort levels for four different intrusion levels and five different discounts offered. Due to the nature of the scenarios a repeated measures ANOVA design was used in order to allow for the analysis of each of the scenarios, intrusion levels and discount offered for each respondent.

It was found that although privacy concerns can and were influenced by the offers made to the respondents, consumers have not yet gained a complete sense of comfort with the privacy boundaries that are being challenged.

# KEYWORDS

Privacy, Mobile Commerce, Location Based Services, Privacy Calculus.

# DECLARATION

I declare that this research project is my own work. It is submitted in partial fulfilment of the requirements for the degree of Master of Business Administration at the Gordon Institute of Business Science, University of Pretoria. It has not been submitted before for any degree or examination in any other University. I further declare that I have obtained the necessary authorisation and consent to carry out this research.

Date: 9th November 2011

________________________________

Dale Rosenberg

# ACKNOWLEDGEMENTS

The completion of this thesis would not have been possible if it were not for certain people in my life:

To my wife, Marié, who has supported and encouraged me throughout this MBA adventure. At times, it has been a bumpy road but words cannot describe how thankful I am for the sacrifices you have made to allow me to do this. Thank you for being you and for putting up with so much, you are an amazing inspiration in my life. This research is dedicated to you.

To my daughter Madison and my son Logan, I cannot wait to spend all my weekends with you guys.

To my supervisor, Howard Fox, thanks for providing me with direction when I needed it most, at the start! You helped me developed my topic into something of true interest.

To Lisa and the team at EOH, thanks for the support and for allowing me the opportunity to complete this journey.

To Rhys and Darryl, thanks for allowing me to start it.

# TABLE OF CONTENTS

# List Of Tables

# List Of Figures

# 1. INTRODUCTION TO RESEARCH PROBLEM

## 1.1. DESCRIPTION OF THE PROBLEM AND BACKGROUND

The mobile phone has been one of the few technologies that have had a significant impact on the world and the people in it (Greengard, 2008). The fact that people can connect freely with any other person at any point in time and at any location has drastically changed the way people think and act which has led to a significant change in social behaviour which has affected all industries and areas (Greengard, 2008).

Advancement of technology, such as the mobile phone, has given rise to new opportunities to both consumers and businesses alike. One of these new opportunities is Location Based Services (LBS), which allows consumers to enjoy services that are independent of location, while for businesses it has allowed the supply of services that are localised to the consumer (Xu H. , Teo, Tan, & Agarwal, 2009). In order for businesses to be able to supply these services they need to be able to establish the consumer's location. The need for this 'information' has raised the concerns that people have around their privacy, as was noted by Langenderfer & Miyazaki (2009), where they found that it was agreed that people have less privacy than they used to and that this development is a bad one.

The privacy concern, especially when related to technology commerce (Electronic commerce (e-commerce), Mobile Commerce (m-commerce) etc.)

has been identified as being a factor that influences the consumer's behaviour and intentions (Zhou, 2011). The concern around privacy is further highlighted by the fact that information which indicates the location of the consumer in real time provides a potential intrusion of privacy which is a critical and acute concern for the consumer (Xu H. , Teo, Tan, & Agarwal, 2009). To add further support to this, Sheng, Fui-Hoon Nah, & Siau (2008) highlight that information privacy has been identified as one of the most important issues in today's technology-based environment.

As identified by Junglas, Johnson, & Spitzmuller (2008), through understanding of the public opinion, privacy threats, is one of the main stumbling blocks that need to be overcome in order for there to be consumer adoption of LBS. They found that most people believed that location information was regarded as highly personal and very private. In other studies highlighted in this article it was found that in 2004, 35% of the people surveyed by Fischer (2004) believed that LBS had the potential to threaten their privacy; in further studies in 2006, this increased to 43% (Redknee, 2006); and in 2007, only ten percent of the respondents felt at ease with their family and friends having their location information (Porus & Ellis, 2007).

All things being equal, it was found that individuals perceive greater vulnerability when disclosing more sensitive information than they do for disclosing less sensitive information (Xu H. , 2009). As highlighted above location is definitely perceived as a sensitive piece of information. Hinz, Gertmeier, Tafreschi, Enzmann, & Schneider (2007) note that even consumers who hold privacy in high regard, recognise the benefits of disclosing information.

It has been agreed that personalisation offers added value to customers however in order for this personalisation to take place, the consumer is required to give up some of their personal information. This transfer of information triggers privacy concerns and creates what is known as the 'personalisation-privacy paradox'. The paradox is the value provided by personalisation against the vulnerability, potential loss of privacy and the possibly disclosure or misuse of their personal information. They examine the trade-off between benefit and risk and they suggest that the 'personalisation-privacy paradox' is better understood by based on the concept of situation dependency, which is rooted in the literature on consumer research. In other words, the effects of personalisation on customers' privacy concerns and intention to adopt vary according to the situation or context (Sheng, Nah, & Siau, 2008).

Sheng, Fui-Hoon Nah, & Siau (2008) state that according to the personalisation-privacy paradox, personalized services trigger privacy concerns and the tolerances around perceived privacy loss are situation dependent. Due to the concerns being directly related to the situation, one could expect that the tolerances would be different for each scenario / situation faced.

Xu, Teo, Tan, & Agarwal (2009) investigated the effect compensation had on an individual and their willingness to relax their privacy concerns when presented with potential benefits. Other research has found that monetary incentives do affect consumers and their preferences for privacy. Research expanded on this by investigating whether there was a risk-benefit trade-off performed by the consumer with regards to their privacy (Hui, Teo, & Tom Lee, 2007).

This research aims to specifically look at the required value to sway the risk-benefit trade-off in favour of disclosing information. It therefore examines whether the debate is really about privacy or rather whether the debate is around the value of the benefit which will be derived by the consumer.

This is of importance to marketers because consumers' attitudes towards the issues around mobile privacy have been seen to be largely influenced by the perceived benefits that mobile advertising and services can provide (Gurau & Ranchhod, 2009). However there is a fine line between information or marketing that is seen as valuable and information that is not valuable (Xu, Luo, Carroll, & Rosson, 2011).

Added to the above is the fact that the size of the m-commerce market is growing at a significant rate and it is predicted that the m-commerce industry will grow to $119billion in 2015 (Global mobile statistics 2011, 2010). This growth shows that there will be significant use of m-commerce in the future and as mentioned above one of the spin-offs of this will be increased use of LBS.
Reports show that LBS have enormous potential revenue growth in the future, and by 2013 it is expected to have an annual total of $13.3 billion (Xu H. , Teo, Tan, & Agarwal, 2009).

The reason why this problem was selected was because advances in technology has made the identification of a consumer's location possible and the technology has continued to evolve to allow a party to track another party to within metres of where they actually are (Junglas & Watson, 2008).

Added to this, Sheng, Nah, & Siau (2008), have identified that the value of a specific technology to a consumers can vary according to the context in which the consumer uses the technology. An entity can be defined as a person, place, or physical or computational object (Hwang et al., 2005). Situation and context are often used interchangeably.

As mentioned above this study wishes to explore the effect that the situation and context has on the privacy decision made by the consumer. It has been found that the Privacy concerns exhibited by people are not absolute concepts. They are rather a perception by the person about their rights and control over their personal information (Galanxhi & Nah, 2006). This perception of privacy often involves a risk/benefit assessment of the potential privacy exposure related to their use of a particular technology or application. In a manner that is consistent with expectancy theory, consumers will act in a manner that maximizes their positive outcomes and minimizes their negative ones (Dinev & Hart, 2006(a)). Based on this consumers usually exhibit 'a calculus of behaviour' trait that accounts for situational constraints. This is also known as the privacy calculus (Culnan & Bies, 2003). Research has found that people are willing to expose themselves to privacy loss provided there was a positive net benefit from the privacy information that was disclosed. In other words, consumers could be willing to disclose some of their personal information to allow for the benefits that would be received from a personalised service/product, but this would only be the case if the value of this personalized service/product far outweighed the potential loss of the information perceived to be private (Sheng, Nah, & Siau, 2008).

## 1.2. Purpose Of The Research

The purpose of this research is to determine whether consumers using LBS are actually concerned with the privacy issues that are raised by this technology or whether the concern is rather related to the consumer receiving an offer that allows the consumer to feel like they have made a fair trade. This will naturally test whether consumers place a specific value on privacy or whether every consumer has their 'privacy price'.

The value of personalising offers to consumers is of tremendous value to marketers and the data collection and use practices of these marketers' forms a social contract with consumers, where consumers are prepared to share their personal information for tangible or intangible benefits being offered by the marketers (Youn, 2009).

This research aims to test the required tangible benefit / value required to cause consumers' to forego their concerns around organisations collecting and using location information which without the offer would not be shared by the consumer. This would allow organisations to offer highly personalised and relevant offers.

## 1.3. Scope Of The Research

The aim of this research was to identify the relative attractiveness of the offer required to entice consumers to forego their privacy concerns around LBS.

The scope of this research was therefore limited to testing three hypotheses around privacy and value as described in chapter three. The research was sampled from the population of consumers that would use cellular phones for LBS. The sample used was the MBA groups at the Gordon Institute of Business Science during the year of 2011, including the full time, modular, evening and entrepreneurship MBA groups. In addition to this, to ensure that the results were not representing a sample of a similar disposition, the sample was extended to employees of five business units within EOH. This would assist in ensuring diversity in the sample used for this research.

# 2. LITERATURE REVIEW

## 2.1. INTRODUCTION

The development and advancement in technology is continually expanding organisations ability to store and use consumers' personal data, which in turn is raising the privacy fears of those consumers (Xu H., 2009). This has resulted in privacy becoming topical and controversial amongst all the relevant stakeholders (Xu H., 2009). According to studies privacy concerns and fears have contributed to the reduction in consumer confidence which has hindered the growth of Business-to-Consumer electronic commerce (B2C e-commence) by tens of billions of dollars (Cavoukian & Hamilton, 2002).

In an effort to try and restore some of this lost confidence in e-business, governments around the world are passing data protection legislation to complement the self-regulation that should already be taking place (Xu H., 2009). Due to the above, information privacy has become a business, social and legal issue that cannot be ignored (Xu H., 2009). It is therefore becoming increasingly important to examine and research this issue to establish where the sensitivities might lie.

Information privacy can be defined as the ability to control the use and collection of an individual's personal information (Bin Mai, Menon, & Sarkar, 2010). When consumers conduct a transaction electronically, the consumer is often required to provide sensitive information (identification and preferences) in order to complete the transaction. This collection of this information is what is driving the privacy concern within the consumer's mind (Bin Mai, Menon, & Sarkar, 2010).

With the above technology shift in mind, namely the electronic transaction and the collection of the data, and with the fact that mobile phones and mobile technology are changing both the digital environment that we live and work in, and it is changing all aspects of life as we know it (Greengard, 2008). Although in the past mobile phones have been accessible to the more affluent nations and consumers, this is no longer accurate, where developing nations are providing opportunities to use mobile technology and mobile commerce to provide services and products that previously might have been difficult to achieve (Greengard, 2008). It therefore makes sense that that there is an estimated five billion mobile users worldwide (Wikipedia, 2011) and it is believed that 80% of the world's population is close enough to be covered and use a cellular transmission tower (Greengard, 2008). This means that a majority of consumers now have mobile based commerce available to them.

The above proliferation in mobile devices within the world has renewed the interest in privacy, along with the advances that have occurred in technology which have allowed these technologies to become increasingly pervasive which makes the separation of privacy from technology increasingly difficult (Junglas, Johnson, & Spitzmuller, 2008). As mentioned in this research the change in the mobile commerce environment and the advent of LBS speaks specifically to the point that is raised above.

However, even though the devices and technologies have renewed some old concerns (namely privacy) and have brought about some new ones (namely location tracking), there are a number of different levels of concern around these privacy issues with consumers and these different levels influence how these consumers act from a privacy perspective. This can clearly be seen in the 2004 Harris Poll, where there were three segments were identified namely 'privacy fundamentalists', 'privacy pragmatists', and 'privacy unconcerned' (Harris Interactive, 2004). The privacy concerns for these segments ranged from very concerned to unconcerned. The 'privacy fundamentalists' felt that consumers should not provide any information to organisations and that there needed to be stronger regulations to assist with the control of how the organisation's acted (Milne & Bahl, 2010). These different levels show that consumers have different levels of concern around privacy and that privacy views is very much dependent on the person in other words it is highly personalised.

The 'privacy pragmatists' believed that the consumer should be able to choose what and how they shared their information and would weigh up the risk associated against this against the value of providing the information (Milne & Bahl, 2010). This clearly shows that consumers' perform a risk analysis on the information being shared. The 'privacy unconcerned' believed that there were no issues with supplying the organisations with the sensitive information and did they did not perceive any value in regulation. These segments represented 26%, 64%, and 10% of the United States of America (USA) adult population, respectively (Harris Interactive, 2004). This would imply that the majority of the USA adult population are concerned with privacy but see the potential value info sharing sensitive information with organisations.

## 2.2. PRIVACY

Privacy is defined as information about an individual that is deemed to be important and unattainable by the general population (Timm & Duven, 2008). The privacy of person is considered a fundamental human right and a clear indication of a democratic environment. Privacy is somewhat subjective as it differs depending on the person or environment and protects an interactions and communications (Birnhack, 2008).

Lessig (1999) identified several reasons as to why privacy protection is important. Firstly privacy empowers the control of information about oneself. Secondly it allows the person the right to be left alone, thereby confirming that the person has made a choice. Thirdly privacy ensures that each party treats the other party's private information with the required respect that is tacit when an exchange occurs between these parties. And fourthly privacy can be used as a means of regulating and controlling the collection and use of information about individuals. (Sheng, Nah, & Siau, 2008). This reiterates that privacy is important but it is extremely subjective.

Altman (1977) stated that privacy is not an absolute concept, but rather it is a control mechanism to a person's information which is regulated through a process whereby the individual continually evaluates the boundaries. Altman argued that privacy is not about avoiding the disclosure of personal information but rather about disclosing the level of information that allows the individual to reconcile the desire to maintain a private life but at the same time allowing the interaction and maintenance of a social persona (Margulis, 2003). This reconfirms what was found in the Harris report (above), which found that most people in the USA do not view it as an absolute concept.

The interest that is being generated in the privacy area has been triggered by the extensive advancement and use of internet-based technologies and the storage of information when using those technologies (Dinev & Hart, 2006(b)). Technologies such as social media and LBS are examples of these internet based technologies.

As such customers start to feel threatened when these technologies have the capability to use this personal information for surveillance/monitoring, storage and analysis, retrieval, and communication (Culnan M. , 1993). The rise in concern around privacy is driven by a customer's feeling and/or perception that the information that they have disclosed is vulnerable and that they are not able to control the use and flow of their personal information (Dinev & Hart, 2004). Motahari, Manikopoulos, Hiltz, & Jones (2007) argue that individuals are not completely aware or understand all of the threats to their privacy.

These areas of concern have been investigated and researched and Smith et al (1996) have identified several areas of concerns for individuals about their information privacy. The four areas are the collection of the individual's personal information, the unauthorised use of this personal information in secondary context, errors in personal information that has been stored, and the lack of the correct controls or security that leads to improper access to the individuals' personal information. Previous research has proven that when consumers' purchase items on the internet, they have a negative relationship between their privacy concerns and the purchase (Dinev & Hart, 2006(b)), and many consumers are therefore reluctant to make a purchase online due to the uncertainty related to the privacy and security of the transaction and/or personal information that is divulged during the transaction (Luo, 2002). These findings reiterate the study done by Cavoukian & Hamilton (2002) who found that the growth of e-commerce was slowed by the privacy concerns of consumers.

Privacy and the discussions around it have been focused to look at to address what are deemed to be the three main challenges namely theoretical-political, technological-commercial and a legal challenge (Birnhack, 2008). It is the area of technological-commercial that which is the most relevant to this study because the emergence of digital technologies has created an easy way for businesses to collect, process, mine and transfer data (Birnhack, 2008). It is this 'usage' of the data which causes individuals to become uncomfortable from a privacy perspective but only if the perceived value received is not sufficient to overcome the privacy fears (Zhou, 2011).

Therefore one of the most important issues relating to any technology-based environment and its use and adoption is the issues around information privacy

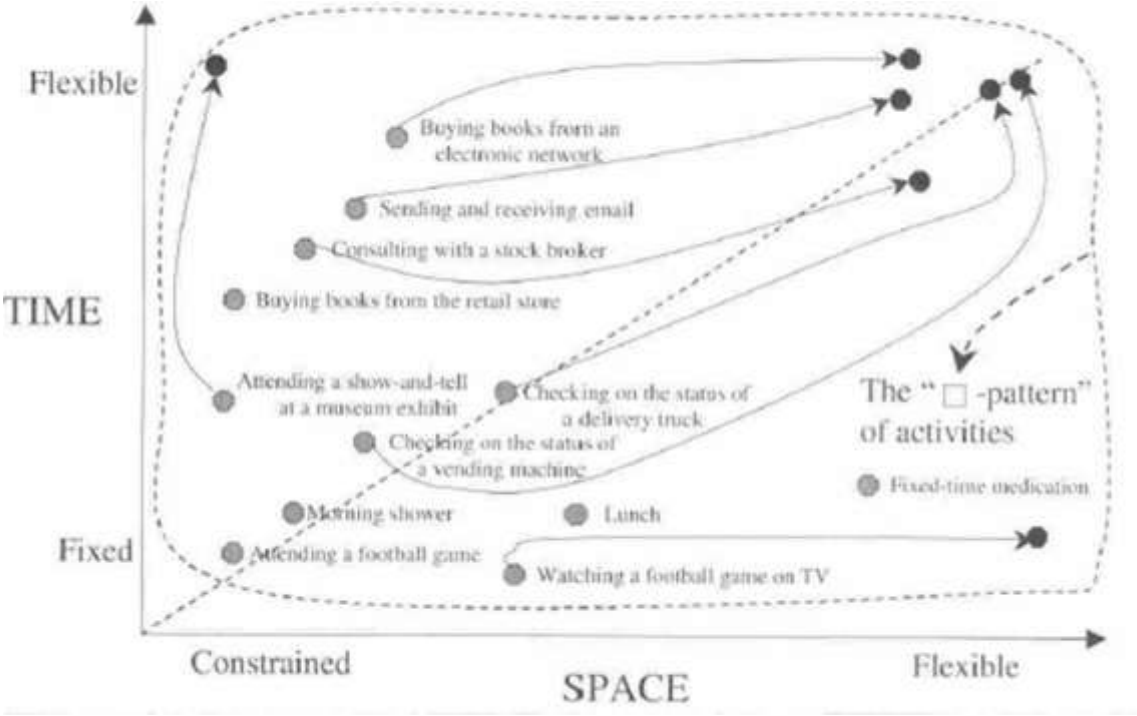
(Stewart & Segars, 2002). This is confirmed by the further findings in the Harris Poll, where 65% of respondents highlighted that they had decided against registering on an e-commerce site because of their privacy concerns (Harris Interactive, 2004). The Oxford Internet Institute survey (Dutton & Helsper, 2007) found that 70% of U.K. Internet users believed that by going onto the Internet, people are putting their privacy at risk and 84% (up from 66% in 2005) believed that their personal information is more than likely being kept without their knowledge.' (Joinson, Reips, Buchanan, & Schofield, 2010)

Consumers have the perception that their loss of privacy in a mobile commerce environment arises from two main concerns, firstly that they or their information can be accessed and/or tracked continuously by another party. Secondly this information can be relatively easily dispersed or used (Ohkubo, Suzuki, & Kinoshita, 2005). These privacy concerns have been reignited by the advances in the capabilities and pervasive nature of this technology. Marketers are now able to gather and assimilate information on consumers unlike ever before. As mentioned above, this is one of the most fundamental concerns that consumers have with these technologies. The main reason behind this collection and use of the information is to target individuals in a more personalised manner thereby hoping to build a longer and more substantial relationship ultimately increasing sales (Rapp, Hill, Gaines, & Wilson, 2009). One of the most pervasive technologies has been LBS, which requires the mobile service providers to be involved. Consumers appear trust in their mobile service provider allows them to believe that they have their best interests at heart (Zhou, 2011). Consumers require their providers to gain their permission before collecting and supplying them with LBS. When consumers receive LBS without their knowledge or permission they believe that their privacy has been violated by their provider (Tsang, Ho, & Liang, 2004). It has been noted in prior research that the advent of mobile phones enables a far easier manner to locate and communicate with these consumers which therefore creates a significant potential threat for consumers' privacy (Leek & Christodoulides, 2009). This privacy concern however, is not unreasonable as was shown in a study that looked at the use of RFID tags within a business environment, consumers made it very clear that they were relatively comfortable with the organisations using these tags within a closed environment or domain like a store however they expected the tracking to end when they left the store (Spiekermann S. , 2009).

## 2.3. Mobile Commerce

Balasubramanian et al (2002) believe that there is a distinct possibility that when a concept heavily relies on technology to deliver the concept, then there is a possibility that the technology gets confused for the concept. They believe that it is extremely important to conceptualise the characteristics of the concept not necessarily the technology. It is important to ensure that the concept of m-commerce is not confused with the technology when looking at the research that has been conducted around m-commerce. They further proposed that in order to properly understand the implications that are brought about by m-commerce, one needs to examine these services and products using a conceptual framework based on space and time. An m-commerce world allows activities to gravitate towards the spatial and temporal dimensions, this can help reduce the fact that, in a world without mobile technologies, space and time are both independently and mutually constraining (Balasubramanian, Peterson, & Jarvenpaa, 2002). This means that items that were previously only available at a time or space can now be used anytime and anywhere (Balasubramanian, Peterson, & Jarvenpaa, 2002).

Figure 1: Space-Time Matrix: Activities In A World With Mobile Technologies (Balasubramanian Et Al, 2002)


TIME
Flexible
Fixed
Buying books from an electronic network
Sending and receiving email
Consulting with a stock broker
Buying books from the retail store
Attending a show-and-tell at a museum exhibit
Checking on the status of a delivery truck
Checking on the status of a vending machine
The "□ -pattern" of activities
Fixed-time medication
Morning shower
Lunch
Attending a football game
Watching a football game on TV
Constrained
SPACE
Flexible

One of the most distinctive features of m-commerce is the importance of the consumer’s location, their context and their goals (Anckar & D'Incau, 2002). Five different goals were identified by Anckar & D'Incau (2002), and they are:

1. Time critical needs and arrangements
2. Spontaneous needs and decisions
3. Entertainment needs
4. Efficiency needs and ambitions

5. Mobility related needs

All of these help to introduce possibly the most interesting portion of m-commerce namely the ability to offer relevant and valuable items based on the consumer's location (Anckar & D'Incau, 2002).

## 2.4. LOCATION-BASED SERVICES (LBS)

LBS are an example of where a person is aware that it is possible for another person to track their movements in an unobtrusive manner. LBS make use of the consumer's location or position in order to provide services or products that are value-adding because of their relevance to the consumer at that point in time and space (Xu H. , Teo, Tan, & Agarwal, 2009). The services and/or products that are examples of this are emergency and safety related, entertainment related, navigation, asset tracking, location guides, traffic related and Location-Based Advertising (LBA). This means that the consumer has a specific need for that service/product at that point in time and space. This corresponds with Balasubramanian et al (2002) definition of m-commerce being time and space independent.

Wu & Hisa (2008), believe that location-aware services, will provide the ability to be able to conduct dynamic promotion and dynamic pricing which in turn will significantly increase both transaction value and frequency. This requires the consumer to feel comfortable with their location being disclosed and for there to be benefit for the consumer. As discussed above, one of the biggest threats to this is the privacy concern of the consumers'. This unobtrusive tracking could be perceived as highly intrusive (Xu & Teo, Alleviating consumers' privacy concern in location-based services: a psychological control perspective, 2004).

As noted by Junglas & Watson (2008), one of the main reasons why LBS have been slow to be adopted is because of consumers' concern around privacy.
As noted by Malhotra & Kubowicz Malhotra (2009) Relevancy-Based Services (RBS) provide a significant higher perception of usefulness. RBS are defined as services that are offered at the appropriate time at a specific location based on either consumer information or service consumption. They also note that LBS are not a proxy to allow suppliers to send consumers' offers simply because they are in a specific location. The consumers interest and past behaviour in the relevant product service needs to be used in conjunction with the location to provide true value (Malhotra & Kubowicz Malhotra, 2009)

The perceived risk associated with using technology, including LBS, varies depending on the context in which the services are used by the consumer, the functionality of the technology, and the consumer's purchasing experience history in a technology environment (Radin, Calkins, & Predmore, 2007). Irrespective of the cause, if consumers have a perception that these services are risky, then they will be less likely to use them. (Chen, Ross, & Huang, 2008)

## 2.5. CONSUMER BEHAVIOUR AND PRIVACY

Consumer behaviour is extremely important when looking at privacy, as the consumers' reactions that are seen in relation to a change or request to change a privacy stance or view, through the collection of information.

Consumers' and their concerns around privacy are increased whenever they feel uninformed and/or a loss of control about who is collecting their personal information, how this information has been obtained and the purposes for collecting this information (Lanier & Saini, 2008). These concerns and negative perceptions could motivate these consumers' to avoid privacy risks associated with sharing their personal information with marketers (Phelps, Nowak, & Ferrell, 2000). The stronger the above mentioned concern is about marketers' information collection practices, the higher the possibility that the individual will adopt risk-reducing behaviours (Lwin, Wirtz, & Williams, 2007).

The increase in the use of the internet as a social interaction tool naturally requires a loss of privacy for the user of these sites due to the increased amount of personal information that is required to be disclosed in order for the user to gain the maximum benefit from the site (Joinson A. N., 2008). This is illustrated in the functionality that allows the user to upload photographs from mobile phones where these photographs have some imbedded location information. This means that the users are required to make decisions on privacy-related issues about levels of access from both a security and disclosure perspective (Ahern, et al., 2007).

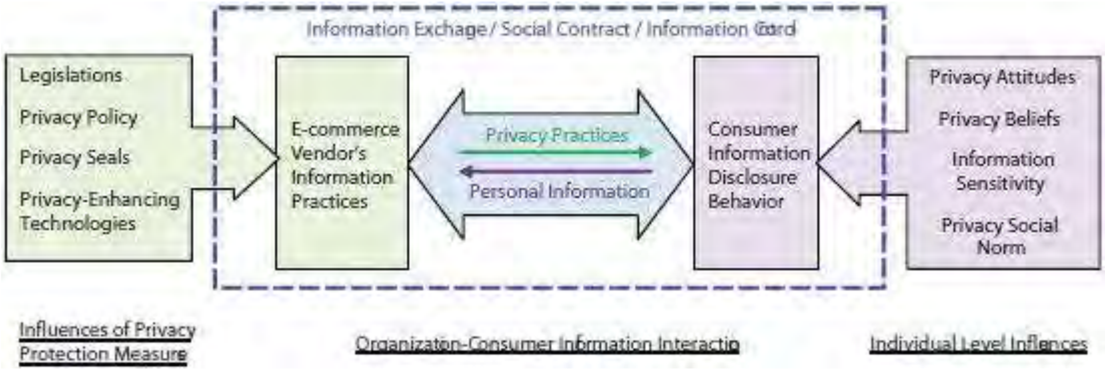
As discussed in the privacy section, privacy concerns generally have a negative effect on a user's intention to adopt a new application and/or technology and are one of the biggest barriers (Sheng, Nah, & Siau, 2008). For most decision makers, decisions are finalised after the user has evaluated the perceived benefits and costs (Goodhue, Wybo, & Kirsch, 1992). Most rational decision makers aim to reduce negative outcomes to their absolute minimum (Dinev & Hart, 2006(a)). A negative result of conducting mobile commerce is the forfeiture of privacy by the user. Privacy concerns can be viewed as a negative precursor belief, which could affect the person's attitude and, therefore it could influences their behaviour and/or intensions (Xu & Teo, 2004).

Much of the research conducted by that examined privacy concern and behaviour measured the reported disclosure or intended disclosure rather than actual behaviour. However when the actual behaviour was measured, it was found that the same pattern of results often emerged (Joinson, Reips, Buchanan, & Schofield, 2010). This is in line with how this study was conducted where an intended behaviour was requested.

The privacy concerns that people have over their data seems to be in situations where they do not control the amount and type of information being released (Lindley, 2010). These concerns however have not been sufficient enough to deter them from posting personal information on social networks (Lindley, 2010).

The Social Contract Lens, which is defined as a social contract, that occurs whenever consumers provide their personal information to an organisation and in response to this, the organisation offers the consumer some benefits (Caudill & Murphy, 2000). This social contract lens provides consumers with a method that allows them to reduce some of the risk associated with these technologies. As described above the social contract defines the trust relationship between the consumer and organisation and for the organisation one commitment is that they will assume the accountability to manage the consumers' personal information that they have provided, properly (Xu H., 2009).

FIGURE 2: INTERACTION BETWEEN E-COMMERCE SITES AND CONSUMERS: (XU H. , 2009)


Information Exchage / Social Contract / Information Card
Legislations
Privacy Policy
Privacy Seals
Privacy-Enhancing Technologies
E-commerce Vendor's Information Practices
Privacy Practices
Personal Information
Consumer Information Disclosure Behavior
Privacy Attitudes
Privacy Beliefs
Information Sensitivity
Privacy Social Norm
Influences of Privacy Protection Measure
Organizaton-Consumer Information Interactio
Individual Level Inflences

Even though this social contract is at best an implied contract, it is considered breached if any of the following events take place:

1. Firstly if the consumers' are unaware that their information has been collected,
2. Secondly if the organisation rents and/or sells the consumers' personal information to a third party without the permission of the consumers',

3. Thirdly if the organisation the information that they have about consumers' with an unauthorised party without first gaining the consumers' consent,
4. Fourthly if the organisation uses the consumers' personal information for purposes other than what they were originally collected for, without notifying these consumers (Phelps, Nowak, & Ferrell, 2000).

The decision made by consumers' with regards to information disclosure will be determined by four main factors:

1. Firstly the privacy attitudes of that consumer such as privacy concerns;
2. Secondly the privacy related attitudes namely the perceived risks, trust with the collecting organisation and the perceived control of the information collected;
3. Thirdly the type of personal information being requested by the organisation and;
4. Lastly the social norm (Xu H., 2009).

Sheng et al (2008) state that customers' intentions to adopt personalized services in mobile commerce are greatly influenced by their privacy concerns in respect of these services. They go on to mention that it was found that the relationship between privacy concerns and the intention to adopt a service depends on whether personalisation is involved in the offering. They also found in the scenarios where personalisation was used, it was found that privacy concerns significantly influenced customers' adoption intentions. However when there were scenarios with no personalisation for the consumer, there was no significant relationship between privacy concerns and the adoption intentions of those people (Sheng, Nah, & Siau, 2008). One possible explanation was that with non-personalisation a customer would not be tracked and therefore these scenarios do not require customers to give up sensitive information (Sheng, Nah, & Siau, 2008). Therefore with non-personalized services, the concern with privacy is significantly mitigated, which means that privacy concerns are non-issues when customers are making an adoption decision (Sheng, Nah, & Siau, 2008). These results lend weight to the fact that there is definitely a personalisation-privacy paradox (Sheng, Nah, & Siau, 2008).

## 2.6. THE PRIVACY CALCULUS

Xu (2009) tried to look at the principle of privacy through a number of different lenses in order to try and gain a better understanding of the influences on privacy. The first lens, which is referred to as the information exchange lens, conceptualizes the concept of privacy as a ‘privacy calculus’ which assists with understanding the trade-offs that consumers’ are willing to make, when these consumers’ exchange their personal information in return for certain benefits (Xu H., 2009). The second lens, which is referred to as the social contract lens (discussed above), outlines the discussions of the trust relationship between organizations and individuals with respect to information privacy. The information control lens, which is the third lens, emphasizes the role of the perception of control when trying to explain the privacy phenomenon. (Xu H., 2009).

He argued that consumers' privacy beliefs were influenced by the situational and environmental elements that determined the level of privacy protections in a particular environment (Xu H., 2009). Privacy decisions made by an individual are sometimes described in terms of a calculus where private personal information is given away in return for certain benefits which are deemed to have sufficient value (Xu H. , Teo, Tan, & Agarwal, 2009). This means that individuals are willing to forgo certain privacy concerns if they receive value in return.

Sheng, Fui-Hoon Nah, & Siau (2008) suggested that consumers' privacy concerns in a mobile commerce environment are triggered by personalisation irrespective of whether the situation was classified as an emergency and/or non-emergency situation. However, although there is a difference in consumers' privacy concerns between non-personalized and personalized offerings, the concern is greater in a non-emergency than in an emergency context (Sheng, Nah, & Siau, 2008). This suggests that consumers' privacy concerns or the extent to which they are prepared to supply their personal information is very much dependant on the situation that they are faced with and whether the services are of a personalised manner which influences the degree of tracking that is performed. This seems to suggest that privacy is a perception of consumers' that is largely influenced by situational factors. Therefore, the results of their study were consistent with the findings from other studies examining the privacy calculus. (Sheng, Nah, & Siau, 2008)

The results of their study suggested a very interesting interaction effect of personalisation and context on the consumers' intention to adopt the service / offering (Sheng, Nah, & Siau, 2008). It was found that consumers' intentions to adopt personalized services in an emergency situation were significantly higher than their intentions to adopt non-personalized services, for obvious reasons (Sheng, Nah, & Siau, 2008). However, in a non-emergency situation, consumers' intentions to adopt non-personalized services were significantly higher than their intentions to adopt more personalized services (Sheng, Nah, & Siau, 2008). The results of the study validate that situational factors greatly influence consumers' attitudes, perceptions, and decisions towards privacy and their concerns around privacy (Sheng, Nah, & Siau, 2008). This would point to consumers' adoption intentions and their related privacy concerns to be situation dependent (Sheng, Nah, & Siau, 2008). This would seem to indicate that in non-emergency situations consumers were more comfortable with non-personalised services.

Based on studies using the calculus perspective, described above, it has been shown that when assessing the privacy concerns relating to a situation where information needs to be given, consumers use a risk-benefit analysis to determine whether the exchange is worthwhile (Xu H. , Teo, Tan, & Agarwal, 2009). The privacy calculus is also both significant and relevant in a LBS context because it is used by the individual to weigh up the risks and benefits related to the information disclosure (Xu H. , Teo, Tan, & Agarwal, 2009). This relates back to the 'privacy pragmatists' view of privacy and how it should be handled.

Consumers have become aware that they need to share their personal information in order for them to have access to information and services at anytime and anywhere. This offering is made possible by using positioning and timelines to ensure that the service and / or information is relevant (Xu H. , Teo, Tan, & Agarwal, 2009). Although consumers are aware of this consumers' are willing to trade this information, which is deemed private, in exchange for rewards such as discounts, gift certificates, coupons etc. (Hann, Hui, Lee, & Png, 2007). It has been proven that these types of compensation generally enhance the consumer's perception of benefit when personal information is shared (Hann, Hui, Lee, & Png, 2007). Based on this, consumers' are therefore partial to giving up their personal information as long as there is a required benefit/value for them.

When 'push' based LBS is used the consumer needs to share a significant amount of personal information and their location in order to gain the benefits of locatability and personalisation (Xu H. , Teo, Tan, & Agarwal, 2009). Financial compensation for the consumer is more relevant when receiving push based LBS due to the fact that the consumer is foregoing more of their privacy in return for these benefits (Xu H. , Teo, Tan, & Agarwal, 2009). It was found that people did not appreciate receiving messages that were unsolicited, but a fair amount found it acceptable if they had subscribed and a significant number thought it acceptable especially if there was a benefit linked to the messages namely discount (Basheer & Ibrahim, 2010).

Service providers need to eliminate the consumers fear around privacy in order for higher adoption and usage of LBS (Zhou, 2011). Although consumers who have a modern smartphone which has GPS capabilities have a fear around the potential intrusion of privacy, they are constantly in a personalisation privacy paradox (Xu, Luo, Carroll, & Rosson, 2011). Consumers are caught between the view that there is great value in receiving customised, relevant messages that reinforce their desires to purchase against the concern around the privacy and disclosure of information (Xu, Luo, Carroll, & Rosson, 2011).

Personalisation is somewhat dependant on the consumers' willingness to divulge their personal information and use of LBS, however the consumer would like to receive these benefits/ services by parting with as little personal information as possible (Xu, Luo, Carroll, & Rosson, 2011). A growing number of consumers recognise that their privacy is for sale in the form of trading of their personal information for discounts and special offers. However, more intrusive attacks on consumers' privacy are conducted in a way that will prevent these consumers from paying the prices that they currently pay unless they are willing to sacrifice their privacy (Langenderfer & Miyazaki, 2009).

To illustrate this point, car insurers have recently begun to offer lower priced policies to consumers who were willing to install a device that would allow the insurer to monitor the distance travelled, speed, and even driving habits (Langenderfer & Miyazaki, 2009). More sophisticated devices which are installed in many of the new cars being released can monitor acceleration, braking, and seatbelt usage (Langenderfer & Miyazaki, 2009). Therefore in order to claim the lower premiums, which were previously offered to consumers based on less intrusive methods, many consumers will now pay for these with their privacy. Research is required in order to examine these more explicit exchanges of reduced privacy for increased benefits and whether such exchanges become more acceptable for consumers as their attitudes toward privacy and privacy protection change (Langenderfer & Miyazaki, 2009). This begins to highlight the need to examine the discount required in certain situations that will overcome these privacy concerns.

Consumers evaluate the type of benefit being offered in exchange for the personal information before deciding whether a specific activity or activities violates their privacy (Sheehan & Hoy, 2000). These benefits could either have a specific financial value or sometimes this value could be information based namely the access to specific information (Sheehan & Hoy, 2000). In a study that attempted to measure the dollar value of information privacy in an e-commerce environment, Hann et al. (2002) found that individuals are willing to trade off privacy concerns for economic benefits (Xu H., 2009). In addition, the practice of rewarding respondents in exchange for them sharing their personal views, attitudes or behaviours is well documented in the survey methodology literature as a method of increasing response rates (Xu H., 2009)). The exchange view of information privacy advocates the importance of rewarding consumers with benefits in return for them disclosing their personal information (Xu H., 2009).

This clearly shows that consumers will exchange their personal information provided they perceive sufficient benefits will be received in return namely the received benefits exceed the perceived risks of disclosing the personal information (Culnan & Bies, 2003). Consumers, when they have been requested to provide personal information to organisations, perform a risk-benefit analysis (a ‘privacy calculus’) to determine the results from the interaction and respond according to the analysis results (Culnan & Bies, 2003).

According to bounded rationality theory, people cannot have complete rationality because of the possible impact of information processing capacity limitations and hyperbolic discounting effect (Xu H., 2009). Some economic literature advocates that people have a tendency to discount ‘hyperbolically’ future costs or benefits (O’Donoghue & Rabin, 2001). This hyperbolic discounting implies inconsistency of personal preferences over time, namely future events and current events may be discounted at different discount rates (Acquisti, 2004). The theory of hyperbolic discounting can be applied to privacy decision making (Acquisti, 2004). The reason why is because, the benefits of disclosing personal information may be apparent immediately, (for example, ordering products/services online) however the risk of disclosing that personal information may be somewhat invisible or spread over time (for example, identity theft). Consumers’ may genuinely want to protect their personal information, however due to the bounded rationality, they could select to enjoy the immediate benefits of the purchase without cautiously calculating the long term risks of disclosing the information (Acquisti, 2004). Therefore, in the environment where the benefits of using e-commerce are immediate (for example, convenience, monetary rewards, and time savings), it is somewhat likely that consumers will opt for immediate gratification by discounting the potential risks of disclosing their personal information (Xu H., 2009). One could argue that consumers use the notion of the social contract in the environment of consumer information privacy context ensures that consumers would be willing to disclose personal information in order to enjoy certain benefits provided that they trust that the organisation will uphold its side of the contract by protecting the consumer's information (Xu H., 2009).

Hann et al. (2007), using an experimental approach, attempted to ascertain whether individuals valued privacy in online transactions and, if so, how much would these individuals pay for guarantee of their privacy. Students were asked to rank the trade-off between three types of privacy concerns and two levels of monetary rewards. The researchers found that the respondents were willing to trade off privacy concerns for a monetary reward of approximately $49 (Bin Mai, Menon, & Sarkar, 2010). The collection and subsequent use of consumers' private information, has raised important concerns about possible privacy invasion among these consumers which results in a personalisation–privacy compromise (Hui, Teo, & Tom Lee, 2007).

Therefore, one of the most central business issues for organisations that personalise their products and/or services is the protection of the consumer's privacy which will ultimately mitigate consumer privacy concerns (Lee, Ahn, & Bang, 2011). From the literature above it would appear that businesses would benefit from understanding the discount amount required in specific situations that would allow consumers to forego their privacy concerns. One of the aims of this study is to contribute to this by understanding the value required to overcome the privacy calculus where the benefits of the offer outweigh the risks associated with the offer.

# 3. RESEARCH HYPOTHESES

Given the literature discussed above, it is clear that research has been conducted on the issue around LBS and privacy. The literature builds the case that this item is becoming increasingly important to the world's population.

In the literature review a number of articles detail the research which has been conducted in order to try and evaluate whether a consumer's privacy can be bought. This relates mainly to the Personalisation-Privacy Paradox (Sheng, Nah, & Siau, 2008), which discusses the cost-benefit decision that is made by consumers with regard to privacy and getting more personalised offers. The research conducted previously has clearly shown that consumers are willing to forgo some privacy in order to enjoy greater benefits. In the research conducted by Hann et al (2007), the price required for the consumer to forgo privacy concerns online was explored.

With the increasingly dominant role mobile commerce and LBS are playing in the global economy, revenue in the LBS area is expected to grow to $14billion in 2014 (Xu, 2010), means that the privacy around LBS has and will increasingly remain a topical item of discussion.

This research will examine the value of offer required to illicit the Personalisation-Privacy Paradox when looking at LBS and privacy. In order to examine this, this research will look at one main hypothesis and then will have three sub-hypotheses which will assist with testing the main hypothesis.

The research hypotheses that will be examined are:

## 3.1. Hypothesis 1

**Hypothesis 1** (**H1**): Privacy concerns around location awareness in mobile commerce reduce as the consumer benefit increases in actual and perceived value: if consumers' are made an offer of value for a product that they are interested in, they will forego their privacy concerns in order to receive the value. This means that they would be prepared to disclose their location in order to recognise the value.

**Hypothesis 1** is operationalised as follows: Consumers express higher levels of comfort with disclosing their location information as the discount offered on their purchase is increased. This is also known as the discount effect.

This research hypothesis equates to the statistical null and alternative hypotheses as follows:

**$H_0$**: There is no discount effect on comfort levels

**$H_1$**: There is a discount effect on comfort levels

## 3.2. Hypothesis 1A

**Hypothesis 1A** (**H1A**): The purchase price of the product / service influences the decision around forgoing privacy irrespective of the offer being made: if the purchase price is low namely less than R500 then irrespective of the offer being made (50% discount), the consumer would be less inclined to reduce their privacy concerns around location.

**Hypothesis 1A** is operationalised as follows: Consumers express higher levels of comfort with disclosing their location information as the discount offered on purchases is increased for high priced items only, but remain the same for low priced items. This is also known as the scenario*discount effect.

This research hypothesis equates to the statistical null and alternative hypotheses as follows:

**$H_0$**: There is no scenario*discount offered effect on comfort levels

**$H_1$**: There is a scenario*discount offered effect on comfort levels

## 3.3. HYPOTHESIS 1B

**Hypothesis 1B** (**H1B**): The quantum of the offer affects the amount of location data given: if the offer has significant value then consumers' would be prepared to disclose significant information to receive the value / offer.

**Hypothesis 1B** is operationalised as follows: Consumers express higher levels of comfort with disclosing increasing amounts of identifying information when the perceived value of the discount offered relative to product value is increased. . This is also known as the scenario*intrusion effect.

This research hypothesis equates to the statistical null and alternative hypotheses as follows:

**$H_0$**: There is no scenario*intrusion level effect on comfort levels

**$H_1$**: There is a scenario* intrusion level effect on comfort levels

## 3.4. HYPOTHESIS 1C

**Hypothesis 1C** (**H1C**): Benefits that are received on an on-going basis will cause more location information to be disclosed than a once off benefit at time of purchase: if the offer that is made makes provision for recurring benefits, the consumer would agree to more location information disclosure than if the benefit was a once off benefit.

**Hypothesis 1C** is operationalised as follows: Consumers express higher levels of comfort with disclosing their location information for benefits that are received on an on-going basis than for a once off benefit at time of purchase. This is also known as the scenario effect.

This research hypothesis equates to the statistical null and alternative hypotheses as follows:

**$H_0$**: There is no scenario effect on comfort levels

**$H_1$**: There is a scenario effect on comfort levels

# 4. RESEARCH METHODOLOGY

## 4.1. INTRODUCTION

Chapter four describes the research process and methodology that was used in order to test the hypotheses described in chapter three above. This research aimed to illustrate that the concerns around location based services were really about price benefit rather than privacy and it also aimed to establish the required offer/discount in order for a consumer to forego their privacy.

Current research is showing that privacy represents *the* major roadblock for the adoption of LBS in the m-commerce environment (Junglas, Johnson, & Spitzmuller, 2008). Previous research done by Little & Briggs (2009) noted that it is important that researchers better understand the cost-benefit trade-off that will cause consumers (e-commerce and mobile) to trade their information in order to achieve an improved service, which has been referred to above as the Personalisation-Privacy Paradox. This research aimed to explore this in the mobile environment and was attempting to determine the quantum of that benefit.

## 4.2. RESEARCH METHOD

This research was predictive in nature as it aimed to attempt to provide a possible explanation for a particular event after it has occurred and possibly allows the possible prediction of when and in what scenarios this event might occur again (Blumberg, Cooper, & Schindler, 2008). Therefore this study attempted to find the possible explanations for the results from the different scenarios in order to attempt to understand those scenarios after the fact. By understanding these results, it might allow the prediction of how consumers will react to scenarios based on these in the future. Blumberg, Cooper, & Schindler (2008) describe how scenario models and expert surveys are other methods that assist with the prediction of future behaviour.

The research made use of quantitative methods which are best used when trying to measure the 'quantity or extent of the' item being research or 'phenomenon' by using numbers or figures (Zikmund, 2003).

The research used scenarios to describe situations that placed the respondents in those situations in order to test their sensitivity to privacy and the cost thereof. These scenarios were written to assist in answering the hypotheses that are described in chapter three. In order to test the sensitivity, each scenario tests to see if the respondents' answers to the same questions change, dependent on the discount being offered.

The use of scenarios in empirical research has been found to be effective in evaluating ethical market behaviour as well as in e-commerce research (Milne & Bahl, 2010). Scenarios are descriptions of possible futures states (Camponovo, Debetaz, & Pigneur , 2004). Scenarios provide a form or tool to study a possible and plausible future, and to create an awareness of which future applications are possible (Sheng, Nah, & Siau, 2008). Scenarios are commonly used in experimental studies to manipulate different conditions of variables, simulate user tasks, or represent a context for study (Xu & Teo, 2004).

A second scale was used in ten control questions which allowed the creation of a baseline in order to establish the respondents feeling towards privacy.

Secondary research took the form of a detailed literature review performed prior to the quantitative section of the research. This was performed in order to provide context and current thinking regarding the identified research problem (Zikmund, 2003).

The information sources consisted of primarily journal articles that dealt with the research area and allowed a review of the areas of focus around privacy and location based items.

The primary research included a five point Likert scale was used in order to ascertain the respondents' perception/feelings on the scenario presented, with one indicating that the respondent was 'Uncomfortable' and with an answer of five indicating that they were 'Comfortable'. This scale indicated how 'Uncomfortable' / 'Comfortable' the respondent felt in disclosing the information in the question, for the discount that was offered. If they felt that the discount was sufficient for the desired information then they would answer 'Comfortable' likewise if they did not feel comfortable disclosing that information for the offered discount then they would answer 'Uncomfortable'. If their feeling was ambivalent, namely neither 'Comfortable' nor 'Uncomfortable' then they would answer 'Neutral' which would mean that they did not feel strongly about disclosing that information for that discount.

The second scale which was used for the control questions also made use of a five point Likert scale in order to ascertain the perception/feelings on these questions, with one indicating that the respondent 'Strongly Disagreed' with the statement made in the question and with an answer of five indicating that they 'Strongly Agreed' with the statement made in the question. This scale indicated whether the respondent disagreed or agreed with the statements that were made in the control questions.

The literature review highlighted that there is a growing concern around privacy and the fact that consumers have less privacy (Langenderfer & Miyazaki, 2009).

It was also highlighted that consumers are beginning to understand that their privacy is for sale by bartering their information for discounts and special offers (Langenderfer & Miyazaki, 2009). Therefore the dependant variable was privacy / privacy concerns and the comfort level that is felt with regards to these privacy concerns. The independent variables were the variables related to the sub-hypotheses, the perceived discount to product value, the level of intrusion and the nature of the product or service (once-off/ recurring). These were all measured in the questionnaire in order to determine their effects on consumers' privacy responses.

## 4.3. Survey Pilot

The survey was piloted with a group of twelve MBA students, randomly selected from the 2010/2011 MBA class. All members of the pilot group were asked to respond and provide feedback on improvements or questions that were unclear.

This piloted survey, used the paper based version to administer the questions and responses from these twelve respondents. The questionnaire was self-administered, meaning that the respondents were not able to interact personally with the researcher while filling in the questionnaire. Reponses to certain questions are mandatory especially in the demographics section.

A follow up call to each of the twelve respondents was be made to elicit feedback on the structure, ease of use and of the ease of understanding of the questionnaire.

Once the feedback from the pilot was incorporated then the updated questionnaire was be handed out to the 2011/2012 GIBS MBA class to complete.

Again, the questionnaire was self-administered, meaning that the respondents were not able to interact personally with the researcher. The updated questionnaire was also sent out to the 2010/2011 GIBS MBA class and certain technology divisions within EOH (+/- 500 people).

## 4.4. Proposed Population And Unit Of Analysis

### 4.4.1. Population

The population was considered to be any consumer, 25 years and older, that had a mobile device and was or had been a member of the working population. The population did not need to know about LBS as the scenarios described a situation and asked the respondent their reaction based on the situation and their feelings around privacy. The population was limited to the above sample in order to ensure that the scenarios described were relevant to the sample.

### 4.4.2. Unit Of Analysis

Blumberg, Cooper, & Schindler (2008), describe the unit of analysis as indicating the level at which the research is performed and which objects are being researched.

The unit of analysis that this research was investigating is the value of discount required for a consumer to forego privacy concerns around location.

## 4.5. Nature And Size Of The Sample

Xu (2010) mentions that some researchers argue students, by their very nature might limit the generalizability of the results however as the sample was an MBA class it was believed that this issue was minimised as majority of the students studying on an MBA level are likely to be representative of the target population of people with mobile which have LBS functionality. The GIBS MBA classes contained the elements described above that allowed them to be used as part of the sample.

The sample also included the 2010/2011, 2011/2012 GIBS MBA classes and certain technology divisions within EOH (+/- 500 people), which helped ensure that the sample had a diversity of respondents and not only respondents from the same cohort namely MBA students. The total size of these samples combined was in the region of +/-800 respondents. The aim was to receive at least 80 responses which would represent a ten percent response rate which would allow for analysis of the research hypotheses. There were 253 responses that were received however only 211 (+/- 26% response rate) of these were completed questionnaires, which meant that the 42 incomplete questionnaires were discarded. These erroneous questionnaires are discussed below.

The nature of the sample was non-probability based and of a convenience sampling nature. As noted by Blumberg, Cooper, & Schindler (2008) although this method of sampling has no controls to ensure precision it is useful to use this approach to test ideas. The sample size that was included was made as large as possible to attempt to overcome some of the biases that are related to this sampling method.

## 4.6. Data Collection And Data Analysis

A descriptive study has four research methods, namely survey; experiments, secondary data studies, and observations (Blumberg, Cooper, & Schindler, 2008). Surveys attempt to quantify factual information in terms of what, who, where, when, and how (Blumberg, Cooper, & Schindler, 2008). Based on the above it is felt that a survey was the best possible way of collecting the required data for this study.

The pilot survey was performed using the paper based questionnaire instrument and it utilised to gather the responses to the questionnaires from the initial respondents. The pilot questionnaire was distributed to twelve randomly selected GIBS MBA students from the 2010/2011 class, in order to test the questionnaire prior to the actual questionnaire being sent out. This allowed the questionnaire to be tested for sufficiency, relevance, language, sequence and layout, which ensured that most of the issues were picked up before the survey was more widely distributed.

The updated questionnaire was then be printed out and handed out to the 2011/2012 GIBS MBA modular and evening group students for them to complete. This completion process allowed for a higher response rate from the distributed questionnaires however this method highlighted response errors even though a pilot was conducted. These response errors appeared to be related to a misunderstanding of how the questionnaire should have been filled in. These incomplete questionnaires were different to the incomplete online questionnaires as the respondents were comfortable completing the questionnaire but did not complete it correctly whereas the online incomplete questionnaires may have been related to respondents not wanting to divulge their feelings on the subject.

The updated questionnaire was sent out via email to the 2010/2011 GIBS MBA class and the EOH technology divisions identified for them to complete. Reminder emails were sent to those groups to try and improve the response rates for the survey.

Advantages and disadvantages of using self-administered surveys as noted by Blumberg, Cooper, & Schindler (2008) are:

1. Costs: they are less costly than conducting personal interviews
2. Sample accessibility: these surveys allow the researcher to contact respondents who through other methods might not have been available to respond.
3. Careful consideration: they allow the respondent's time to consider their views and answers.
4. Anonymity: this might allow the respondent to answer in a more accurate manner than if they were being interviewed.
5. Topic coverage: a limitation of this method is that these surveys need to be quick and easy to complete and therefore are generally suited to research of a quantitative nature.

6. Non-response error: this is also a limitation of this method as respondents do not feel obliged to respond. This research will reduce the risk around this by having a paper and online self-administered questionnaire which should help with the non-response errors.
7. Non-representative: due to the convenience sampling method, the sample might not be representative of the population.

The data was analysed using the Likert responses to each of the questions in the questionnaire. The data was analysed from a demographic perspective in order to frame the characteristics of the sample. Descriptive statistics was done on the questions where a Likert scale was supplied in order to analyse the results from these questions. These included frequency analysis as well as pie-charts and histograms which will allow the diagrammatical presentation of the results.

The hypotheses listed above were tested by repeated measures Analysis of Variance with fixed factors of discount, intrusion, perceived discount to product. Repeated measures ANOVA is used to analyse the means of measures of the same respondent measured repeatedly, and removes the within person variance from the analysis. The factors are termed fixed rather than random as their levels are the specific levels under investigation rather randomly selected levels.

Repeated measures ANOVA are used when all respondents of a sample are all measured under a number of different situations (Consulting group of the Division of Statistics and Scientific Computing at the University of Texas at

Austin, 1997). As the sample is subjected to each situation in turn, the measurement of the dependent variable is repeated. Using a standard ANOVA in this case is not appropriate because it fails to model the correlation between the repeated measures: the data violate the ANOVA assumption of independence (Consulting group of the Division of Statistics and Scientific Computing at the University of Texas at Austin, 1997).

## 4.7. POTENTIAL RESEARCH LIMITATIONS

The limitations of this research were as follows:

1. Consumers' responses might have been different when asking about a perception/ feeling rather than testing the actual response.
2. The research did not test any perceptions/feelings from the suppliers' point of view.
3. The research did not match the value given away against the product being sold.
4. The research excludes certain age groups and therefore will not be able to infer any relationships between privacy and age for those age groups.
5. The scenarios used may not allow all respondents to clearly articulate their feelings on the personalisation-privacy paradox
6. The sample does not take into account the respondents feelings toward technology namely early adopter vs. laggard.
7. Non-representative: due to the convenience sampling method, the sample might not be representative of the population.

# 5. Results

## 5.1. Introduction

This chapter presents the data collected and the results of the statistical analysis. Some ambiguities were identified during the survey pre-test, which are described together with how they were corrected. The demographic profiles of the respondents are then described. The main results of the research is then presented and described. The last portion of this section describes the results specifically in respect to the hypotheses in chapter three.

## 5.2. Findings and Correction from the Pilot of the Survey

The survey was piloted with 12 randomly selected 2010/2011 students who were asked to fill in the survey and at the same time suggest improvements. Each of these students filled in the survey from start to finish and then handed it back to the researcher. Each of these students was then asked to suggest ways in which the survey could be improved, both from an aesthetic / flow perspective as well as from a content perspective. There were a number of positive suggestions that were incorporated into the second version of the questionnaire. Some of these were:

1. Comments about length.
2. Guidance in terms of the discount structures.
3. Layout of the discount structures.

The second version of the questionnaire was then distributed, in paper form, to the EOH division within which the researcher worked. There were a number of responses received and while reviewing the responses, the researcher discovered another issue with the questionnaire. This issue was around the confusion that respondents did not understand that they were required to provide an answer on each discount and not only on one of them. The questionnaire was enhanced to ensure that the answer requirements were clearly spelt out for each question to ensure that there was no further confusion.

All of the responses linked to version two of the questionnaire were discarded in order to ensure that the results only contained data collected from respondents who answered the third version of the questionnaire.

This third version of the questionnaire was the version that was used to collect all the data that is presented below. This version was used for both the paper based and online version of the survey.

## 5.3. RESPONDENTS / SAMPLE DESCRIPTION

The sample group as defined in chapter four was the various MBA classes, both the 2010/2011 classes as well as the 2011/2012 classes. The survey was also sent out to various technology divisions within EOH. The respective head of these divisions were sent a mail requesting whether they would be comfortable with their staff completing the survey and if they were they were then asked to forward the mail to these employees. The mail was sent to five technology divisions within EOH, each of those divisional heads were comfortable with the survey and forwarded it onto their staff. For this reason it is difficult to ascertain the exact number of people that received the survey however it is estimated that in the region of 500 people received the email in this manner.

Together with this, an email was sent by each of the programme managers for the different MBA programmes at the Gordon Institute of Business Science (GIBS) to all the 2010/2011 and all the 2011/2012 students. This mean this batch would have gone to in the region of a further 400 people. In an attempt to improve response rates the researcher took paper versions of the questionnaire and visited the 2011/2012 students just after they had finished a lecture. This meant that the response rate on these were higher as there was an immediate call to action for the respondent to complete the questionnaire.

In the region of 800 people received the questionnaire, with 253 (+/-31.6%) people responding to the questionnaire. However of these 253 only 211 had all the questions completed. The 211 represents an approximate response rate of +/- 26.3%. The paper based questionnaires were captured into the online survey by the researcher. All the results were then downloaded and these results were given to a qualified statistician, in order for them to clean & analyse the data.

## 5.4. Demographic Data (All Scenarios)

This section shows all the demographic data from the questionnaire, which allows some further analysis of how certain demographical groups behave with regards to privacy.

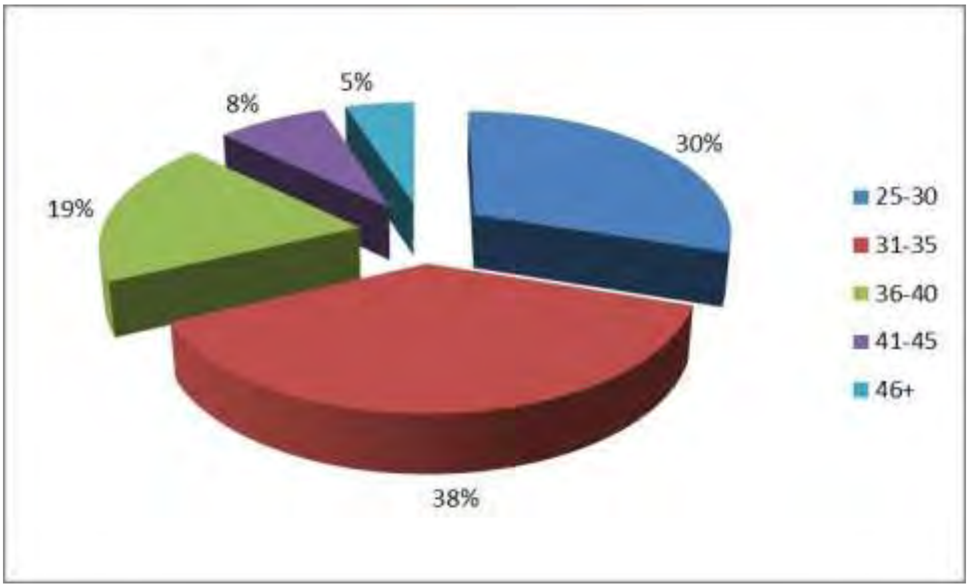
### 5.4.1. Gender Distribution

The gender distribution of the respondents who completed the questionnaire showed that the number of males who completed the survey was more than double that of females and actually made up +/-68% of the respondents.

### 5.4.2. Age Distribution

The age distribution of the respondents can be seen below. More than two-thirds of the respondents were below 35 (68%). Although age was not brought into any of the hypotheses, it is important to note that the younger generation has had more exposure to LBS which could have an influence on the results and perceptions of these respondents. Another observation is that the younger generation are more generally more comfortable with technology and mobile commerce.

FIGURE 3: AGE DISTRIBUTION



### 5.4.3. LANGUAGES DISTRIBUTION

The predominant language was English which would mean that the questionnaire and content was relatively well understood.

### 5.4.4. EMPLOYMENT STATUS DISTRIBUTION

The majority of the respondents were employed on a full time basis. The employment status was not included in the hypotheses but it offers an area of discussion around whether the employment status might influence the need or desire to take up a discount more willingly.

## 5.5. PRIVACY CONTROL QUESTIONS

These are the base questions that will allow the researcher to establish the respondents feeling towards privacy and will also provide a check against whether these questions reveal a different stance on privacy than is shown in the scenarios. The questions below test the respondents' feelings towards privacy and receiving offers with regards to reducing their privacy concerns. As can be seen by looking at the questionnaire, these questions had a five point Likert scale with the scale responses being defined as:

1. Strongly Disagree
2. Disagree
3. Neutral
4. Agree
5. Strongly Agree

### 5.5.1. DESCRIPTIVE STATISTICS: DESCRIPTION

The descriptive statistics of the ten questions provides some interesting data in understanding where the average responses were. When looking at the means it is important to keep the Likert scale in mind, which was defined from one to five, with one being 'Strongly Disagree' and five being 'Strongly Agree'. As can be seen from the table below question one 'I am concerned with privacy' had a mean of 4.19 which meant that the average of the respondents was that they

'Agreed' with this statement, this obviously shows that the respondents are concerned with privacy.

The next highest question was question two 'I value my privacy above all else' which had a mean of 3.92, which indicates that the average response for this question was very close to 'Agree', which reinforces the findings in question one.

The 3rd highest average was question four 'I care if someone knows where I am', which further reinforces that the respondents are concerned with their privacy and who has access to their information. This question had a mean of 3.74 which indicates that the average response was close to being that the respondents 'Agreed' with this statement.

The three questions that had the lowest averages and therefore were closet to 'Strongly Disagree' were questions six, nine and three. Question six 'I will be comfortable with anyone knowing my location' which had a mean of 1.69 and therefore was closet to 'Strongly Disagree'. This was not out of the ordinary as this question did not have any restrictions in terms of who was able to know the respondents location. This does however reinforce that there is a strong concern around privacy when it is not controlled or limited.

The next question closet to the bottom of the scale was question nine 'No relevant offer would entice me to give up private information', which had a mean of 2.77, which meant that the average of the respondents was to disagree with this statement, which highlights that the respondents, on average, felt that a relevant offer could entice them to give up some of their private info.

The third lowest average was from question three ‘I will give up some private information for the right offer’ where the mean was 3.18 which shows that the respondents on average had a ‘Neutral’ feeling towards this question which means that the respondents could possibly be swayed either way depending on the offer that was put forward and the private information that was requested.

Questions five (I only want my friends to know where I am), seven (The offer is only valuable to me if it is relevant at that moment in time), eight (I will only relinquish my data if the offer is valuable in a relevance sense) and ten (The amount of value will influence how much data I will share) are the four middle most questions with each having means of 3.6, 3.59, 3.59 and 3.43 respectively. This shows for questions five, seven and eight that the respondents felt closer to agreeing with those questions than having a neutral feeling, whilst with question ten they felt closer to neutral than agreeing with the question. The mostly positive responses show that the respondents feel that they are willing to barter with their privacy in order to receive benefits.

This should indicate that in the scenario based questions the respondents should be more comfortable sharing information when the discount amounts increase.

### 5.5.2. DESCRIPTIVE STATISTICS: TABLE WITH RESULTS

TABLE 1: DESCRIPTIVE STATISTICS ON ALL QUESTIONS

| Question | Mean | Median | Mode | Std.Dev. |
|---|---|---|---|---|
| 1. I am concerned with privacy | 4.19 | 4 | 4 | 0.80 |
| 2. I value my privacy above all else | 3.92 | 4 | 4 | 0.91 |
| 3. I will give up some private information for the right offer | 3.18 | 4 | 4 | 1.02 |
| 4. I care if someone knows where I am | 3.75 | 4 | 4 | 0.98 |
| 5. I only want my friends to know where I am | 3.60 | 4 | 4 | 1.08 |
| 6. I will be comfortable with anyone knowing my location | 1.69 | 2 | 1 | 0.85 |
| 7. The offer is only valuable to me if it is relevant at that moment in time | 3.59 | 4 | 4 | 1.06 |
| 8. I will only relinquish my data if the offer is valuable in a relevance sense | 3.59 | 4 | 4 | 1.00 |
| 9. No relevant offer would entice me to give up private information | 2.77 | 2 | 2 | 1.02 |
| 10. The amount of value will influence how much data I will share | 3.43 | 4 | 4 | 1.11 |

## 5.6. DATA STRUCTURE AND HYPOTHESES

The structure of the second half of the questionnaire is described as follows:

- the three different scenarios representing the product value or scenario effect
- four different intrusion levels representing the intrusion effect
  - In the case of scenarios one and two, intrusion was composed of the two factors of active and consolidated, with two levels each. The active tracking was where the respondent was 'tracked' outside of the location namely a wider radius while the passive tracking was a confined radius. The other factor was whether the respondent's information was consolidated with other consumers' information.
- five different discount amounts representing the discount offered effect

These completely crossed factors yielded (3 x 4 x 5 = 60) treatment combinations.

The respondents were required to indicate how comfortable they felt for each treatment combination. Each of these scenarios was crafted in an attempt to answer the hypotheses which were presented in chapter three. These have been repeated below and are as follows:

H1A: The purchase price of the product / service influences the decision around forgoing privacy irrespective of the offer being made: if the purchase price is low namely less than R500 then irrespective of the offer being made (50% discount), the consumer would be less inclined to reduce their privacy concerns around location.

This hypothesis was directly linked with the first scenario in the questionnaire, where a small value once off purchase was being made and the comfort level of tracking were explored for each of the discount levels.

H1B: The quantum of the offer affects the amount of location data given: if the offer has significant value then consumers' would be prepared to disclose significant information to receive the value / offer.

This hypothesis was directly linked with the second scenario in the questionnaire, where a high value once off purchase was being made and the comfort level of tracking were explored for each of the discount levels

H1C: Benefits that are received on an on-going basis will cause more location information to be disclosed than a once off benefit at time of purchase: if the offer that is made makes provision for recurring benefits, the consumer would agree to more location information disclosure than if the benefit was a once off benefit.

This hypothesis was directly linked with the third scenario in the questionnaire, where a small value recurring purchase was being made and the comfort level of tracking were explored for each of the discount levels

In presenting the results, the intrusion levels have been re-ordered from the questionnaire in order for the levels to flow from least intrusive to most intrusive. In the questionnaire the levels were ordered as follows:

1. Least intrusive (Level 1)
2. 2nd Most intrusive (Level 3)
3. 2nd Least intrusive (Level 2)
4. Most intrusive (Level 4)

They were therefore re-ordered as follows:

1. Least intrusive (Level 1)
2. 2nd Least intrusive (Level 2)
3. 2nd Most intrusive (Level 3)
4. Most intrusive (Level 4)

This logical error/ anomaly in the design was found after analysing the data and was related to whether that question for that level referred to the data as being consolidated or not.

Whilst examining the data it was found that the intrusion levels were the same for scenarios one and two however it differed slightly for scenario three. This meant that in scenario one and two the questionnaire referred to the data either being consolidated or not consolidated. Scenario three did not refer to consolidation of data, which meant that scenario three's results were slightly different to that of the other two scenarios.

However the data was further analysed by looking at scenarios one and two to see if the 'consolidation' of data, which is referred to as either 'active' or 'passive' monitoring influenced the respondents' feelings about the scenario at all.

The results of the research are presented in line with the hypotheses previously stated. The operationalised version of each hypothesis is re-stated and the results of the repeated measures analyses are presented with their supporting graphs.

It should be noted in the Analysis Of Variance (ANOVA) tables shown in each of the sub hypotheses (1A-1C) that all the interaction effects of the variables are statistically significant. This reconfirms the interrelation of these variables and the fact that although the main effects might be significant, the fact that all the interaction effects are significant overrides the fact that the main effect is or is not significant.

### 5.6.1. Hypothesis 1: The Discount Main Effect

Hypothesis 1 is operationalised as follows: Consumers express higher levels of comfort with disclosing their location information as the discount offered on their purchase is increased.

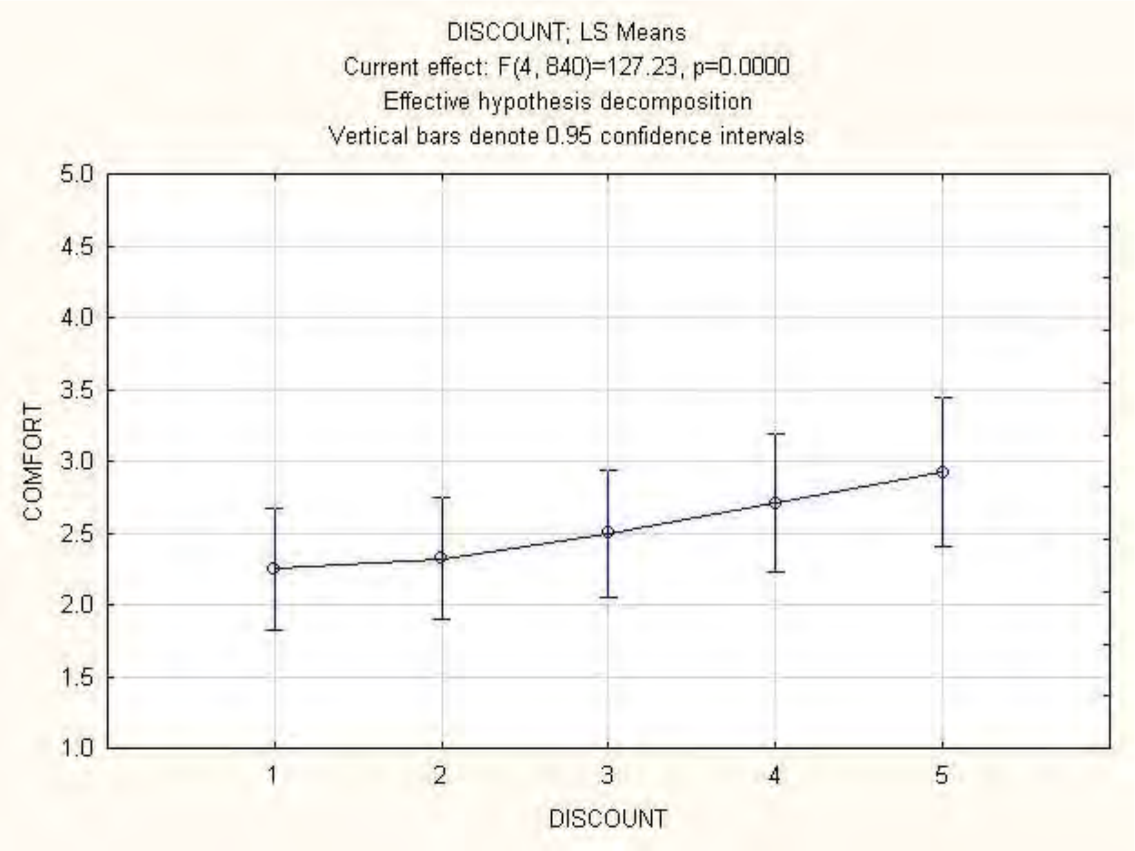
The main effect of discount is significant (F (4,840) = 127.227, p<0.001) as shown by the repeated measures ANOVA with the main effects of scenario, intrusion and discount, and their first and second-order interactions. This result implies a difference in the mean comfort levels dependent on discount.

Moreover, based on the values of the mean comfort levels in the four discount levels (with the effects of scenario and intrusion level held constant, it is observed that comfort levels increase monotonically with increasing discount (**Figure 4: H1 – Discount Main Effect** ).

The figure below shows the increase in comfort level as the discount offered increases from one (5%) to five (40%). These changes are statistically significant as can be seen by the p value being less than 0.001. This confirms that the respondents comfortableness with disclosing more info increased as the levels of discount increased.

The increase in comfort level is independent of scenario and intrusion level.

FIGURE 4: H1 – DISCOUNT MAIN EFFECT – FOR ALL SCENARIOS



The Scheffe post hoc analysis reveals significant increases in comfort with increases in discount levels, except between the first two levels of discount (see Scheffe Appendix on pg. 127).

It is important to note that although the comfort level increases with each discount offered, the means is consistently below the scale midpoint of three ('Neutral' comfort level), which implies that although the respondents became more comfortable with each additional discount, they never reach a level where they were feeling even 'Slightly Uncomfortable'.

TABLE 2: H1 – DISCOUNT MAIN EFFECT –ANOVA

| | SS | df | MS | F | p |
|---|---|---|---|---|---|
| Intercept | 81614.28 | 1 | 81614.28 | 1595.564 | 0.000000 |
| Error | 10741.66 | 210 | 51.15 | | |
| SCENARIO | 85.84 | 2 | 42.92 | 2.856 | 0.058638 |
| Error | 6312.53 | 420 | 15.03 | | |
| INTRUSION | 1993.22 | 3 | 664.41 | 182.675 | 0.000000 |
| Error | 2291.38 | 630 | 3.64 | | |
| **DISCOUNT** | **783.69** | **4** | **195.92** | **127.227** | **0.000000** |
| **Error** | **1293.55** | **840** | **1.54** | | |
| SCENARIO*INTRUSION | 736.45 | 6 | 122.74 | 54.551 | 0.000000 |
| Error | 2835.05 | 1260 | 2.25 | | |
| SCENARIO*DISCOUNT | 31.79 | 8 | 3.97 | 8.412 | 0.000000 |
| Error | 793.67 | 1680 | 0.47 | | |
| INTRUSION*DISCOUNT | 10.68 | 12 | 0.89 | 7.171 | 0.000000 |
| Error | 312.88 | 2520 | 0.12 | | |
| SCENARIO*INTRUSION*DISCOUNT | 4.42 | 24 | 0.18 | 1.544 | 0.043736 |
| Error | 600.92 | 5040 | 0.12 | | |

### 5.6.2. CONCLUSION: HYPOTHESIS 1 – THE DISCOUNT MAIN EFFECT

There is significant support for Hypothesis 1, with comfort levels increasing monotonically with increasing discount. Moreover, the increases in comfort level are significant with increasing discount levels, except between the first two levels of discount. The levels of comfort are however low (below the ‘Neutral’ position of comfort) with the highest comfort level being below ‘Neutral’ or 3, even at highest discount rates of 40% off the purchase price.

### 5.6.3. HYPOTHESIS 1A: THE SCENARIO*DISCOUNT INTERACTION EFFECT

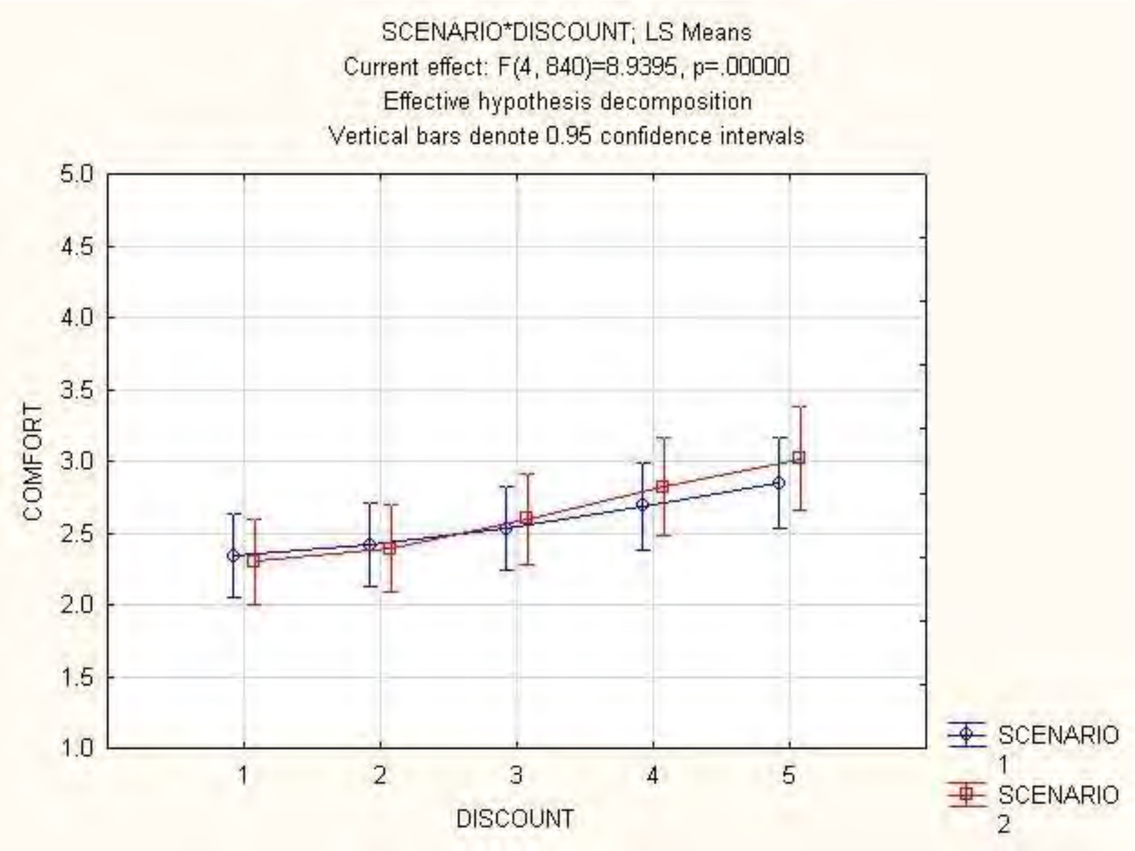
Hypothesis 1A is operationalised as follows: Consumers express higher levels of comfort with disclosing their location information as the discount offered on purchases is increased for high priced items only, but remain the same for low priced items. This hypothesis relates to the first two scenarios only.

TABLE 3: H1A – SCENARIO*DISCOUNT INTERACTION EFFECT – ANOVA

| | SS | df | MS | F | p |
|---|---|---|---|---|---|
| Intercept | 56815.45 | 1 | 56815.45 | 1537.017 | 0.000000 |
| Error | 7762.6 | 210 | 36.96 | | |
| SCENARIO | 7.76 | 1 | 7.76 | 0.752 | 0.386876 |
| Error | 2168.79 | 210 | 10.33 | | |
| INTRUSION | 2627.52 | 3 | 875.84 | 178.567 | 0.000000 |
| Error | 3090.03 | 630 | 4.9 | | |
| DISCOUNT | 426.71 | 4 | 106.68 | 103.745 | 0.000000 |
| Error | 863.74 | 840 | 1.03 | | |
| SCENARIO*INTRUSION | 78.38 | 3 | 26.13 | 10.762 | 0.000001 |
| Error | 1529.47 | 630 | 2.43 | | |
| **SCENARIO*DISCOUNT** | **15.15** | **4** | **3.79** | **8.939** | **0.000000** |
| **Error** | **355.8** | **840** | **0.42** | | |
| INTRUSION*DISCOUNT | 8.95 | 12 | 0.75 | 4.541 | 0.000000 |
| Error | 414 | 2520 | 0.16 | | |
| SCENARIO*INTRUSION*DISCOUNT | 2.89 | 12 | 0.24 | 1.783 | 0.045471 |
| Error | 340.76 | 2520 | 0.14 | | |

Based on the results of Table 3:, the first order interaction effect scenario*discount is significant (F(4,840) = 8.939, p<0.001)). This result implies that the pattern of the mean comfort levels for the different levels of discount is dependent on whether the item price is low (scenario one) versus high (scenario two). The following figure illustrates the interaction effect.

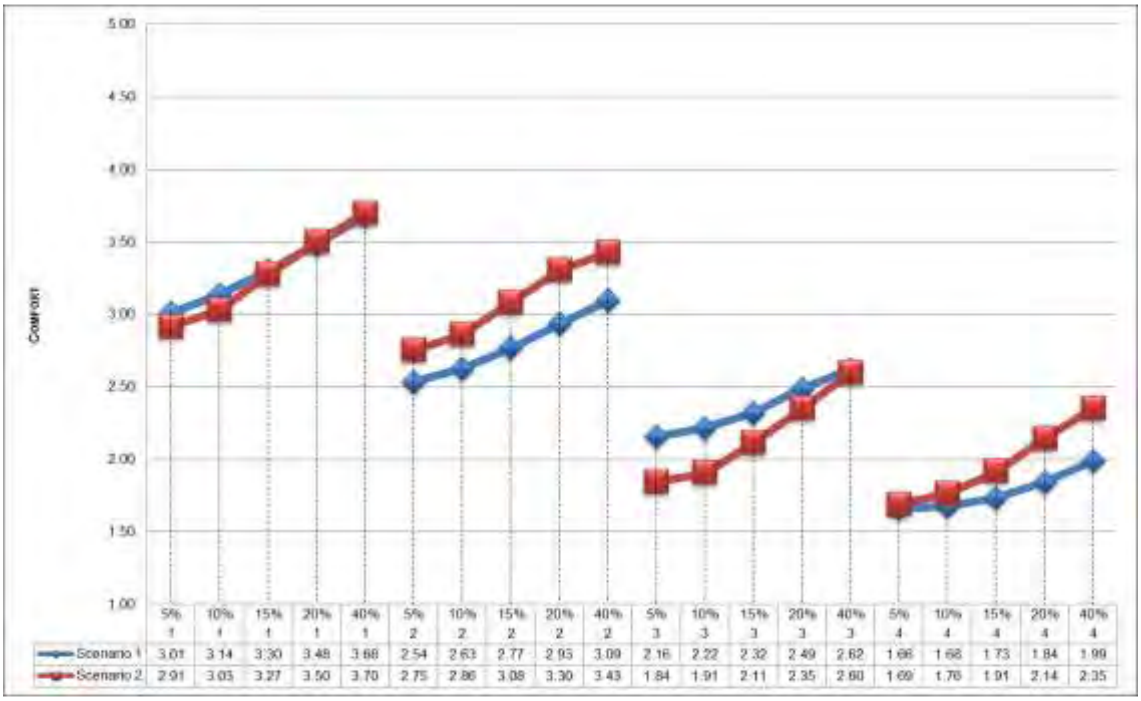
Figure 5: H1a – Scenario*Discount Interaction Effect – Scenario One And Two



The pattern of the mean comfort levels shows that for higher priced items (scenario two), comfort levels increase at a greater rate with increasing discount levels, than for lower priced items (scenario one). The post hoc Scheffe test shows no significant difference in means from discount levels one to two for either scenario, and no significant difference from discount levels two to three for scenario one only. Although all the other differences in comfort levels are significant for both scenarios, the differences are more noticeable for scenario two than for scenario one, implying greater increases in the case of higher priced items than lower priced items. It would appear that this interaction effect is primarily described by the ‘No interaction’ type of interaction, as the lines that describe the interactions are primarily parallel with one another. However at when the discount offered increases from level two to level three then the type of interaction appears to be of an 'ordinal interaction' nature.

It should be noted that only for scenario two with the highest level of discount (40%) does the mean comfort level climb higher (though marginally so) than the neutral scale midpoint of three, implying that the respondents no longer experience an 'Uncomfortable' comfort level for this treatment combination.

FIGURE 6: H1A – SCENARIO*DISCOUNT INTERACTION EFFECT – MEAN COMFORT



| | 5%<br>1 | 10%<br>1 | 15%<br>1 | 20%<br>1 | 40%<br>1 | 5%<br>2 | 10%<br>2 | 15%<br>2 | 20%<br>2 | 40%<br>2 | 5%<br>3 | 10%<br>3 | 15%<br>3 | 20%<br>3 | 40%<br>3 | 5%<br>4 | 10%<br>4 | 15%<br>4 | 20%<br>4 | 40%<br>4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Scenario 1 | 3.01 | 3.14 | 3.30 | 3.48 | 3.68 | 2.54 | 2.63 | 2.77 | 2.93 | 3.09 | 2.16 | 2.22 | 2.32 | 2.49 | 2.62 | 1.66 | 1.68 | 1.73 | 1.84 | 1.99 |
| Scenario 2 | 2.91 | 3.03 | 3.27 | 3.50 | 3.70 | 2.75 | 2.86 | 3.08 | 3.30 | 3.43 | 1.84 | 1.91 | 2.11 | 2.35 | 2.60 | 1.69 | 1.76 | 1.91 | 2.14 | 2.35 |

### 5.6.4. CONCLUSION: HYPOTHESIS 1A – THE SCENARIO*DISCOUNT INTERACTION EFFECT

There is partial support for Hypothesis 1A as the rate of increase in comfort levels tends to be greater with greater discount for higher priced items than for lower priced items, with the difference is apparent from discount levels two and higher. Comfort levels are starting to rise beyond the scale midpoint

### 5.6.5. Hypothesis 1B: The Scenario*Intrusion Interaction Effect

Hypothesis 1B is operationalised as follows: Consumers express higher levels of comfort with disclosing increasing amounts of identifying information when the perceived value of the discount offered relative to product value is increased.

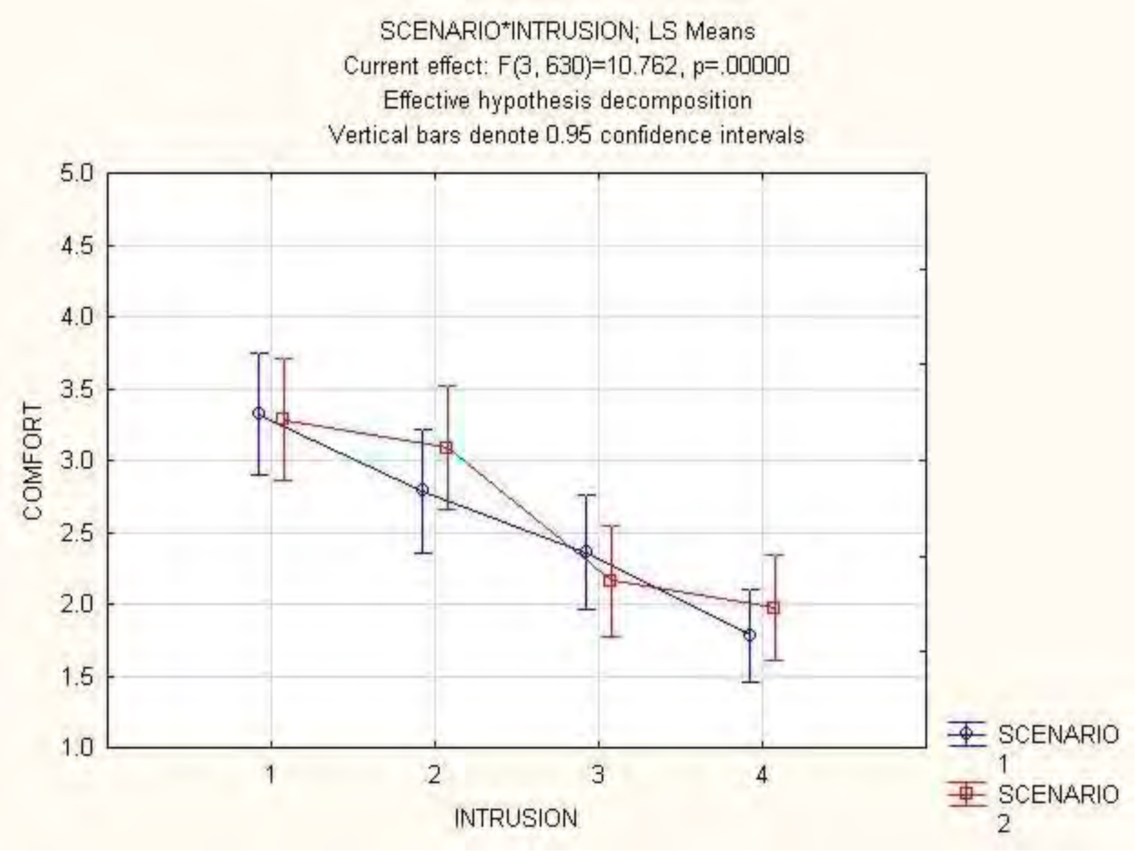
Table 4: H1b – Scenario*Intrusion Interaction Effect – Anova

| | SS | df | MS | F | P |
|---|---|---|---|---|---|
| Intercept | 56815.45 | 1 | 56815.45 | 1537.017 | 0.000000 |
| Error | 7762.60 | 210 | 36.96 | | |
| SCENARIO | 7.76 | 1 | 7.76 | 0.752 | 0.386876 |
| Error | 2168.79 | 210 | 10.33 | | |
| INTRUSION | 2627.52 | 3 | 875.84 | 178.567 | 0.000000 |
| Error | 3090.03 | 630 | 4.90 | | |
| DISCOUNT | 426.71 | 4 | 106.68 | 103.745 | 0.000000 |
| Error | 863.74 | 840 | 1.03 | | |
| **SCENARIO*INTRUSION** | **78.38** | **3** | **26.13** | **10.762** | **0.000001** |
| **Error** | **1529.47** | **630** | **2.43** | | |
| SCENARIO*DISCOUNT | 15.15 | 4 | 3.79 | 8.939 | 0.000000 |
| Error | 355.80 | 840 | 0.42 | | |
| INTRUSION*DISCOUNT | 8.95 | 12 | 0.75 | 4.541 | 0.000000 |
| Error | 414.00 | 2520 | 0.16 | | |
| SCENARIO*INTRUSION*DISCOUNT | 2.89 | 12 | 0.24 | 1.783 | 0.045471 |
| Error | 340.76 | 2520 | 0.14 | | |

The figure below shows the results from the respondents when examining the comfort level of the respondents against the intrusion level for the two different scenarios. As can be seen by the p value of less than 0.00000, these differences are statistically significant.

When the intrusion is the least intrusive, the comfort levels for scenarios one and two are above 'Neutral' which shows that the respondents do not have a tendency towards feeling either comfortable or uncomfortable about the information that they are disclosing. However as the intrusion level increases, the comfort level decreases for each of the scenarios. For each scenario this rate of change is different, with scenario one decreasing at a uniform rate from being above 'Neutral' for intrusion level one to being lower than 'Slightly Uncomfortable' at intrusion level four. In scenario two, it can clearly be seen that intrusion level one and level two are viewed in a similar way by the respondents as the comfort level is above 'Neutral' for both these intrusion levels, when the intrusion moves to level three then the comfort level drops drastically to close to 'Slightly Uncomfortable', which shows that this intrusion level is viewed seriously by the respondents.

FIGURE 7: H1B – SCENARIO*INTRUSION INTERACTION EFFECT – SCENARIO ONE AND TWO



There is a difference in the pattern there is some evidence that the respondents are have more comfort when the intrusion levels increase esp. two and four. They seem to be tolerating the intrusion levels between level one and two in scenario two whereas in scenario one there is a constant drop. It would appear that this interaction effect is primarily described by the ‘ordinal interaction’ type of interaction, as the lines that describe the interactions are not constant for the effect of each treatment and therefore are not parallel with one another.

### 5.6.6. Conclusion: Hypothesis 1B – The Scenario*Intrusion Interaction Effect

There is appears to be significant support for Hypothesis 1B as the rate of decrease in comfort levels tends to be greater with each higher intrusion level that takes place for scenario one where the quantum of the offer is smaller. It can be seen that the respondents tolerate more intrusion for scenario two.

### 5.6.7. Hypothesis 1C: Scenario Main Effect For Scenarios One Vs. Three

Hypothesis 1C is operationalised as follows: Consumers express higher levels of comfort with disclosing their location information for benefits that are received on an on-going basis than for a once off benefit at time of purchase.

To test this effect, only scenarios one and three were compared and the main effect of scenarios is tested. This was done as scenario one looked at a once off purchase and benefit while scenario three looked at a recurring monthly benefit.

TABLE 5: H1C – SCENARIO MAIN EFFECT – ANOVA

| | SS | df | MS | F | p |
|---|---|---|---|---|---|
| Intercept | 52585.13 | 1 | 52585.13 | 1395.819 | 0.000000 |
| Error | 7911.4 | 210 | 37.67 | | |
| **SCENARIO** | **39.17** | **1** | **39.17** | **2.2** | **0.139523** |
| **Error** | **3739.55** | **210** | **17.81** | | |
| INTRUSION | 865.76 | 3 | 288.59 | 112.617 | 0.000000 |
| Error | 1614.41 | 630 | 2.56 | | |
| DISCOUNT | 486.7 | 4 | 121.67 | 109.586 | 0.000000 |
| Error | 932.65 | 840 | 1.11 | | |
| SCENARIO*INTRUSION | 507.79 | 3 | 169.26 | 69.982 | 0.000000 |
| Error | 1523.78 | 630 | 2.42 | | |
| SCENARIO*DISCOUNT | 28.41 | 4 | 7.1 | 12.566 | 0.000000 |
| Error | 474.74 | 840 | 0.57 | | |
| INTRUSION*DISCOUNT | 10.77 | 12 | 0.9 | 7.599 | 0.000000 |
| Error | 297.68 | 2520 | 0.12 | | |
| SCENARIO*INTRUSION*DISCOUNT | 1.32 | 12 | 0.11 | 0.973 | 0.472825 |
| Error | 285.73 | 2520 | 0.11 | | |

It can be seen in **Figure 8** below that there is not a significant difference in comfort levels between the two scenarios. The comfort level for scenario one was just over 2.5 while the level was just under 2.5 for scenario three.

FIGURE 8: H1C – SCENARIO MAIN EFFECT – SCENARIO ONE AND TWO

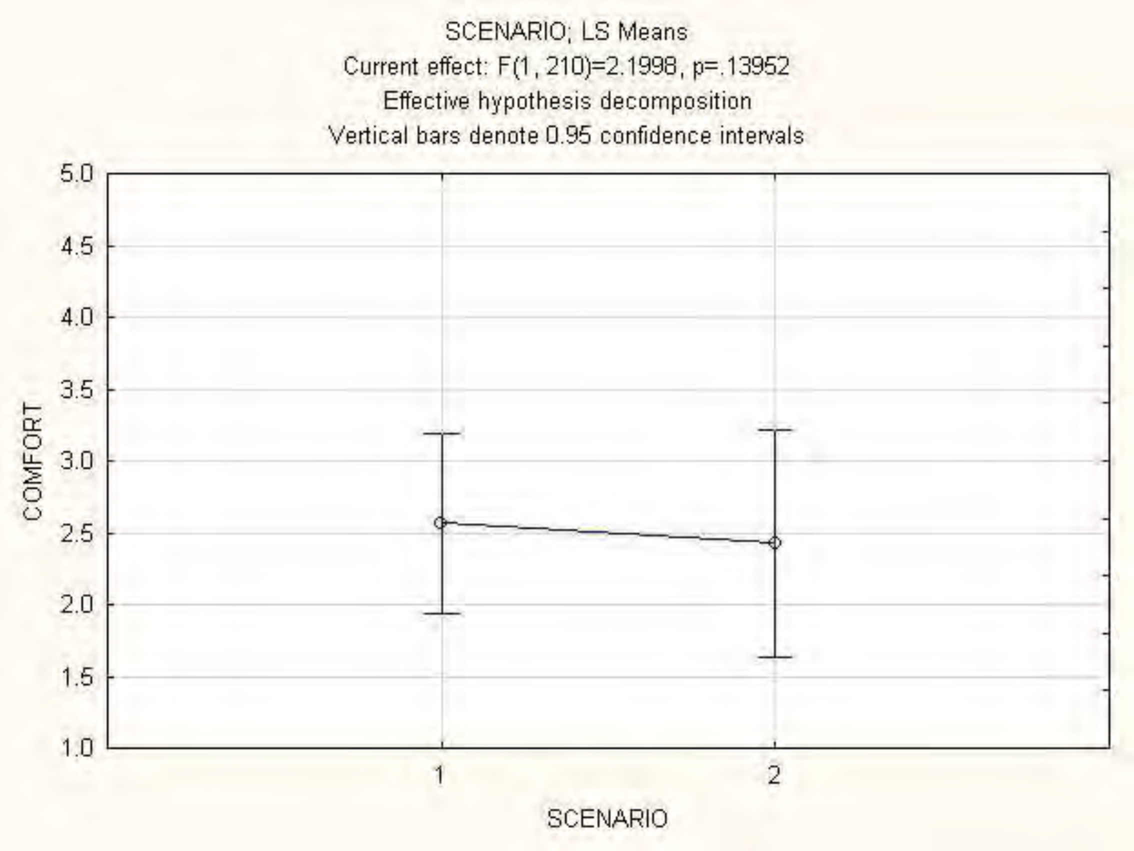
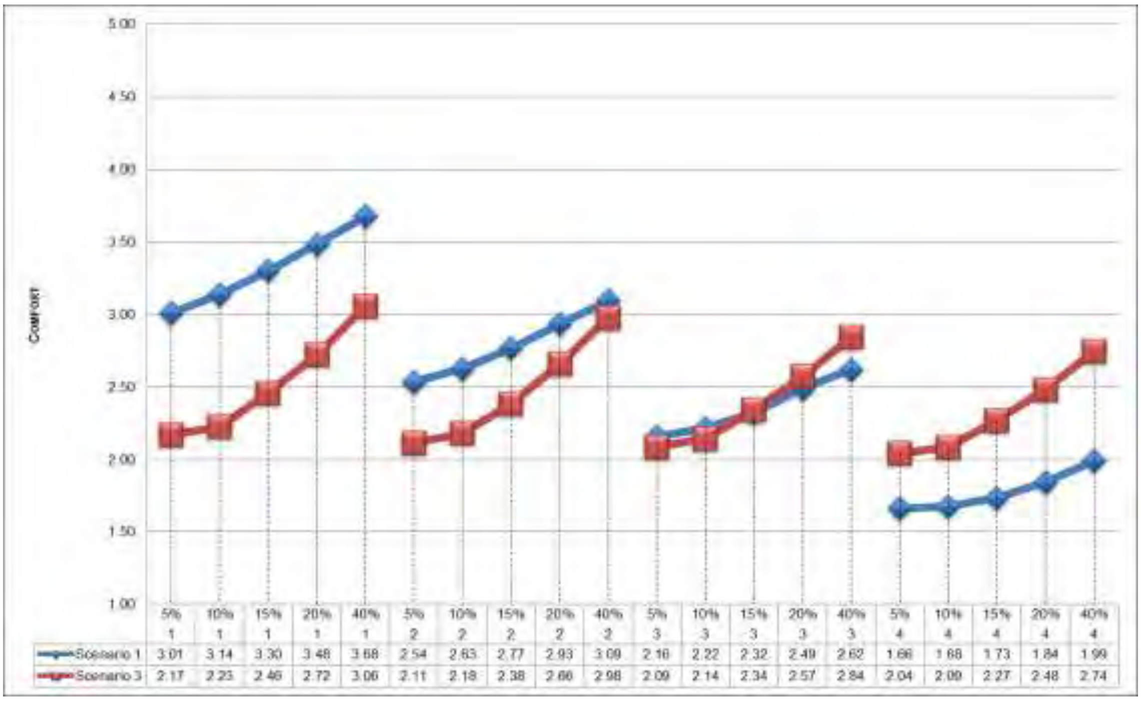


Figure 9: H1C – Scenario Main Effect – Mean Comfort



| | 5%<br>1 | 10%<br>1 | 15%<br>1 | 20%<br>1 | 40%<br>1 | 5%<br>2 | 10%<br>2 | 15%<br>2 | 20%<br>2 | 40%<br>2 | 5%<br>3 | 10%<br>3 | 15%<br>3 | 20%<br>3 | 40%<br>3 | 5%<br>4 | 10%<br>4 | 15%<br>4 | 20%<br>4 | 40%<br>4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Scenario 1 | 3.01 | 3.14 | 3.30 | 3.48 | 3.68 | 2.54 | 2.63 | 2.77 | 2.93 | 3.09 | 2.16 | 2.22 | 2.32 | 2.49 | 2.62 | 1.66 | 1.68 | 1.73 | 1.84 | 1.99 |
| Scenario 3 | 2.17 | 2.23 | 2.46 | 2.72 | 3.06 | 2.11 | 2.18 | 2.38 | 2.66 | 2.98 | 2.09 | 2.14 | 2.34 | 2.57 | 2.84 | 2.04 | 2.09 | 2.27 | 2.48 | 2.74 |

### 5.6.8. Conclusion: Hypothesis 1C – Scenario Main Effect For Scenarios One Vs. Three

There appears to be no support for Hypothesis 1C as there were no significant difference in comfort levels were found ((F(1.210) = 2.2, p>0.05). therefore the respondents appeared to have felt that a recurring benefit was not more significant than a once off benefit. However again it should be noted that the interaction effects are all significant which overrides the fact that the 'scenario' main effect is not significant.

# 6. DISCUSSION OF THE RESULTS

## 6.1. INTRODUCTION

This chapter discusses in detail the research findings outlined in chapter five. The findings from chapter five are then evaluated against the literature that was found and discussed in chapter two. This chapter uses the research hypotheses to give structure to the discussion. The questionnaire provided a tremendous amount of data that will be used in the discussion and which allowed the acceptance or rejection of the hypotheses, there was some data and analysis that was available but was not used as the data did not relate to any specific hypotheses. In the questionnaire, there was a section that had ten general privacy questions and these will be used in the discussions for each separate hypothesis.

## 6.2. RESEARCH HYPOTHESES 1

There was one main research hypotheses that was created which was then broken down into three sub hypotheses. The main research hypothesis was stated as follows:

> Privacy concerns around location awareness in mobile commerce reduce as the consumer benefit increases in actual and perceived value: if consumers' are made an offer of value for a product that they are interested in, they will forego their privacy concerns in order

to receive the value. This means that they would be prepared to disclose their location in order to recognise the value.

The aim of this hypothesis was to determine whether the consumers' privacy can be bought by making them an offer which is of sufficient benefit that they forego their privacy concerns. As mentioned by Xu (2009), due to the fact that more personal data is being stored and used, people's concerns over privacy are rising and therefore there is a need to try and overcome these concerns.
As argued by Altman (1977), privacy is about achieving the balance required to maintain a private life whilst at the same time allowing the person to interact and maintain a social persona. This would agree with the thought that people are able to find a balance where they would be willing to forego privacy to allow this social persona interaction and maintenance.

As can be seen in the questions shown in section 5.5, the respondents are concerned with privacy but do not value it above everything else which could intimate that their feelings could be influenced. It was found that the respondents were open to foregoing privacy if the offer was the right one and depending on the offer will depend on how much data they share. It is clearly shown that the respondents have a definite feeling about which means that they care about who has access to their location data. The findings in the privacy / location questions are consistent with what Culnan (1993) found as to when people start to feel uncomfortable with the information being stored about them.

Although this hypothesis was not tested for directly in the questionnaire, the scenarios were aimed at testing the sub hypotheses, as can be seen in **Figure 4** and **Table 2** the discount effect is significant for all scenarios and intrusion levels which shows that the offering of increased discount irrespective of the scenarios or the intrusion level caused the respondents to forego some of their privacy concerns. **Table 2** shows the ANOVA results from the repeated measures for the discount effect, which shows that the discount effect is significant. This makes logical sense because one would expect with increasing benefits that the respondents' comfort level increased, as generally nothing is ever for free. This is in line with findings of Xu, Teo, Tan, & Agarwal (2009) who found that due to the privacy calculus effect, individuals are willing to forego some of their privacy concerns as long as they receive value in return.

The Scheffe results (as shown in the Appendix: **Hypothesis 1**) clearly show that except for between discount offered one and discount offered two all the other results are significant which illustrates that there is a significant interaction between the different discount offered levels.

This would appear to start to illustrate that the respondents privacy does have a price however it is poignant to note that although the comfort level increases significantly, the comfort level never rises above the middle point of three or 'Neutral'. This shows that although the comfort levels increase as the discount offered increases, the respondents never have a neutral feeling of comfort with regards to the increased information requested. This shows that although the privacy levels reduce the discount offered is not sufficient to cause the respondents to have a comfortable feeling about the foregoing of privacy. The fact that the respondents could have felt that the information that they had disclosed was vulnerable might be influencing their feelings and ensuring that they never really reach a high enough comfort level (Dinev & Hart, 2004). As identified by Stewart & Segars (2002), the biggest threat to the adoption of these new technologies is information privacy. This may suggest that in order to increase the comfort level of the respondents one needs to make a significant offer (L5 or 40%) and even at this discount, the respondents comfort level is below 'Neutral'. Xu, Teo, Tan, & Agarwal (2009) found that consumers perform a risk-benefit analysis on the situation where privacy information has been requested in order to determine whether the exchange is beneficial. Hann et al (2007) found that consumers are definitely willing to trade some information that they deem as private in order to receive monetary reward in the form of discounts, gift cards and coupons. The findings in this research are therefore in line with the respondents performing the risk-benefit in the scenario and concluding that there is enough benefit for them to be more comfortable with each increase in discount.

This means that we are able to reject the null hypothesis or ***$H_0$*: There is no discount effect on comfort levels** which means that we can accept the alternative hypothesis being ***$H_1$*: There is a discount effect on comfort levels**.

## 6.3. RESEARCH SUB HYPOTHESES 1A

This was the first sub hypothesis which was used to assist in proving or disproving the main research hypothesis stated above. The research hypothesis was stated as follows:

> The purchase price of the product / service influences the decision around forgoing privacy irrespective of the offer being made: if the purchase price is low namely less than R500 then irrespective of the offer being made (50% discount), the consumer would be less inclined to reduce their privacy concerns around location.

This sub hypothesis 1A aimed at testing the whether the purchase price of the product influenced the privacy decisions made by the respondents. In order to do this this hypothesis compared scenario one (low value ticket item) and scenario two (high value ticket item). This would therefore compare a low value ticket item and a high value ticket item in order to see whether the respondent's comfort level responded more significantly to the high ticket item rather than the low ticket item when the discount was increased. Xu, Teo, Tan, & Agarwal, (2009) found that the privacy calculus was applicable and important in a LBS situation due to the fact that it was used by individual's to perform the risk-benefit analysis. It was also proven by Hann et al (2007) that the compensation of the consumer generally assists with creating the perception that there has been benefit for the consumer. It should be noted that as proven by Culnan &

Bies (2003), consumers will exchange information if the benefits exceed the risks, which appears to be the case when one looks at the high value ticket item.

Selected questions from the ten control questions are specifically relevant to this hypothesis. The questions that are believed to be relevant are question three, seven, eight, nine and ten. These questions all established the respondent's feeling towards forgoing privacy for the correct offer, relevance of the offer, the influence relevance has on the foregoing of privacy, the fact that a relevant offer would cause the respondents to forego some privacy concerns and that the amount of information parted with influences how much data is shared.

The last question asks the question in hypothesis 1A without using a scenario to test the responses and it was found that a majority of the respondents (60.66%) either 'Agreed' or 'Strongly Agreed' that the amount of information given is directly related to the amount of value being received. Only +/- 25% of respondents had a negative feeling about this.

As mentioned this hypothesis was tested for by comparing the results from scenario one and scenario two. This was tested by looking at the scenario*discount offered effects. **Figure 5** and **Table 3** show that the 'scenario*discount offered' effect is significant for scenario two versus scenario one, the statistical significance per scenario and discount combination can be seen by looking at the Scheffe table shown in **Table 21**. This clearly shows that for a high value ticket item respondents are more comfortable in sharing location information holding the intrusion levels constant. **Table 3**, shows the ANOVA results from the repeated measures for the scenario*discount effect, which shows that this effect is significant. This result might show that consumers need a substantial reason to forego their privacy concerns. As found by Hann et al (2007) concerns in an online environment were willing to trade off their privacy concerns for a benefit of $49 which equates to roughly R400. This would mean that it is double what is being offered in scenario one and would mean that the item offered in scenario one would be almost free. This gives further weight to the fact that a high value ticket item more private information will be disclosed.

This would appear to illustrate that the respondents believe that unless the offer that is being made in exchange for the relaxation of privacy concerns is substantial, the respondents are not as willing to forego their privacy concerns. This might be explained by the fact that the privacy calculus that was done for scenario one did not result in a risk-benefit result that was higher than the risk-benefit result that the respondents got when it was performed on scenario two. As mentioned above and by Xu (2009), unless consumers believe that the benefits outweighs the risks they will not be willing to share as much information with an organisation, which substantiates the view and findings above. The obvious way that this might be done is by using a high value ticket item instead of a low value ticket item because five percent on R300, 000 is significantly more than five percent on R500. As argued in the literature, bounded rationality might be causing respondents to be blinded by the instant gratification of the immediate benefits without truly evaluating the long term risks. One must however note that although the comfort level increases significantly, the comfort level for scenario two reaches the middle point of three or ‘Neutral’ on the highest discount level (L5 or 40%) but for scenario one it only gets to roughly 2.8. this clearly shows that one needs to offer a large amount of discount on a high value ticket item in order for the respondent to reach a ‘Neutral’ comfort level in terms of the privacy exchanged. It has been identified that the mobile service providers need to assist with the elimination of the consumers’ fears around privacy when it comes to LBS. This might explain why the comfort level is never at a level that is higher than ‘Neutral’ (Zhou, 2011). The increase in comfort level with the high value ticket item may be explained by the fact that consumers understand that there is tremendous value in receiving personalised and relevant offers. This value reinforces their purchasing desire against their privacy concerns around sharing information (Xu, Luo, Carroll, & Rosson, 2011). Langenderfer & Miyazaki (2009) found that an increasing number of consumers are becoming aware that their privacy is for sale through the trading of their private information for either discounts or special offers. This reinforces the results shown above where the comfort level increases with each subsequent offer.

This means that we are able to reject the null hypothesis or ***$H_0$*: There is no scenario*discount offered effect on comfort levels** which means that we can accept the alternative hypothesis being ***$H_1$*: There is a scenario*discount offered effect on comfort levels**.

## 6.4. RESEARCH SUB HYPOTHESES 1B

This was the second sub hypothesis which was used to assist in proving or disproving the main research hypothesis stated above. The research hypothesis was stated as follows:

> The quantum of the offer affects the amount of location data given: if the offer has significant value then consumers' would be prepared to disclose significant information to receive the value / offer.

This sub hypothesis 1B aimed at testing the whether the size of the offer influenced the privacy decisions made by the respondents. In order to do this this hypothesis compared scenario one (low quantum based on low purchase price) and scenario two (high quantum based on high purchase price). This hypothesis tested the intrusion levels, one through four and compared the comfort level for both of the scenarios in order to see whether the respondent's comfort level decreased more significantly for scenario one (low quantum) than for scenario two (high quantum). This would then allow the research to test whether with each additional intrusion (namely more data required) would the respondents be more comfortable with scenario two than scenario one.

Selected question from the ten control questions are specifically relevant to this hypothesis. The questions that are believed to be relevant are questions three, eight and ten. These questions all established the respondent's feeling towards forgoing privacy for the correct offer, the influence relevance has on the foregoing of privacy and that the amount of information parted with influences how much data is shared.

The last question asks the question in hypothesis 1B without using a scenario to test the responses and it was found that a majority of the respondents (60.66%) either ‘Agreed’ or ‘Strongly Agreed’ that the amount of information given is directly related to the amount of value being received. Only +/- 25% of respondents had a negative feeling about this.

As mentioned this hypothesis was tested for by comparing the results from scenario one and scenario two. This was tested by looking at the scenario*intrusion level effect. **Figure 7** and **Table 4** show that the scenario*intrusion level effect is significant for scenario two versus scenario one, the statistical significance per scenario and discount combination can be seen by looking at the Scheffe table shown in **Table 22**. This clearly shows that the respondents appear to be more comfortable with each increasing intrusion level for scenario two as opposed to scenario one, holding the discount offered constant. **Table 4**, shows the ANOVA results from the repeated measures for the scenario*intrusion level effect, which shows that this effect is significant. This result might show that consumers definitely feel more comfortable disclosing more information when the quantum of the offer is more substantial. Sheng, Fui-Hoon Nah, & Siau (2008), found that the situation strongly influences the consumers’ privacy concerns and the extent to which they are willing to share their private information. They further argued that privacy was a consumer’s perception which was mostly influenced by situational factors. This may explain why the comfort level for respondents changed with each different intrusion level and might also explain why scenario two had less drastic changes between intrusion level's one and two, and, intrusion level's three and four. The respondents could have felt that intrusion level's one and two, were very similar in scenario two which therefore caused only a slight change in comfort level while they felt that intrusion level's one and two, in scenario one were not the same and therefore the drop in comfort level was more severe.

This would appear to illustrate that the respondents believe that unless the offer that is being made in exchange for the relaxation of privacy concerns is substantial, the respondents are prepared to forego their privacy concerns at a different rate than if the offer is not substantial. It has been found that consumers decided whether an activity or activities violated their privacy depending on the outcome of the evaluation of the type of benefit being offered against the personal information being requested (Sheehan & Hoy, 2000). The fact that the comfort levels attained for either scenario are not extremely high might be directly related to the fact that there is a perceived risk that is linked to this technology which may vary depending on the respondents positive or negative experiences (Radin, Calkins, & Predmore, 2007). This may be done by using a high quantum offer instead of a low quantum offer because five percent or R15, 000 (scenario two) is significantly more than five percent or R25 (scenario one). One must however note that the comfort levels decrease quickly with each increased intrusion level for both scenario one and two, however the respondents appear to be less sensitive to the change between intrusion levels one and two, and, three and four for scenario two than for scenario one. This may further illustrate that the quantum overcomes the smaller changes in intrusion levels.

With both scenarios however the comfort levels are not high to start with, for both scenarios and intrusion level one they are around 3.25 and drop down to around two for intrusion level four. These values for the comfort levels could be explained by the fact that the respondents are not applying hyperbolic discounting. This is where the benefits from parting with personal information are enjoyed immediately however the risk associated with this sharing of personal information may be invisible or spread over time (Acquisti, 2004). This appears to not be the case with the respondents of this study where it appears that they are evaluating the risks as and when the scenario, intrusion level and discount offered are presented to them and determining the risks associated with the benefits. The fact that Acquisti (2004) focused on Electronic Commerce could have influenced the findings as the risks with a consumer's personal information are far less apparent than with mobile phones and LBS.

This shows that although the quantum does affect the comfort level with each increase in information requested, the respondents are still not comfortable with the idea of a business or person having access to that information.

This means that we are able to reject the null hypothesis or ***$H_0$*: There is no scenario*intrusion level effect on comfort levels** which means that we can accept the alternative hypothesis being ***$H_1$*: There is a scenario* intrusion level effect on comfort levels**.

## 6.5. Research Sub Hypotheses 1C

This was the third sub hypothesis which was used to assist in proving or disproving the main research hypothesis stated above. The research hypothesis was stated as follows:

> Benefits that are received on an on-going basis will cause more location information to be disclosed than a once off benefit at time of purchase: if the offer that is made makes provision for recurring benefits, the consumer would agree to more location information disclosure than if the benefit was a once off benefit.

This sub hypothesis 1C was aimed at testing the whether the recurring nature of a benefit received will influence a consumer to forego more privacy than if the benefit was once off. In order to do this this hypothesis compared scenario one (once off benefit) and scenario three (recurring benefit). This would therefore compare a once off benefit scenario item and a recurring benefit item in order to see whether the respondent’s comfort level responded more significantly to the recurring benefit item rather than the once off benefit item when the intrusion level and discount are held constant.

Selected question from the ten control questions are specifically relevant to this hypothesis. The questions that are believed to be relevant are question three, eight and ten. These questions all established the respondent’s feeling towards forgoing privacy for the correct offer, the influence relevance has on the foregoing of privacy and that the amount of information parted with influences how much data is shared.

As mentioned this hypothesis was tested for by comparing the results from scenario one and scenario three. This was tested by looking at the scenario effect. **Figure 8** and **Table 5** show that the scenario effect is not significant when comparing scenario one and scenario two., the statistical insignificance per scenario can be seen by looking at the Scheffe table shown in **Table 23**. This clearly shows that for either scenario one or two there is no significant difference in comfort levels between the two scenarios holding the intrusion levels and discount offered constant. **Table 5**, shows the ANOVA results from the repeated measures for the scenario effect, which shows that this effect is not significant. This result might show that consumers do not differentiate between a benefit that is once off versus a benefit that is recurring or on-going. Langenderfer & Miyazaki (2009) found that consumers are beginning to accept that their privacy has some value and are starting to relinquish some of their privacy in order to unlock this value. The scenario as described in scenario three has become a reality and a growing number of organisations are beginning to see the value in having more detailed information about their consumers. For car insurers this means offering lower premiums for those consumers that are prepared to allow the car insurance company to track their driving habits. In their research they proposed further research to determine whether the exchange of privacy for benefits was becoming more acceptable (Langenderfer & Miyazaki, 2009).

These results would appear to illustrate that the respondents do not believe that a recurring benefit when compared against a once off benefit is enough to cause them to forego more information. It may therefore be related to more factors other than just the recurring benefit. Sheng, Fui-Hoon Nah, & Siau (2008) advocated that consumers' privacy concerns were triggered by personalisation irrespective of the situation.

This means that we are not able to reject the null hypothesis or ***$H_0$*: There is no scenario effect on comfort levels** which means that we cannot accept the alternative hypothesis being ***$H_1$*: There is a scenario effect on comfort levels**.

# 7. Conclusion and Recommendations

## 7.1. Introduction

This chapter summarises the findings of the research and relates this to the original aim, and assess if the research objectives have been met. The chapter also highlights the results in relation to the existing academic literature, offers some general recommendations based on the findings. It also examines the limitations that were experienced while conducting the research and concludes the chapter with recommendations for future research

## 7.2. Summary of Key Findings From the Research

This research aimed to examine the price required to negate consumer's concerns around privacy when using location based services. In order to do this it used a scenario based questionnaire and then asked the respondents to rate their feelings on the scenario, intrusion level and discount in terms of comfort levels.

The research found that there was a discount effect that influences the respondents and causes them to increase their comfort levels, this meant that the main hypothesis was accepted which added some support to the view that consumers privacy can be bought. However it was observed that the respondents comfort levels increased but they never became truly comfortable with the organisation tracking their movements closely. This means that the respondents' privacy feelings were definitely influenced through the discount offered, which therefore implies that to some degree their privacy could be bought. Although this main effect was significant, it is important to note that all the other interaction effects were also significant which shows that the combination of the variables chosen for this research were the correct combination.

The research also found that the combination of the different scenarios and the discount being offered also had an effect on the comfort levels felt by the respondents. Consumers are becoming acutely aware that their privacy is for sale and that organisations need to make compelling offers in order to buy the privacy. This added weight to the argument mentioned above. This shows that the respondents for this research report clearly felt that their privacy could be bought with a high enough offer. However it can clearly be seen that although their privacy can be bought, the respondents are certainly not at the stage where they feel completely comfortable with exposing their location details to organisations.

The research examined the effect that the scenario and the intrusion level had on the respondents comfort level in terms of their privacy. This showed that the respondents were influenced by the intrusion level and this affected their comfort levels when looking at the privacy aspect. The results for this clearly showed that the respondents felt strongly about the fact that as the intrusion levels became more invasive their comfort levels diminished rapidly. This once again reiterates that the respondents although open to the idea of 'selling' their privacy, are not yet entirely comfortable with this allowing a high intrusion level.

Interestingly it was found that the respondents did not consider receiving on-going benefits as a differentiator versus once off benefits when looking at their privacy concerns. This was surprising considering that the benefits would be received every month. This might have been due to the quantum of the benefit that was being received which was relatively small even though it was recurring. It is again worth noting that although the main effect that was tested did not show significance all the other interaction effects were significant.

## 7.3. RECOMMENDATIONS

The recommendations that come out of this research have implications for both academia and business.

As mentioned in the literature above, consumers are realising that their privacy can be sold. This has been referred to as the privacy calculus where a risk benefit analysis has been carried out by the consumer in order to decide whether the offer is sufficient for them to forego their privacy. This has also been described where the consumers do an analysis on the risk but discount it because the benefit is enjoyed immediately but the risk is not considered because it is not immediate.

It is therefore important to examine the factors that could influence this in a mobile commerce environment because the risk is not discounted because the event happens immediately. The main academic recommendation is to understand the effect that mobile commerce and location based services have on the risk benefit analysis and how the fact that the immediate risk is known affects the decision making process. It would also be of benefit to academia to look at previous e-commerce research and evaluate whether the principles proven in those reports need to be revisited. Based on the results of this study it would seem that the respondents did not fall into the bounded rationality trap as they appeared to calculate the longer term risks.

The recommendations to business are that organisations need to understand that consumers are concerned by the risks around privacy disclosure but are still willing to forego these depending on the deal offered. The consumers clearly require some reassurances that address these concerns. Organisations should therefore take the time to try and understand these concerns and group their customers accordingly. As mentioned above consumers could be grouped in three distinct groups which would allow organisations to treat these three groups differently. This would also allow them to make business offers based on these groups. Marketers' must realise that one of the key elements in the adoption of these services and/or technology is related to trust and therefore they need to find ways of constantly reassuring consumers while at the same time slowly exposing them to the benefits of LBS, both from a financial and relevance perspective. Marketers should focus on the 'privacy pragmatists' group of consumers as these consumers are partial to the benefits of using their privacy to gain benefits. It is felt that this group of consumers would show higher comfort levels across the various scenarios, intrusion levels and discount offered levels because of their attitude.

## 7.4. Limitations Of This Study

The limitations of the study are mostly related to the way in which the research was conducted where a scenario was described as opposed to experienced and even though the literature confirms that a scenario is a relatively good approximation of actual behaviour. It would therefore add weight to the research if the respondent's actually experienced the scenario.

The sample group could have been divided between consumers in different age groups because it is assumed that age would play a large part in the consumers feeling around privacy.

## 7.5. Recommendations For Further Research

The research's aim was to establish the price required to negate a consumer's concerns around privacy in LBS. While conducting this segment of research a number of other areas of future research were identified, these are listed below'

1. The trust relationship between the consumer and organisation could be examined to see if this affected the decisions of the consumer. A brand or organisation that was considered more trustworthy or with which the consumer had more trust in might influence the consumer to forego more privacy than one in which they don't.
2. Active rather than passive tracking of the consumer could be examined to determine what affect this had on the privacy concerns of the consumer. This could mean that privacy concerns could be lessened if the consumer knew that their information was only available within a certain radius.
3. The non-personalisation or consolidation of the consumer's data could be examined to determine the affect this had on the privacy concerns. This could mean that privacy concerns could be lessened if the consumer felt that their information was 'unidentifiable'.
4. The research found literature that discussed how in an ecommerce environment, consumer's discounted the risk associated with privacy concerns because the event of privacy violation might only occur in the future some time. This research appeared to find that the respondents did not discount this risk because the risk with LBS is immediate and can be comprehended. Further research could establish whether LBS changes this risk/benefit analysis for the consumer because of the fact that the risk is known and can be understood immediately.

## 7.6. CONCLUSION

The study achieved the objectives as outlined in chapter three, by answering the questions posed by the research hypothesis. Chapter five and six described the results and discussed these results in relation to past literature. It was found that the respondents' privacy could be purchased; they were not overly comfortable with the concept of organisations tracking their every movement.

Most of the results supported the previous literature with one exception where it would appear that mobile commerce causes the risks associated with a privacy 'incident' to be considered and evaluated at the point of sale/purchase.

In conclusion, understanding the items that affect the privacy concerns and disclosures of consumers' in a mobile commerce and LBS environment is becoming increasingly prevalent for businesses because their consumers are becomingly aware of the benefits and risks associated with these services. It is clear that consumers and organisations alike are struggling with these technologies and concepts due to the fact that they are multifaceted and can be influenced by a multitude of items. It is believed that this research has assisted in gaining insight into these items that influence which will allow consumers and marketers to try to better understand one another.

# 8. BIBLIOGRAPHY

(n.d.).

*Global mobile statistics 2011*. (2010, March 1). Retrieved April 4, 2011, from mobiThinking: http://mobithinking.com/stats-corner/global-mobile-statistics-2011-all-quality-mobile-marketing-research-mobile-web-stats-su

Acquisti, A. (2004). Privacy in Electronic Commerce and the Economics of Immediate Gratification. *Proceedings of ACM Electronic Commerce Conference (EC 04)* (pp. 21-29). New York: ACM Press.

Ahern, S., Eckles, D., Good, N. S., King, S., Naaman, M., & Nair, R. (2007). Photo sharing: Over-exposed?: Privacy patterns and considerations in online and mobile photo sharing. *Proceedings of CHI '07.* New York: ACM.

Albright, S. C., Winston, W. L., & Zappe, C. J. (2009). *Data Analysis & Decision Making.* Mason: South-Western Cengage Learning.

Altman, I. (1977). Privacy regulation: culturally universal or culturally specific? *Journal of Social Issues, 33*(3), 66-84.

Anckar, B., & D'Incau, D. (2002). Value Creation in Mobile Commerce: Findings from a Consumer Survey. *Journal of Information Technology Theory and Application, 4*(1), 43-64.

Balasubramanian, S., Peterson, R. A., & Jarvenpaa, S. L. (2002). Exploring the Implications of M-Commerce for Markets and Marketing. *Journal of Academy of Marketing Science, 30*(4), 348-361.

Basheer, A., & Ibrahim, A. (2010, March). Mobile Marketing: Examining the Impact of Trust, Privacy Concern and Consumers' Attitudes on Intention to Purchase. *International Journal of Business and Management, 5*(3), 28-41.

Bin Mai, B., Menon, N. M., & Sarkar, S. (2010, Fall). No Free Lunch: Price Premium for Privacy Seal–Bearing Vendors. *Journal of Management Information Systems, 27*(2), 189–212.

Birnhack, M. D. (2008). The EU Data Protection Directive: An engine of a global regime. *Computer Law & Security Report, 24*, 508-520.

Blumberg, B., Cooper, R. D., & Schindler, S. P. (2008). *Business Research Methods.* New York: McGraw-Hill.

Bruner II, G. C., & Kumar, A. (2007, Spring). Attitude toward Location-Based Advertising. *7*(2), 3-15.

Camponovo, G., Debetaz, S., & Pigneur , Y. (2004). A Comparative Analysis Of Published Scenarios For M-Business. *Third Annual MBusiness Conference* (pp. 1-16). New York City: MBusiness 2004.

Caudill, M. E., & Murphy, E. P. (2000). Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy & Marketing, 19*(1), 7-19.

Cavoukian, A., & Hamilton, T. (2002). *The Privacy Payoff: How Successful Businesses Build Customer Trust.* Toronto: McGraw-Hill Ryerson.

Chen, J., Ross, W., & Huang, S. (2008). Privacy, trust, and justice considerations for location-based mobile telecommunication services. *Online Information Review, 10*(4), 30-45.

Chow, C.-Y., Mokbel, M. F., & Aref, W. G. (2009, December). Casper: Query Processing for Location Services without Compromising Privacy. *ACM Transactions on Database Systems, 34*(4), 2-48.

Consulting group of the Division of Statistics and Scientific Computing at the University of Texas at Austin. (1997). *Consulting group*. Retrieved 10 2011, from University of Texas at Austin: http://ssc.utexas.edu/

Coyle, F. P. (2001). *Wireless Web: A Manager's Guide.* Boston: Addison-Wesley.

Cullen, R. (2009). Culture, identity and information privacy in the age of digital government. *Online Information Review, 33*(3), 405-421.

Culnan, M. (1993). “How did they get my name?” An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly, 17*(3), 341-363.

Culnan, M. J., & Bies, J. R. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues, 59*(2), 323-342.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behavior and Information Technology, 23*(6), 413-422.

Dinev, T., & Hart, P. (2006 (a)). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.

Dinev, T., & Hart, P. (2006 (b)). Internet privacy and social awareness as determinants of Intention to transact. *International Journal of Electronic Commerce, 10*(2), 7-29.

Dolnicar, S., & Jordaan, Y. (2007, Summer). A Market-Oriented Approach to Responsibly Managing Information Privacy Concerns in Direct Marketing. *Journal of Advertising, 36*(2), 123–149. doi:10.2753

Dutton, W. H., & Helsper, E. (2007). *Publications.* Retrieved 10 2011, from OxIS - Oxford Internet Surveys: http://www.oii.ox.ac.uk/microsites/oxis/publications.cfm

Fischer, K. (2004). *Consumers ready for wireless location-based services; 2005 will be a strong year for carrier deployment*. Retrieved 10 2011, from InStat: http://www.instat.com/press.asp?ID¼1175&sku¼IN0401660MCD

Friedewalda, M., Wright, D., Gutwirthc, S., & Mordini, E. (2010). Privacy, data protection and emerging sciences and technologies: towards a common framework. *Research, Innovation - The European Journal of Social Science, 23*(1), 61-67.

Galanxhi, H., & Nah, F. (2006). Privacy issues in the era of ubiquitous commerce. *Electronic Markets, 16*(3), 222-232.

Goldfarb, A., & Tucker, C. (2011, May). Online Advertising, Behavioral Targeting, and Privacy. *COMMUNICATIONS OF THE ACM, 54*(5), 25-27.

Goodhue, D. L., Wybo, M. D., & Kirsch, L. J. (1992). The impact of data integration on the costs and benefits of information systems. *MIS Quarterly, 16*(3), 293-311.

Greengard, S. (2008, December). Upwardly Mobile. *Communications of the ACM, 51*(12), 17-19.

Gurau, C., & Ranchhod, A. (2009). Consumer privacy issues in mobile commerce: a comparative study of British, French and Romanian consumers. *Journal of Consumer Marketing, 26*(7), 496-507. doi:10.1108/07363760911001556

Hann, I. H., Hui, K.-L., Lee, S. Y., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems, 24*(2), 13-42.

Harris Interactive. (2004). *Harris Vault*. Retrieved from Harris Interactive: http://www.harrisinteractive.com/Insights/HarrisVault.aspx

Hinz, O., Gertmeier, E., Tafreschi, O., Enzmann, M., & Schneider, M. (2007). Customer Loyalty programs and privacy concerns. *20th Bled eConference eMergence: Merging and Emerging Technologies* (p. 406). Bled, Slovenia: Processes and Institutions.

Hui, K. L., Teo, H. H., & Tom Lee, S.-Y. (2007, March). The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly, 31*(1), 19-33.

Jin, C. H., & Villegas, J. (2008, December). MOBILE PHONE USERS' BEHAVIORS: THE MOTIVATION FACTORS OF THE MOBILE PHONE USER. *International Journal of Mobile Marketing, 3*(2), 4-14.

Joinson, A. N. (2008). “Looking at,” “Looking up” or “Keeping up with” people? Motives and uses of Facebook. *Proceedings of CHI.* New York: ACM.

Joinson, A., Reips, U.-D., Buchanan, T., & Schofield, C. (2010). Privacy, Trust, and Self-Disclosure Online. *HUMAN–COMPUTER INTERACTION, 25*, 1-24.

Junglas, I. A., & Watson, R. T. (2008, March). Location-Based Services. *Communications of the ACM, 51*(3), 65-69.

Junglas, I. A., Johnson, N. A., & Spitzmuller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems, 17*, 387-402.

Kalakota, R., & Robinson, M. (2002). *M-Business: The Race to Mobility.* New York: McGraw-Hill.

Langenderfer, J., & Miyazaki, A. D. (2009). Privacy in the Information Economy. *The Journal Of Consumer Affairs, 43*(3), 380-388.

Lanier, C. D., & Saini, A. (2008). Understanding Consumer Privacy: A Review and Future Directions. *Academy of Marketing Science Review*, 1-45. Retrieved from http://www.amsreview.org/articles/lanier02-2008.pdf

Lee, D.-J., Ahn, J.-H., & Bang, Y. (2011, June). MANAGING CONSUMER PRIVACY CONCERNS IN PERSONALIZATION: A STRATEGIC ANALYSIS OF PRIVACY PROTECTION. *MIS Quarterly, 35*(2), 423-444.

Leek, S., & Christodoulides, G. (2009). “Next-generation mobile marketing: how young consumers react to Bluetooth-enabled advertising”. *Journal of Advertising Research, 49*(1), 44-53.

Lessig, L. (1999). *Code and other laws of cyberspace.* New York: Basic Books.

Lindley, D. (2010, December). A Matter of Privacy. *COMMUNICATIONS OF THE ACM, 53*(12), 23.

Little, L., & Briggs, P. (2009). Privacy Factors for Successful Ubiquitous Computing. *International Journal of E-Business Research, 5*(2), 1-20.

Luo, X. (2002). Trust production and privacy concerns on the Internet: a framework based on relationship marketing and social exchange theory. *Industrial Marketing Management, 31*, 111-118.

Lwin, M. O., Wirtz, J., & Williams, J. D. (2007). Consumer Online Privacy Concerns and Responses: A Power-Responsibility Equilibrium Perspective. *Journal of the Academy of Marketing Science, 35*(4), 572-585.

Malhotra, A., & Kubowicz Malhotra, C. (2009, July). A Relevancy-Based Services View for Driving Adoption of Wireless Web Services in the U.S. *Communications of the ACM, 52*(7), 130-134.

Margulis, T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues, 52*(2), 243-261.

Milne, G. R., & Bahl, S. (2010, Spring). Are There Differences Between Consumers' and Marketers' Privacy Expectations? A Segment- and Technology-Level Analysis. *Journal of Public Policy & Marketing, 29*(1), 138-149.

Milne, G., & Bahl, S. (2010, Spring). Are There Differences Between Consumers' and Marketers' Privacy Expectations? A Segment- and Technology-Level Analysis. *Journal of Public Policy & Marketing, 29*(1), 138-149.

Motahari, S., Manikopoulos, C., Hiltz, R., & Jones, Q. (2007). Seven privacy worries in ubiquitous social computing. *Symposium on usable privacy and security (SOUPS)* (pp. 171-172). Pittsburgh: CMU Usable Privacy and Security Laboratory (CUPS).

O'Donoghue, T., & Rabin, M. (2001). Choice and procrastination. *Quartely Journal of Economics, 116*, 121-160.

Ohkubo, M., Suzuki, K., & Kinoshita, S. (2005). RFID privacy issues and technical challenges. *Communications of the ACM, 48*(9), 66-71.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing, 19*(Spring), 27-41.

Porus, J., & Ellis, M. (2007). *The Harris Report: Location-based services and presence technology: the future of telecommunications is closer than you think*. Retrieved 10 2011, from Harris Interactive: http://www.harrisinteractive.com/news/newsletters/HarrisReport/HI_TheHarrisReport_2007_v02_i01.pdf

Radin, T., Calkins, M., & Predmore, C. (2007). ''New challenges to old problems: building trust in e-marketing''. *Business and Society Review, 112*(1), 73-98.

Rapp, J., Hill, R. P., Gaines, J., & Wilson, R. M. (2009, Winter). ADVERTISING AND CONSUMER PRIVACY. *Journal of Advertising, 38*(4), 51-61.

Redknee. (2006). *Redknee protects wireless subscribers' privacy concerns with industry first solution: personalization allows users to decide which wireless services, applications and users can access their personal data*. Retrieved 10 2011, from Redknee: http://www.redknee.com/news_events/news_releases/archive_2006/156/?PHPSESSID¼d99270ce1b41ea4c

Sheehan, K., & Hoy, M. (2000). Dimensions of Privacy Concern Among Online Consumers. *Journal of Public Policy & Marketing, 19*(1), 62-73.

Sheng, H., Nah, F. F.-H., & Siau, K. (2008). An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy Concerns. *Journal of the Association for Information Systems, 9*(6), 344-376.

Shoemaker, D. W. (2010). Self-exposure and exposure of the self: informational privacy and the presentation of identity. *Ethics Inf Technol, 12*, 3-15.

Smith, H., Milberg, S., & Burke, S. (1996). Information privacy: measuring individual's concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.

Spiekermann, S. (2009). RFID and privacy: what consumers really want and fear. *Pers Ubiquit Comput, 13*, 423-434.

Spiekermann, S. (2009). RFID and privacy: what consumers really want and fear. *Pers Ubiquit Comput, 13*, 423-434.

Spiekermann, S., & Langheinrich, M. (2009). An update on privacy in ubiquitous computing. *Pers Ubiquit Comput, 13*, 389-390. doi:10.1007/s00779-008-0210-7

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information. *Information Systems Research, 13*(1), 36-49.

Timm, D. M., & Duven, C. J. (2008, Winter). Privacy and Social Networking Sites. *New Directions for Student Services, 124*, 89-102.

Tsang, M. M., Ho, S. C., & Liang, T. P. (2004). Consumer attitudes toward mobile advertising: an empirical study. *International Journal of Electronic Commerce, 8*(3), 65-78.

Unni, R., & Harmon, R. (2007, Spring). Perceived Effectiveness of Push vs. Pull Mobile Location-Based Advertising. *7*(2), 28-40.

Wikipedia. (2011, April 12). *List of countries by number of mobile phones in use*. Retrieved April 8, 2011, from Wikipedia: http://en.wikipedia.org/wiki/List_of_countries_by_number_of_mobile_phones_in_use

Wu, J.-H., & Hisa, T.-L. (2008). DEVELOPING E-BUSINESS DYNAMIC CAPABILITIES: AN ANALYSIS OF E-COMMERCE INNOVATION FROM I-, M- TO U-COMMERCE. *Journal of Organisational Computing and Electronic Commerce, 18*, 95-111.

Xu, H. (2009). Consumer Responses to the Introduction of Privacy Protection Measures: An Exploratory Research Framework. *International Journal of E-Business Research, 5*(2), 21-47.

Xu, H. (2010). Locus of Control and Location Privacy: An Empirical Study in Singapore. *Journal of Global Information Technology Management, 13*(3), 63-87.

Xu, H., & Teo, H. (2004). Alleviating consumers' privacy concern in location-based services: a psychological control perspective. *Twenty-Fifth International Conference on Information Systems* (pp. 793-806). Washington DC: International Conference on Information Systems.

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51*, 43-52.

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2009, Winter). The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. *Journal of Management Information Systems, 26*(3), 135-173.

Youn, S. (2009, Fall). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *The Journal of Consumer Affairs, 43*(3), 389-418.

Zhou, T. (2011). The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems, 111*(2), 212-226.

Zikmund, W. G. (2003). *Business Research Methods.* Thomson South Western.

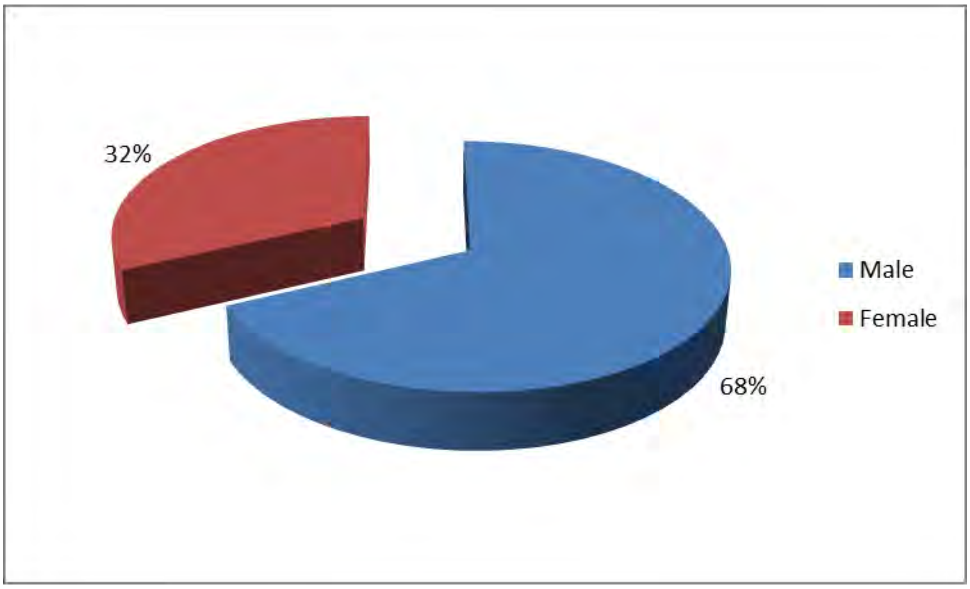
# 9. DISTRIBUTIONS

## 9.1. GENDER

TABLE 6: GENDER DISTRIBUTION (FREQUENCY TABLE)

| | Count | Percent |
|---|---|---|
| Male | 144 | 68% |
| Female | 67 | 32% |

FIGURE 10: GENDER DISTRIBUTION (PIE CHART)

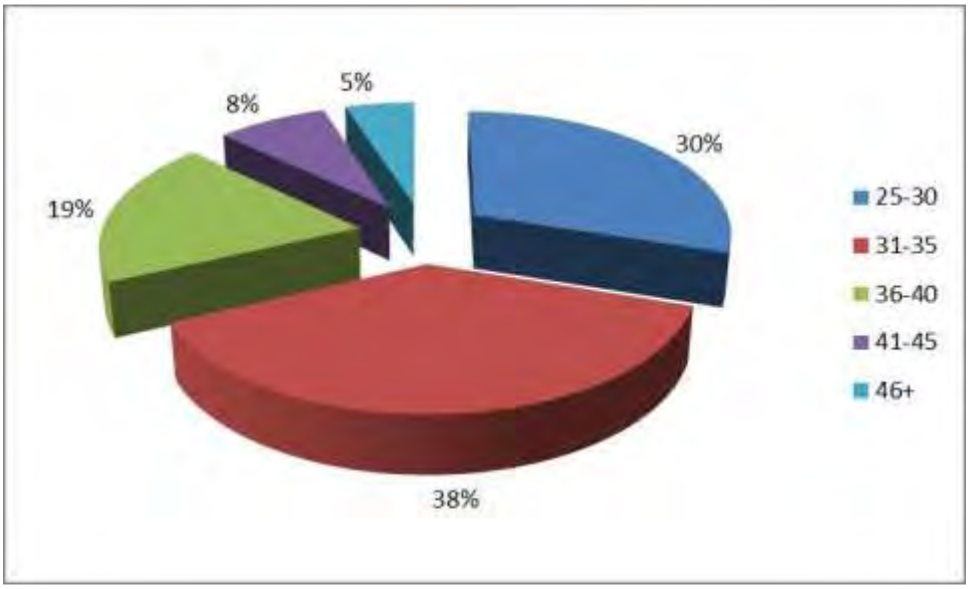


## 9.2. AGE

TABLE 7: AGE FREQUENCY TABLE

| | Count | Percent |
|---|---|---|
| 25-30 | 63 | 30% |
| 31-35 | 80 | 38% |
| 36-40 | 41 | 19% |
| 41-45 | 17 | 8% |
| 46+ | 10 | 5% |

FIGURE 11: AGE DISTRIBUTION (PIE CHART)

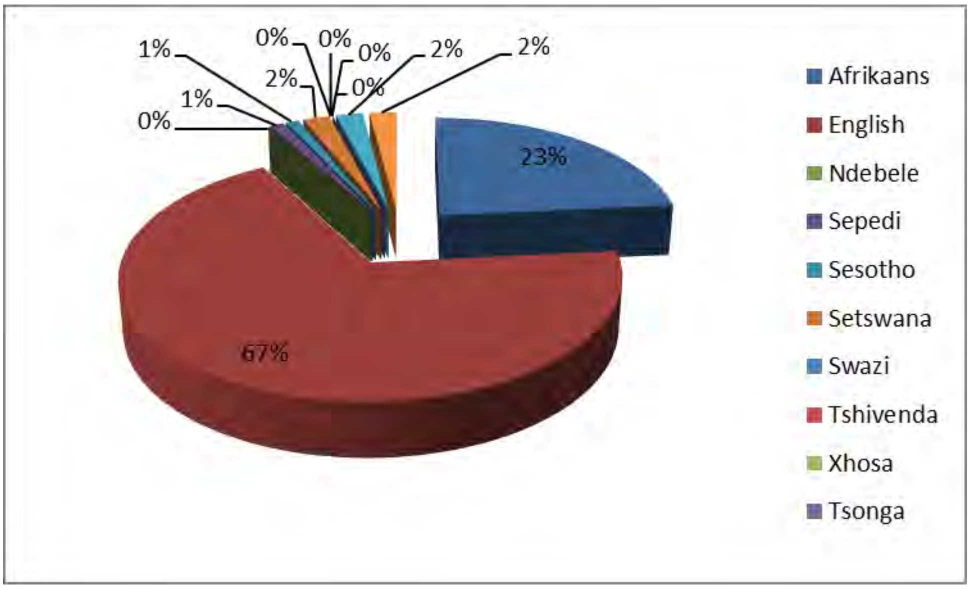


## 9.3. LANGUAGE

TABLE 8: LANGUAGES FREQUENCY TABLE

| | Count | Percent |
|---|---|---|
| Afrikaans | 48 | 23% |
| English | 141 | 67% |
| Ndebele | 0 | 0% |
| Sepedi | 3 | 1% |
| Sesotho | 3 | 1% |
| Setswana | 4 | 2% |
| Swazi | 0 | 0% |
| Tshivenda | 1 | 0% |
| Xhosa | 1 | 0% |
| Tsonga | 1 | 0% |
| Zulu | 5 | 2% |
| Other | 4 | 2% |

FIGURE 12: LANGUAGE DISTRIBUTION (PIE CHART)

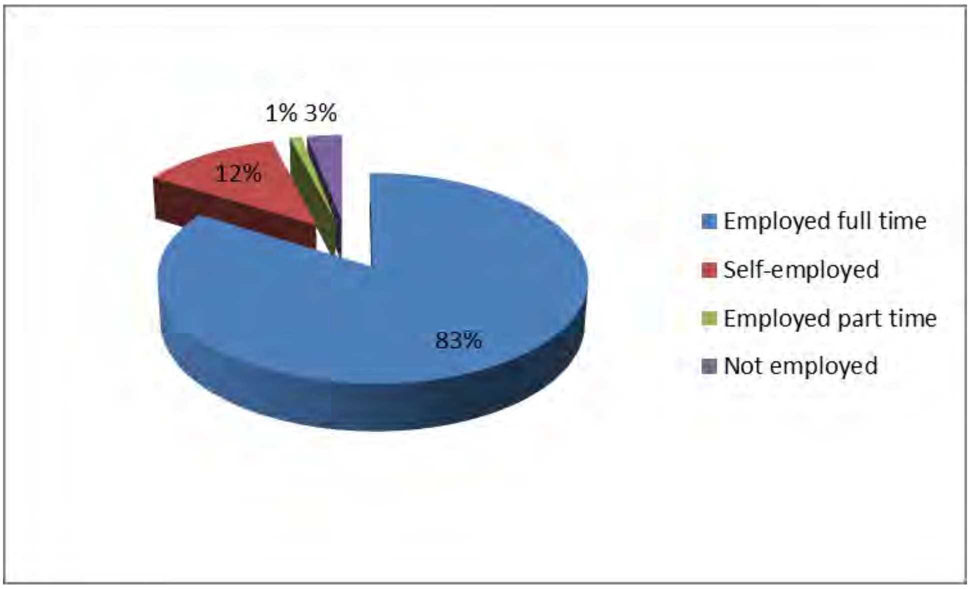


## 9.4. EMPLOYMENT STATUS

TABLE 9: EMPLOYMENT STATUS FREQUENCY TABLE

| | Count | Percent |
|---|---|---|
| Employed full time | 176 | 83% |
| Self-employed | 26 | 12% |
| Employed part time | 3 | 1% |
| Not employed | 6 | 3% |

FIGURE 13: EMPLOYMENT DISTRIBUTION (PIE CHART)

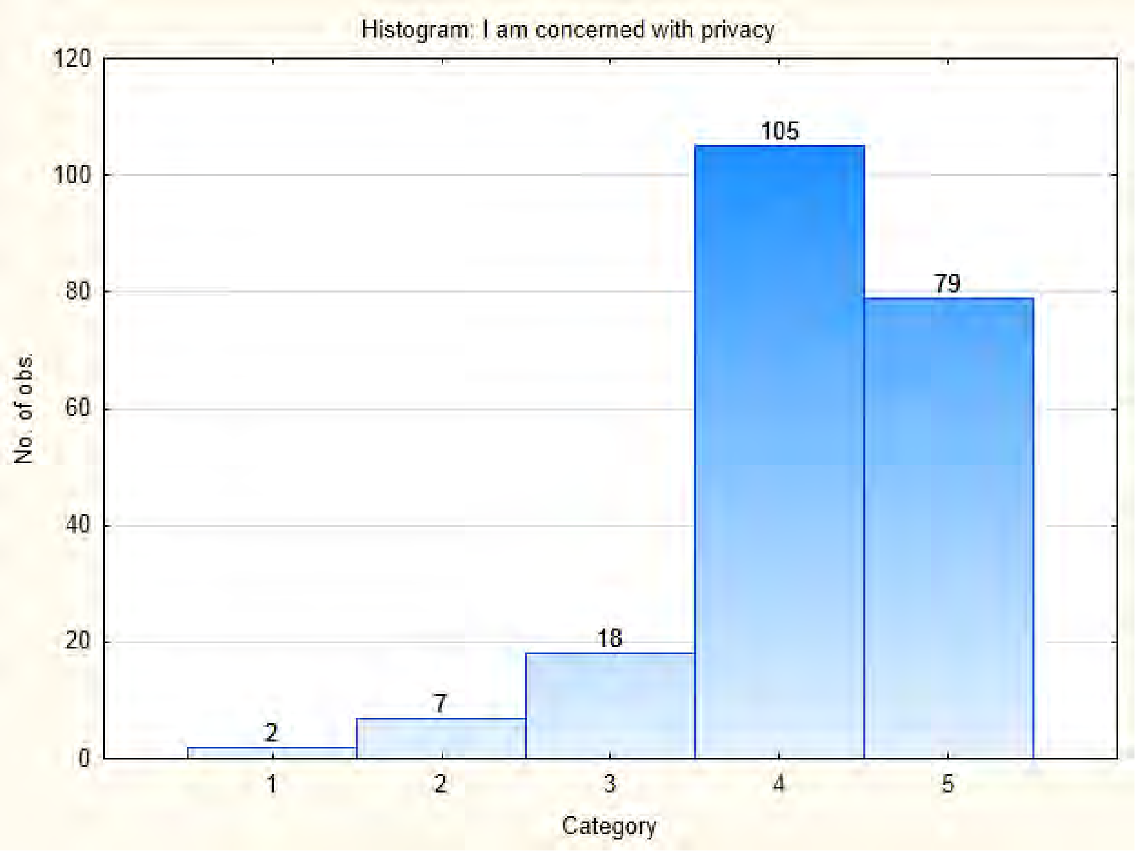


## 9.5. QUESTION 1: I AM CONCERNED WITH PRIVACY

TABLE 10: QUESTION 1: I AM CONCERNED WITH PRIVACY

| | Count | Percent |
|---|---|---|
| 1 | 2 | 0.95% |
| 2 | 7 | 3.32% |
| 3 | 18 | 8.53% |
| 4 | 105 | 49.76% |
| 5 | 79 | 37.44% |

FIGURE 14: QUESTION 1: I AM CONCERNED WITH PRIVACY

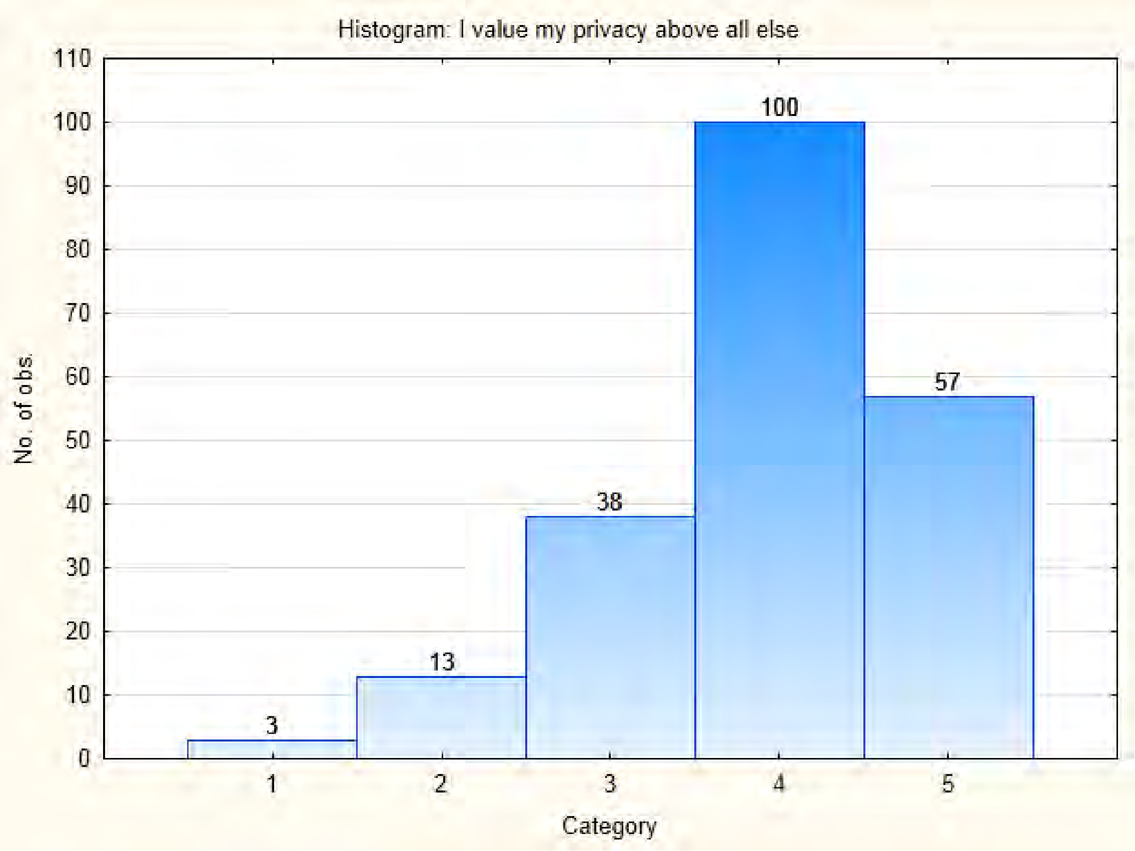


## 9.6. QUESTION 2: I VALUE MY PRIVACY ABOVE ALL ELSE

TABLE 11: QUESTION 2: I VALUE MY PRIVACY ABOVE ALL ELSE

| | Count | Percent |
|---|---|---|
| 1 | 3 | 1.43% |
| 2 | 13 | 6.16% |
| 3 | 38 | 18.01% |
| 4 | 100 | 47.39% |
| 5 | 57 | 27.01% |

FIGURE 15: QUESTION 2: I VALUE MY PRIVACY ABOVE ALL ELSE

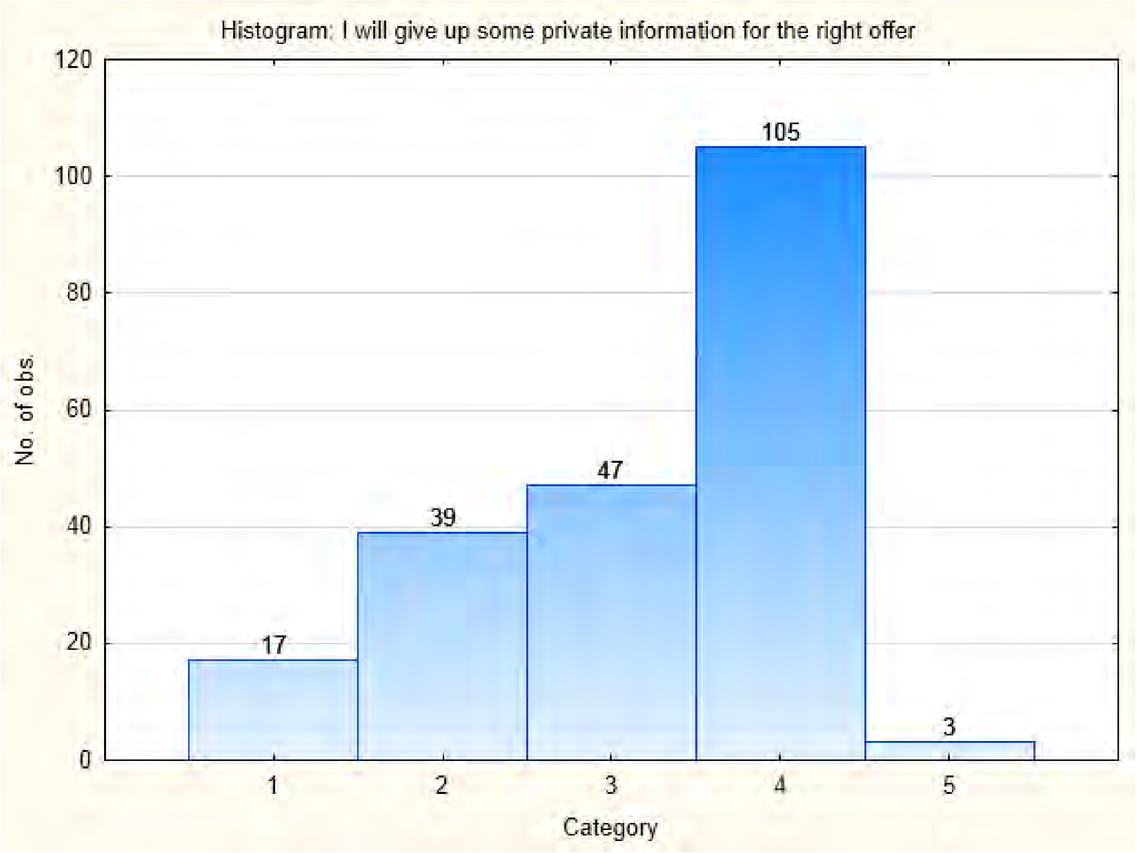


## 9.7. QUESTION 3: I WILL GIVE UP SOME PRIVATE INFORMATION FOR THE RIGHT OFFER

TABLE 12: QUESTION 3: I WILL GIVE UP SOME PRIVATE INFORMATION FOR THE RIGHT OFFER

| | Count | Percent |
|---|---|---|
| 1 | 17 | 8.07% |
| 2 | 39 | 18.48% |
| 3 | 47 | 22.27% |
| 4 | 105 | 49.76% |
| 5 | 3 | 1.42% |

FIGURE 16: QUESTION 3: I WILL GIVE UP SOME PRIVATE INFORMATION FOR THE RIGHT OFFER

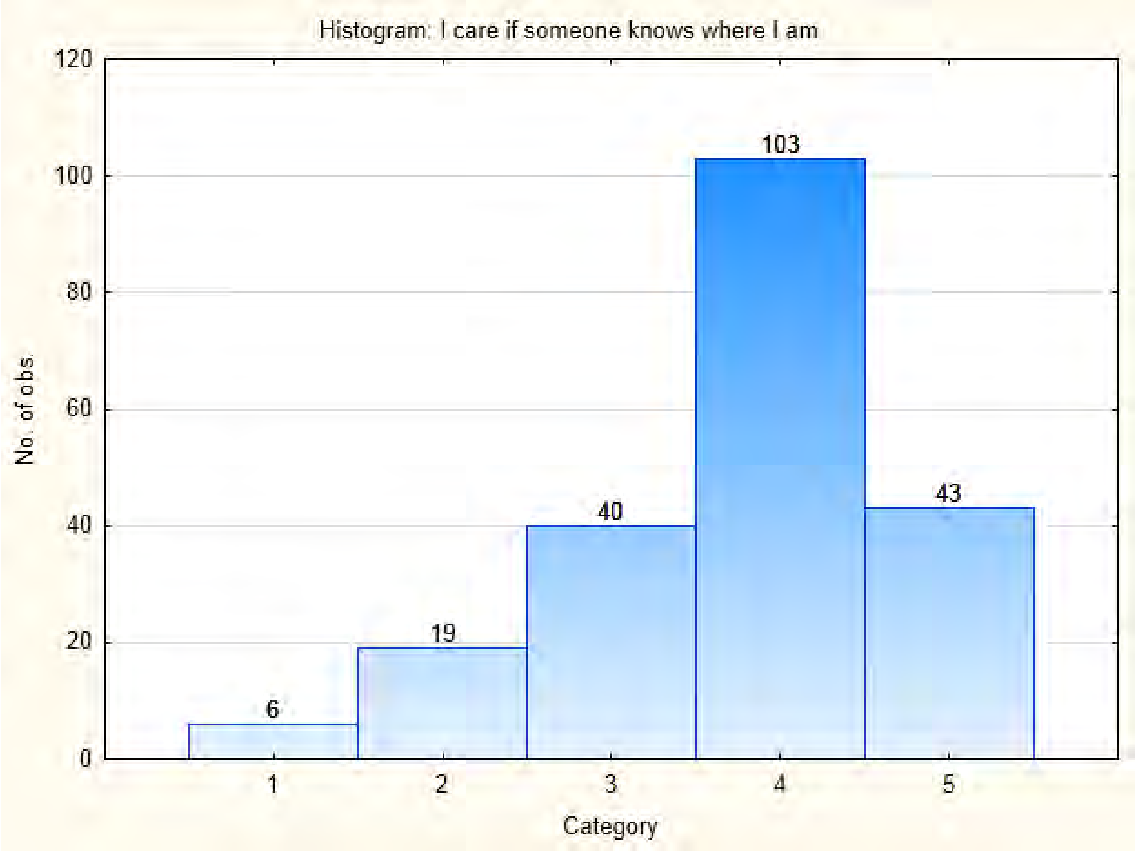


## 9.8. QUESTION 4: I CARE IF SOMEONE KNOWS WHERE I AM

TABLE 13: QUESTION 4: I CARE IF SOMEONE KNOWS WHERE I AM

| | Count | Percent |
|---|---|---|
| 1 | 6 | 2.84% |
| 2 | 19 | 9.00% |
| 3 | 40 | 18.96% |
| 4 | 103 | 48.82% |
| 5 | 43 | 20.38% |

Figure 17: Question 4: I Care If Someone Knows Where I Am

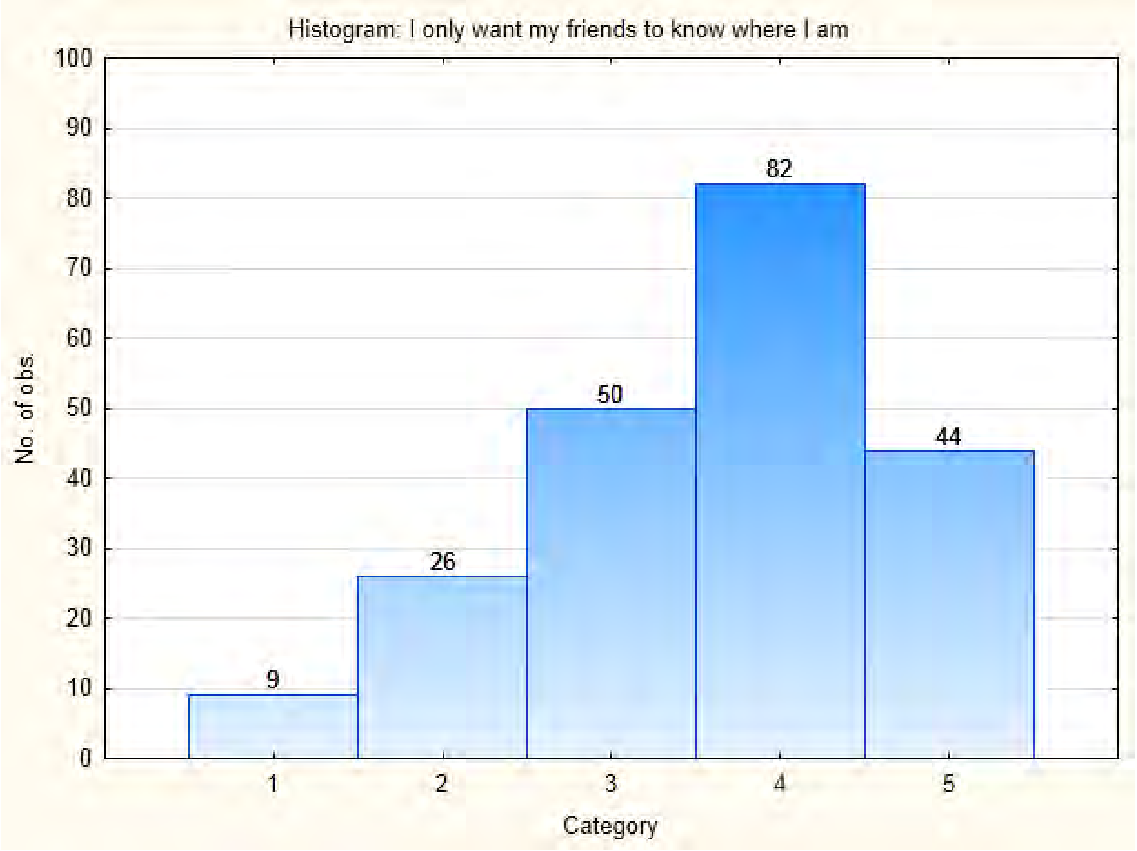


## 9.9. Question 5: I Only Want My Friends To Know Where I Am

Table 14: Question 5: I Only Want My Friends To Know Where I Am

| | Count | Percent |
|---|---|---|
| 1 | 9 | 4.27% |
| 2 | 26 | 12.32% |
| 3 | 50 | 23.70% |
| 4 | 82 | 38.86% |
| 5 | 44 | 20.85% |

Figure 18: Question 5: I Only Want My Friends To Know Where I Am

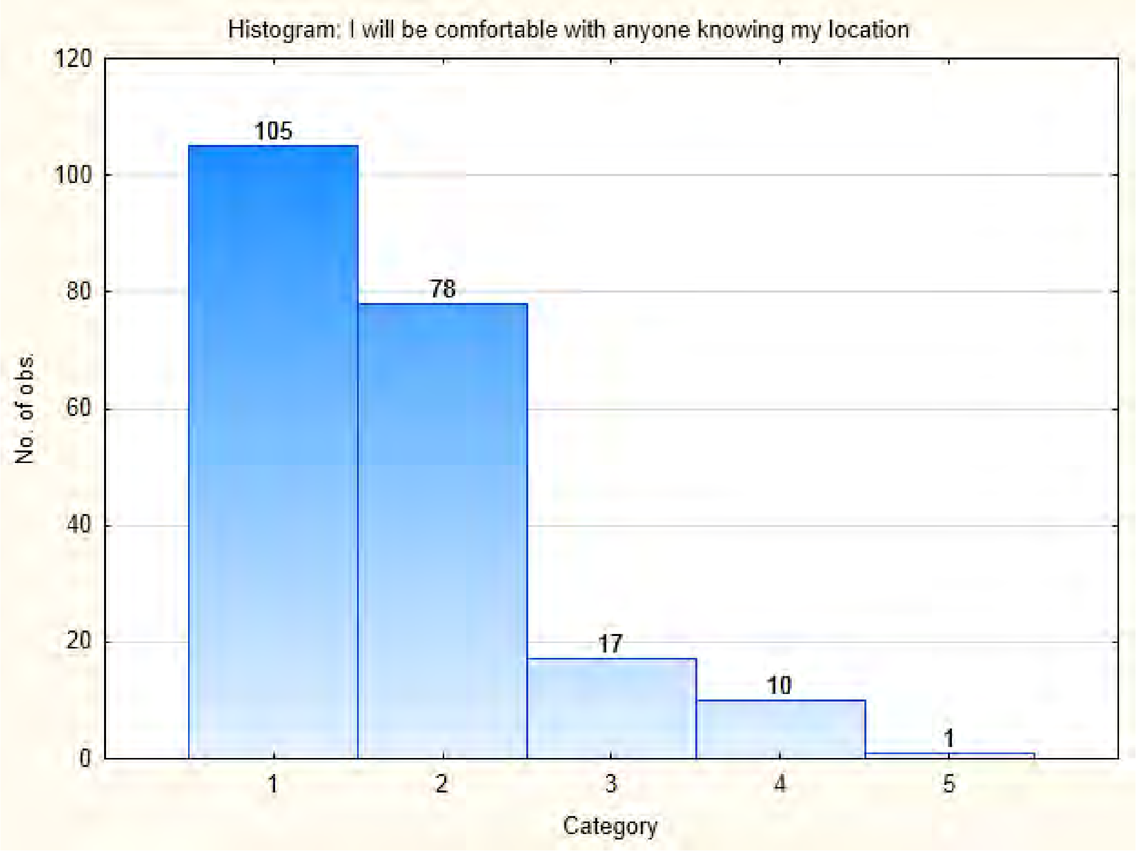


## 9.10. Question 6: I Will Be Comfortable With Anyone Knowing My Location

Table 15: Question 6: I Will Be Comfortable With Anyone Knowing My Location

| | Count | Percent |
|---|---|---|
| 1 | 105 | 49.76% |
| 2 | 78 | 36.97% |
| 3 | 17 | 8.06% |
| 4 | 10 | 4.74% |
| 5 | 1 | 0.47% |

Figure 19: Question 6: I Will Be Comfortable With Anyone Knowing My Location

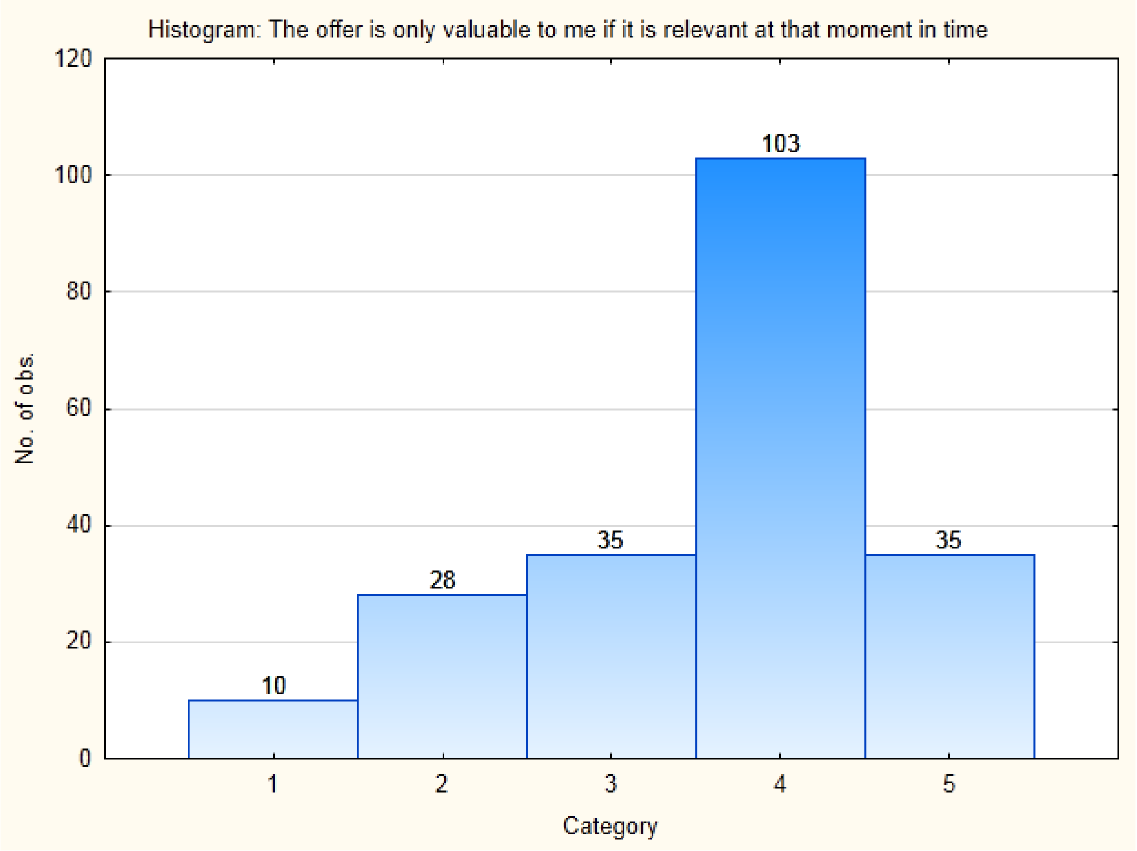


## 9.11. Question 7: The Offer Is Only Valuable To Me If It Is Relevant At That Moment In Time

Table 16: Question 7: The Offer Is Only Valuable To Me If It Is Relevant At That Moment In Time

| | Count | Percent |
|---|---|---|
| 1 | 10 | 4.73% |
| 2 | 28 | 13.27% |
| 3 | 35 | 16.59% |
| 4 | 103 | 48.82% |
| 5 | 35 | 16.59% |

FIGURE 20: QUESTION 7: THE OFFER IS ONLY VALUABLE TO ME IF IT IS RELEVANT AT THAT MOMENT IN TIME

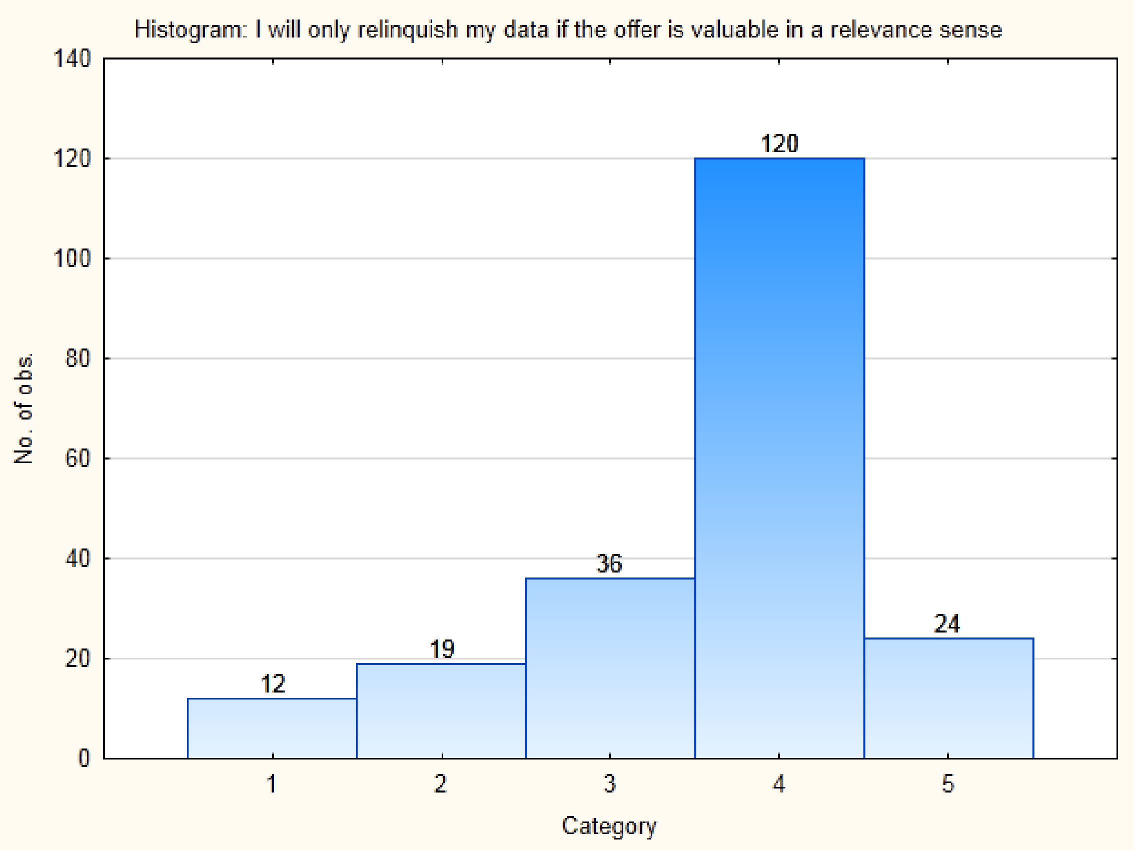


## 9.12. QUESTION 8: I WILL ONLY RELINQUISH MY DATA IF THE OFFER IS VALUABLE IN A RELEVANCE SENSE

TABLE 17: QUESTION 8: I WILL ONLY RELINQUISH MY DATA IF THE OFFER IS VALUABLE IN A RELEVANCE SENSE

| | Count | Percent |
|---|---|---|
| 1 | 12 | 5.69% |
| 2 | 19 | 9.00% |
| 3 | 36 | 17.07% |
| 4 | 120 | 56.87% |
| 5 | 24 | 11.37% |

Figure 21: Question 8: I Will Only Relinquish My Data If The Offer Is Valuable In A Relevance Sense

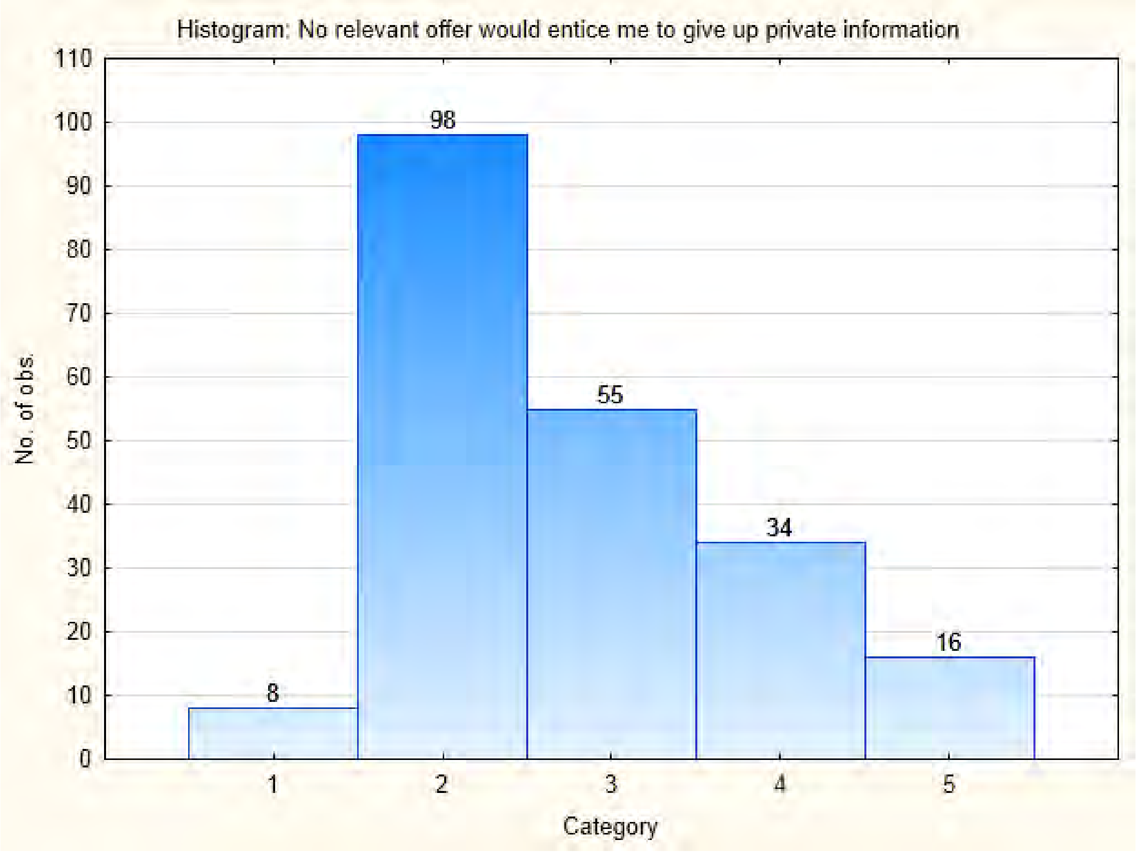


## 9.13. Question 9: No Relevant Offer Would Entice Me To Give Up Private Information

Table 18: Question 9: No Relevant Offer Would Entice Me To Give Up Private Information

| | Count | Percent |
|---|---|---|
| 1 | 8 | 3.79% |
| 2 | 98 | 46.45% |
| 3 | 55 | 26.07% |
| 4 | 34 | 16.11% |
| 5 | 16 | 7.58% |

FIGURE 22: QUESTION 9: NO RELEVANT OFFER WOULD ENTICE ME TO GIVE UP PRIVATE INFORMATION

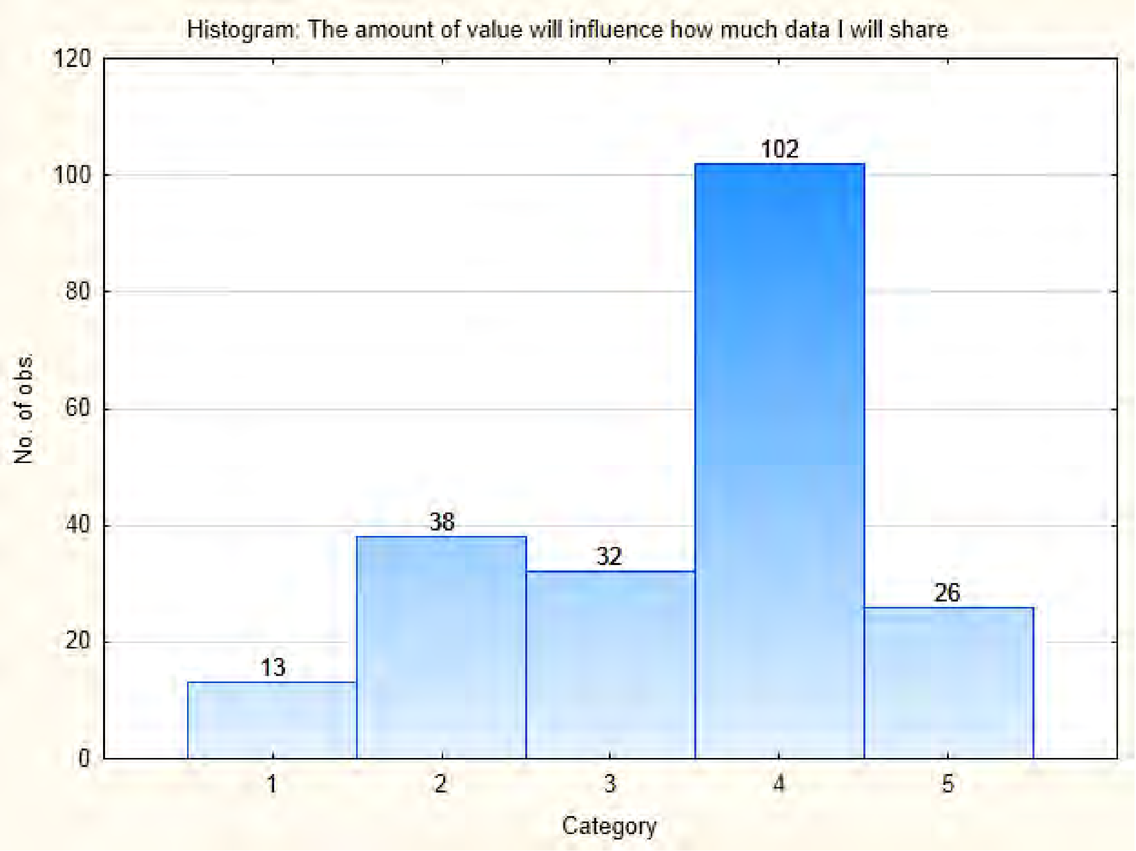


## 9.14. QUESTION 10: THE AMOUNT OF VALUE WILL INFLUENCE HOW MUCH DATA I WILL SHARE

TABLE 19: QUESTION 10: THE AMOUNT OF VALUE WILL INFLUENCE HOW MUCH DATA I WILL SHARE

| | Count | Percent |
|---|---|---|
| 1 | 13 | 6.16% |
| 2 | 38 | 18.01% |
| 3 | 32 | 15.17% |
| 4 | 102 | 48.34% |
| 5 | 26 | 12.32% |

FIGURE 23: QUESTION 10: THE AMOUNT OF VALUE WILL INFLUENCE HOW MUCH DATA I WILL SHARE



# 10. Scheffe Tests

## 10.1. Hypothesis 1

Table 20: Hypothesis 1 – Scheffe Test

| | D1 | D2 | D3 | D4 | D5 |
|---|---|---|---|---|---|
| D1 | | 0.350931 | 0.000000 | 0.000000 | 0.000000 |
| D2 | 0.350931 | | 0.000047 | 0.000000 | 0.000000 |
| D3 | 0.000000 | 0.000047 | | 0.000000 | 0.000000 |
| D4 | 0.000000 | 0.000000 | 0.000000 | | 0.000000 |
| D5 | 0.000000 | 0.000000 | 0.000000 | 0.000000 | |

## 10.2. Hypothesis 1A

Table 21: Hypothesis 1A – Scheffe Test

| | S1-D1 | S1-D2 | S1-D3 | S1-D4 | S1-D5 | S2-D1 | S2-D2 | S2-D3 | S2-D4 | S2-D5 |
|---|---|---|---|---|---|---|---|---|---|---|
| S1-D1 | | 0.799873 | 0.000046 | 0.000000 | 0.000000 | 0.994027 | 0.984472 | 0.000000 | 0.000000 | 0.000000 |
| S1-D2 | 0.799873 | | 0.135190 | 0.000000 | 0.000000 | 0.146095 | 0.999924 | 0.000180 | 0.000000 | 0.000000 |
| S1-D3 | 0.000046 | 0.135190 | | 0.004692 | 0.000000 | 0.000000 | 0.018005 | 0.905702 | 0.000000 | 0.000000 |
| S1-D4 | 0.000000 | 0.000000 | 0.004692 | | 0.003144 | 0.000000 | 0.000000 | 0.505601 | 0.034516 | 0.000000 |
| S1-D5 | 0.000000 | 0.000000 | 0.000000 | 0.003144 | | 0.000000 | 0.000000 | 0.000000 | 0.999950 | 0.000642 |
| S2-D1 | 0.994027 | 0.146095 | 0.000000 | 0.000000 | 0.000000 | | 0.505601 | 0.000000 | 0.000000 | 0.000000 |
| S2-D2 | 0.984472 | 0.999924 | 0.018005 | 0.000000 | 0.000000 | 0.505601 | | 0.000004 | 0.000000 | 0.000000 |
| S2-D3 | 0.000000 | 0.000180 | 0.905702 | 0.505601 | 0.000000 | 0.000000 | 0.000004 | | 0.000000 | 0.000000 |
| S2-D4 | 0.000000 | 0.000000 | 0.000000 | 0.034516 | 0.999950 | 0.000000 | 0.000000 | 0.000000 | | 0.000022 |
| S2-D5 | 0.000000 | 0.000000 | 0.000000 | 0.000000 | 0.000642 | 0.000000 | 0.000000 | 0.000000 | 0.000022 | |

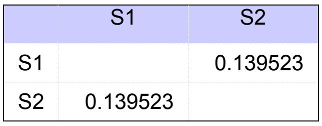
## 10.3. Hypothesis 1B

Table 22: Hypothesis 1B – Scheffe Test

| | S1-I1 | S1-I2 | S1-I3 | S1-I4 | S2-I1 | S2-I2 | S2-I3 | S2-I4 |
|---|---|---|---|---|---|---|---|---|
| S1-I1 | | 0.000000 | 0.000000 | 0.000000 | 0.999839 | 0.093289 | 0.000000 | 0.000000 |
| S1-I2 | 0.000000 | | 0.000002 | 0.000000 | 0.000000 | 0.010128 | 0.000000 | 0.000000 |
| S1-I3 | 0.000000 | 0.000002 | | 0.000000 | 0.000000 | 0.000000 | 0.277532 | 0.000036 |
| S1-I4 | 0.000000 | 0.000000 | 0.000000 | | 0.000000 | 0.000000 | 0.000074 | 0.351347 |
| S2-I1 | 0.999839 | 0.000000 | 0.000000 | 0.000000 | | 0.290285 | 0.000000 | 0.000000 |
| S2-I2 | 0.093289 | 0.010128 | 0.000000 | 0.000000 | 0.290285 | | 0.000000 | 0.000000 |
| S2-I3 | 0.000000 | 0.000000 | 0.277532 | 0.000074 | 0.000000 | 0.000000 | | 0.351347 |
| S2-I4 | 0.000000 | 0.000000 | 0.000036 | 0.351347 | 0.000000 | 0.000000 | 0.351347 | |

## 10.4. Hypothesis 1C

Table 23: Hypothesis 1C – Scheffe Test



|  | S1 | S2 |
|---|---|---|
| S1 |  | 0.139523 |
| S2 | 0.139523 |  |

## 11. Sample Questionnaire

# Consent Section:

I am doing my Masters of Business Administration (MBA) research on privacy and Location Based Services (LBS) in mobile commerce. The study looks at the consumer attitudes towards privacy.

Please can you assist by filling out the questionnaire below with your feelings / perceptions towards privacy, your location information (Location Based Services), the offer being made to you and whether the offer influences your feelings towards your privacy?

You will also be asked some demographic information which will also be used in the analysis of the data provided. The questionnaire is anonymous and the results will also only be presented in an aggregated format to ensure complete confidentiality. The results of the survey may be used and disseminated in any format the researcher deems appropriate. There is no cost other than the time spent in completing this questionnaire.

Respondent's participation is voluntary and participation can be withdrawn at any time without penalty. By completing the survey, you indicate that you voluntarily participate in this research.

If you have any concerns, please contact me or my supervisor. Our details are provided below.

**Thank You**

| | | | |
|---|---|---|---|
| Researcher: | Dale Rosenberg | Supervisor: | Howard Fox |
| Email: | DPRosenberg@Gmail.com | Email: | foxh@gibs.co.za |
| Phone: | +27 84-851-3412 | Phone: | +27 11 771 4000 |

# PLEASE BE AS HONEST AS POSSIBLE.

## GENDER:

| | | | |
|---|---|---|---|
| Male | | Female | |

## AGE:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 25 – 30 | | 31 – 35 | | 36 – 40 | | 41 – 45 | | 46+ | |

## LANGUAGE:

| | | | |
|---|---|---|---|
| Afrikaans | | Swazi | |
| English | | Tshivenda | |
| Ndebele | | Xhosa | |
| Sepedi | | Tsonga | |
| Sesotho | | Zulu | |
| Setswana | | Other | |

## EMPLOYMENT STATUS

| | | | |
|---|---|---|---|
| Employed full time | | Employed part time | |
| Self-employed | | Not employed | |

# PLEASE BE AS HONEST AS POSSIBLE.

## LOCATION BASED SERVICES:

A **Location-Based Service** (LBS) is an information or entertainment service that is offered by a company to consumers based on the company using the location information of that consumer, which is available through their mobile device, to analyse that consumer's information or to market to that consumer. In order for LBS to work properly, the supplier must be able to use the location of the consumer to make the service relevant to the consumer at that moment in time.

> When location information is **CONSOLIDATED** this means that the consumer's individual information cannot be seen and therefore they maintain their privacy.

> If the location information is **NOT CONSOLIDATED** then the consumer's individual information can be seen and therefore their privacy is NOT maintained.

Some examples of location-based services are:

- Recommending social events in a city;
- Requesting the nearest business or service, such as an ATM or restaurant;
- Turn by turn navigation to any address;
- Locating people on a map displayed on the mobile phone;

Please read the following ten questions and indicate your feeling for each one:

| # | Question | Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree |
|---|---|---|---|---|---|---|
| 1. | I am concerned with privacy | | | | | |
| 2. | I value my privacy above all else | | | | | |
| 3. | I will give up some private information for the right offer | | | | | |
| 4. | I care if someone knows where I am | | | | | |
| 5. | I only want my friends to know where I am | | | | | |
| 6. | I will be comfortable with anyone knowing my location | | | | | |
| 7. | The offer is only valuable to me if it is relevant at that moment in time | | | | | |
| 8. | I will only relinquish my data if the offer is valuable in a relevance sense | | | | | |
| 9. | No relevant offer would entice me to give up private information | | | | | |
| 10. | The amount of value will influence how much data I will share | | | | | |

The next few pages detail **THREE** different scenarios, please read each one carefully and then answer the questions that follow.

## SCENARIO ONE:

You continually shop at a store which you like, that sells low value items (<R500 per item). The store forms part of a larger national chain with stores in all the major provinces.

They offer you, a regular customer, the opportunity to earn a discount if you are prepared to allow the store to track your movements. They will be able to track your **LOCATION** when you are within 100 metres of any of their stores.

Please read the questions below and confirm **FOR EACH OF THE QUESTIONS AND DISCOUNTS** where on the range (from **Uncomfortable** to **Comfortable**) you would be, based on the store offering you a discount on each purchase, assuming you purchase **ONE ITEM i.e. Spend R500**:

| # | Question | Discount offer made Percent / Rand Amount | Uncomfortable | Slightly Uncomfortable | Neutral | Slightly Comfortable | Comfortable |
|---|---|---|---|---|---|---|---|
| 1. | Tracking of your movements when you are ***INSIDE*** the store, with your ***INFORMATION CONSOLIDATED*** with other consumers i.e. your individual movement s are **NOT** identifiable. | 5% / R25 | | | | | |
| | | 10% / R50 | | | | | |
| | | 15% / R75 | | | | | |
| | | 20% / R100 | | | | | |
| | | 40% / R200 | | | | | |
| 2. | Tracking of your movements when you are ***INSIDE*** the store, with your ***INFORMATION NOT CONSOLIDATED*** with other consumers i.e. your individual movement s are identifiable. | 5% / R25 | | | | | |
| | | 10% / R50 | | | | | |
| | | 15% / R75 | | | | | |
| | | 20% / R100 | | | | | |
| | | 40% / R200 | | | | | |
| 3. | Tracking of your movements when you are ***OUTSIDE AND INSIDE*** the store, with your ***INFORMATION CONSOLIDATED*** with other consumers i.e. your individual movement s are **NOT** identifiable. | 5% / R25 | | | | | |
| | | 10% / R50 | | | | | |
| | | 15% / R75 | | | | | |
| | | 20% / R100 | | | | | |
| | | 40% / R200 | | | | | |
| 4. | Tracking of your movements when you are ***OUTSIDE AND INSIDE*** the store, with your ***INFORMATION NOT CONSOLIDATED*** with other consumers i.e. your individual movement s are identifiable. | 5% / R25 | | | | | |
| | | 10% / R50 | | | | | |
| | | 15% / R75 | | | | | |
| | | 20% / R100 | | | | | |
| | | 40% / R200 | | | | | |

## SCENARIO TWO:

You are about to buy a luxury car, the purchase price is more than R300, 000. It is a car that you greatly desire; you made the decision to purchase this car.

The sales person says that you cannot have any discount. When you start negotiating with the sales person, they mention that if you allow the car company to track your location while driving, they would be prepared to give you a discount on the purchase price. They will be able to track your movements in the car to within 20 metres by using the **LOCATION** information from your cell phone.

Please read the questions below and **FOR EACH OF THE QUESTIONS AND DISCOUNTS** confirm where on the range (from **Uncomfortable** to **Comfortable**) you would be, based on the car company offering you a discount on the purchase price:

| # | Question | Discount offer made Percent / Rand Amount | Uncomfortable | Slightly Uncomfortable | Neutral | Slightly Comfortable | Comfortable |
|---|---|---|---|---|---|---|---|
| 1. | Tracking of your car's movements to allow ***DRIVING TREND ANALYSIS*** with your ***INFORMATION CONSOLIDATED*** with other consumers i.e. your individual movement s are **NOT** identifiable. | 5% / R15000 | | | | | |
| | | 10% / R30 000 | | | | | |
| | | 15% / R45 000 | | | | | |
| | | 20% / R60 000 | | | | | |
| | | 40% / R120 000 | | | | | |
| 2. | Tracking of your car's movements to allow ***DRIVING TREND ANALYSIS*** with your ***INFORMATION NOT CONSOLIDATED*** with other consumers i.e. your individual movement s are identifiable. | 5% / R15000 | | | | | |
| | | 10% / R30 000 | | | | | |
| | | 15% / R45 000 | | | | | |
| | | 20% / R60 000 | | | | | |
| | | 40% / R120 000 | | | | | |
| 3. | Tracking of your car's movements to allow ***DRIVING TREND ANALYSIS AND MARKETING USE*** with your ***INFORMATION CONSOLIDATED*** with other consumers i.e. your individual movement s are **NOT** identifiable. | 5% / R15000 | | | | | |
| | | 10% / R30 000 | | | | | |
| | | 15% / R45 000 | | | | | |
| | | 20% / R60 000 | | | | | |
| | | 40% / R120 000 | | | | | |
| 4. | Tracking of your car's movements to allow ***DRIVING TREND ANALYSIS AND MARKETING USE*** with your ***INFORMATION NOT CONSOLIDATED*** with other consumers i.e. your individual movement s are identifiable. | 5% / R15000 | | | | | |
| | | 10% / R30 000 | | | | | |
| | | 15% / R45 000 | | | | | |
| | | 20% / R60 000 | | | | | |
| | | 40% / R120 000 | | | | | |

## SCENARIO THREE:

You want to save money on your car insurance and you find a company who offers SIGNIFICANTLY reduced premiums. When you enquire how they do this, you are told that they monitor how you drive and where you drive and based on this, they reduce you premiums by a certain percentage. They will track your **LOCATION** while you are driving.

Please read the questions below and **FOR EACH OF THE QUESTIONS AND DISCOUNTS** confirm where on the range (from **Uncomfortable** to **Comfortable**) you would be, based on the car insurance company offering you a discount on your premium with your premium being R800:

| **#** | **Question** | **Discount offer made Percent / Rand Amount** | **Uncomfortable** | **Slightly Uncomfortable** | **Neutral** | **Slightly Comfortable** | **Comfortable** |
|---|---|---|---|---|---|---|---|
| 1. | Tracking of your ***AREAS DRIVEN IN*** and ***SPEED***. | 5% / R40pm | | | | | |
| | | 10% / R80pm | | | | | |
| | | 15% / R120pm | | | | | |
| | | 20% / R160pm | | | | | |
| | | 40% / R320pm | | | | | |
| 2. | Tracking of your ***AREAS DRIVEN IN***, ***SPEED*** and ***BRAKING DISTANCES***. | 5% / R40pm | | | | | |
| | | 10% / R80pm | | | | | |
| | | 15% / R120pm | | | | | |
| | | 20% / R160pm | | | | | |
| | | 40% / R320pm | | | | | |
| 3. | Tracking of your ***AREAS DRIVEN IN***, ***SPEED***, ***BRAKING DISTANCES*** and ***DRIVING STYLE*** (aggressive / non-aggressive). | 5% / R40pm | | | | | |
| | | 10% / R80pm | | | | | |
| | | 15% / R120pm | | | | | |
| | | 20% / R160pm | | | | | |
| | | 40% / R320pm | | | | | |
| 4. | Tracking of YOUR ***AREAS DRIVEN IN***, ***SPEED***, ***BRAKING DISTANCES***, ***DRIVING STYLE*** (aggressive / non-aggressive) and ***TIME OF TRAVEL***. | 5% / R40pm | | | | | |
| | | 10% / R80pm | | | | | |
| | | 15% / R120pm | | | | | |
| | | 20% / R160pm | | | | | |
| | | 40% / R320pm | | | | | |