Ethical concerns of consumers in mobile marketing

Bernardus Franco Maseke

Department of Management Science,
University of Namibia,
Windhoek, Namibia
Email: fmaseke@gmail.com

Abstract: This paper investigated various ethical concerns in mobile marketing. Smartphones have become intelligent devices which store a wide range of rich detail about the owner's personal life. Third-party applications which can lead to unforeseen privacy and security risks have become a treat. The research questions: focused on privacy concerns, malware and spam and permission marketing concerns of consumers in Namibia? Positivist quantitative survey research was applied in this study. A sample size of 384 consumers were selected from the target population 500,000 in Windhoek. This study found that consumers are aware of privacy concerns in Namibia. This is similar to what was found in a previous studies. This study also found that consumers are concerned about malware and spam in Namibia, which is a general concern of mobile device users globally. Privacy concerns awareness, spam, malware filtering should become prerequisites for mobile marketing to be effective.

Keywords: ethics mobile marketing; privacy; mobile spam; malware; permission marketing.

Reference to this paper should be made as follows: Maseke, B.F. (2020) 'Ethical concerns of consumers in mobile marketing', *Int. J. Markets and Business Systems*, Vol. 4, No. 1, pp.1–16.

Biographical notes: Bernardus Franco Maseke received his Doctorate of Business Administration from the University of Namibia Business School, and a Lecturer in the Department of Management Sciences at the University of Namibia. He is responsible for lecturing strategic marketing, strategic HR and business research methodology. His research interests are in mobile and electronic marketing and ethics in marketing.

1 Introduction

A mobile device is perceived as a personalised technology, providing consumers with a feeling of dependency and companionship, according to Goasduff and Pettey (2012). Büscher et al. (2010) suggest that attitudes with regards to privacy, control and permission in mobile marketing may vary from person to person, because some users may be more attached to their mobiles than others. In light of this Persaud and Azhar (2012, p.14) concluded that the importance attached to the mobile phone determines consumers' readiness to release personal data in mobile marketing. This paper investigated the different types of ethical concerns related to mobile marketing, in

particular focused on the mobile device as an easy target for cyber-crimes, hacking and privacy invasion.

Goasduff and Pettey (2012) state that "malware for smartphones evolved in the same trend as malware for PCs: hence, as more users download and install third-party applications for smartphones, the chances of installing malicious programs increases as well." Furthermore, "since users increasingly exploit smartphones for sensitive transactions, such as online shopping and banking, and there are likely to be more threats designed to generate profits for the attackers" [Smalley, (2012), p.14]. In the same trend, there has been an increase in attention to the security issues from security researchers with regards to privacy invasion.

Currently mobile devices (in particular smartphones) "provide lots of the capabilities of traditional personal computers (PCs) and, in addition, offer a large selection of connectivity options, such as Bluetooth, GSM, GPRS, UMTS, and HSPA" [La Polla et al., (2013), p.18]. This "plethora of appealing features has led to a widespread diffusion of smartphones that, as a result, are now an ideal target for attackers" (Leino, 2010). In the beginning, "smartphones came packaged with standardized operating system (OS): less heterogeneity in OS allowed attackers to exploit just a single vulnerability to attack a large number of different kinds of devices by causing major security outbreaks" [La Polla et al., (2013), p.19].

1.1 This paper is edged on the following research questions

The research questions in this paper are threefold:

1 What are the *privacy concerns* of mobile marketing consumers in Namibia?

2 To what extent is *malware and spam* a concern for Namibian mobile marketing consumers?

3 What are the privacy and *permission marketing* concerns of consumers in Namibia?

1.2 Hypothesis

Hypothesis 1 Consumers are not aware of privacy concerns in Namibia.

Hypothesis 2 Consumers are not concerned about malware and spam in Namibia.

Hypothesis 3 Consumers are not concerned about privacy and permission marketing in Namibia.

2 Literature review

2.1 Fundamental issues in mobile marketing

Currently mobile devices (in particular smartphones) "provide lots of the capabilities of traditional personal computers (PCs) and, in addition, offer a large selection of connectivity options, such as Bluetooth, GSM, GPRS, UMTS, and HSPA" [La Polla et al., (2013), p.18]. This "plethora of appealing features has led to a widespread diffusion of smartphones that, as a result, are now an ideal target for attackers" (Leino,

2010). In the beginning, "smartphones came packaged with standardized operating system (OS): less heterogeneity in OS allowed attackers to exploit just a single vulnerability to attack a large number of different kinds of devices by causing major security outbreaks" [La Polla et al., (2013), p.19]. The number of operating systems for mobile devices (Symbian OS, Windows Mobile, Android and iPhone OS) has become more and is exposing users to various cyber attackers.

Goasduff and Pettey (2012) state that "malware for smartphones evolved in the same trend as malware for PCs: hence, as more users download and install third-party applications for smartphones, the chances of installing malicious programs increases as well." Furthermore, "since users increasingly exploit smartphones for sensitive transactions, such as online shopping and banking, and there are likely to be more threats designed to generate profits for the attackers" [Smalley, (2012), p.14]. In the same trend, there has been an increase in attention to the security issues from security researchers with regards to privacy invasion.

A mobile device is perceived as a personalised technology, providing consumers with a feeling of dependency and companionship, according to Goasduff and Pettey (2012). Büscher et al. (2010) suggest that attitudes with regards to privacy, control and permission in Mobile Marketing may vary from person to person, because some users may be more attached to their mobiles than others. In light of this Persaud and Azhar (2012, p.14) concluded that the importance attached to the mobile phone determines consumers' readiness to release personal data in mobile marketing.

2.2 Privacy concerns

Leontiadis et al. (2012) submit that since privacy concerns are becoming more visible, there an increase in the amount of free mobile applications. For example, "in July 2011 Google announced that there are more than 250,000 applications (up from 5,000 applications less than two years ago) in the Android market that were downloaded more than 8 billion times by more than 100 million Android devices" [Leontiadis et al., (2012), p.189]. Free offers and financial incentives offered by the mobile advertising industry allow developers to distribute applications to a wider audience and is therefore and integral part for marketers. However, "the success of the advertising industry is interlinked with the accurate profiling of users who are the recipients of targeted advertisement" (Felt et al., 2012). This means that a successful advertisement campaign "requires access to personal information that can potentially be considered private" (Felt et al., 2012). Mobile phones have become a "ubiquitous piece of technology that is carried by virtually every individual throughout their daily life." The improved capabilities of "smartphones (computation, sensing and communication) have transformed them into avatars of the individual in the digital world" [Leontiadis et al., (2012), p.189]. Therefore, it cannot not be ignored that smartphones have become custodians of individuals' social networking patterns, mobility habits, pictures, videos, web history and phonebook contacts.

Smartphones have become advanced, intelligent devices which are able to process and store a wide range of personal information. This is echoed by Enck et al. (2015) who submit that "the combined information that can be accessed through a smartphone is vast, rich in detail, and covers a variety of the owner's personal life" [Leontiadis et al., (2012), p.189]. Enck et al. (2015) further suggest that "at the same time, the proliferation of

smartphones can be largely attributed to their ability to host a range of third-party applications that can be downloaded and installed by the user." It can however not be overlooked that "permitting third-party applications to operate within a device holding private information about their owner can lead to unforeseen privacy and security risks" (Felt et al., 2012). While "current solutions to privacy can offer some level of protection to the user, they are unable to consider the repercussions for a market primarily driven by accurate profiling of consumer behaviour" [Ferrer, (2007), p.31]. Nevertheless, consumers need to understand that data collected through mobile application is used by marketers to generate revenue that eventually pays for the free applications (Leontiadis et al., 2012).

According to Culnan and Williams (2009), common agreement between retailers and consumers should exist, where "consumers are willing to reveal personal information for economic or social benefits, provided that their personal information will consequently only be used fairly and will not result in negative consequences in the future." For such an agreement to work, Culnan and Williams (2009) also stress it would only be possible for such an agreement to work if retailers are open and honest about their motives for collecting consumer information and not betray consumers' confidence.

A virus "is a piece of code that can replicate itself and (the) replica of a virus can infect other programs, boot sector, or files by inserting or attaching itself to them" (Shabtai et al., 2010). A worm is "a program that makes copies of itself, typically from one device to another one, using different transport mechanisms through an existing network without any user intervention" [Felt et al., (2011a), p.141]. Usually "a worm does not attach to existing programs of the infected host but it may damage and compromise the security of the device or consume network bandwidth" [Shabtai et al., (2010), p.19]. Again, viruses are another threat to both mobile marketing and the mobile device as it has the ability to completely destroy the mobile device.

A Trojan is "software that appears to provide some functionalities but, instead, contains a malicious program" [Wang et al., (2016), p.82], while rootkits achieve their malicious goal by "infecting the operating system (OS): usually, they hide malicious user-space processes and files or install Trojans, disable firewalls and anti-virus" [Damopoulos et al., (2012), p.15].

Rootkits can "operate stealthily since they directly apply changes to the OS and, hence, can retain longer control over the infected devices" [Felt et al., (2011b), p.142]. This type of malware infection can become costly, especially if the OS cannot be self-restored and they have to dive into their pockets to get the device for repaired.

Finally, a "botnet is a set of devices that are infected by a virus that gives an attacker the ability to remotely control them" [Shabtai et al., (2010), p.19]. Botnets "represent a serious security threat on the internet and most of them are developed for organized crime doing attacks to gain money" [Arnold and Becker, (2010), p.19]. Botnets seem to pose an extremely dangerous threat to consumers since access the mobile device remotely and can go undetected, making the consumers more vulnerable to privacy intrusion.

Mobile "malware can spread through several and distinct vectors, such as an SMS containing a link to a site where a user can download the malicious code, an MMS with infected attachments, or infected programs received via Bluetooth" [Shabtai et al., (2010), p.19]. The "main goals of malware targeted at smartphones include theft of personal data stored in the phone or the user's credit" [Damopoulos et al., (2012), p.15].

Users may not become aware when their mobile device has been infected with malware and may assume their device is malfunctioning or simply needs to be replaced.

Consumer education on malware can be used to reduce the threat of malware on mobile marketing and also to create awareness and sensitisation on how to curb the effects of malware on privacy intrusion.

2.3 Permission marketing

Carroll et al. (2007) state that permission marketing is focused on nurturing a relationship with customers based on consent to receive and accept information from the businesses. Carroll et al. (2007) stressed that "permission marketing is a two-way mobile communications process between the customer and the mobile marketer" (business).

Basheer and Ibrahim (2010) and Tanakinjal et al. (2010) suggest that "trust influence consumers' intention to participate in permission-based adverting programs especially in mobile marketing, where risk and uncertainty is very high compared to other marketing types." Kautonen et al. (2007) advocate personal and organisational trust as two noteworthy variables that directly influence permission marketing. Personal trust develops from the interaction between a customer and a business and experiences of friends and family and associates. Institutional trust is associated with a much larger audience whereas the institutional environment and reputation are based on trust.

In the context of mobile marketing, institutional trust is frequently denoted as consumers' media perception of the marketing organisation (Kautonen et al., 2007). The media has the ability to positively or negatively influence the trust consumers can have on innovations such as mobile marketing. Media reports should therefore emphasise both the benefits and drawbacks of mobile marketing on consumers and how these drawbacks can be overcome. It is therefore critical that consumers' education about security devices such as anti-spam, malware and viruses are also advocated through the media. This will reduce the threat on institutional trust and consumer perception marketing organisations as well as allow consumers to have an open-minded approach to mobile marketing and safely enjoy its benefits.

Most studies provide controverting views on the importance of the two trust variables. For example Amir et al. (2013) and Welter and Kautonen (2005) advise that categorically personal trust play a more important role compared to institutional in mobile marketing as a whole experience. While Jayawardhena et al. (2009) suggest "institutional trust as the most important variable of mobile marketing permission compared to personal trust."

Furthermore, firms must manage two critical aspects to ensure the success of a permission-based marketing programme: the customer's opt-in and opt-out timing (Kumar et al., 2014). Recent research on permission marketing has explored several factors that influence a customer's eagerness for permission for marketing, brand image and trust (Jayawardhena et al., 2009), brand equity and previous relationship with the organisation (Tezinde et al., 2002), income, gender, advertising message volume, previous experience with mobile ads (Barnes and Scornavacca, 2008). Whereas customers' opt-in decisions are influenced by the aforementioned factors, it is also important to identify the drivers of customers' opt-out decisions so that firms can make targeted efforts to retain their existing subscribers (Kumar et al., 2014).

Much earlier research on customers' opt-out decisions has revealed that message relevance and monetary benefits may also positively influence customers' interest in a permission marketing (Krishnamurthy, 2006) and that highly personalised messages have

a tendency to cause customers to opt out (Marinova et al., 2002). In agreement, (Chittenden and Rettie, 2003) submit that protracted e-mails and mobile offerings with fewer links tend to result in higher unsubscribe rates.

2.4 Code of conduct for mobile marketing

The code of conduct for mobile marketing is a universal 'set of rules' developed for marketers by the Mobile Marketing Association (MMA) to provide guidance to marketers. These 'set of rules' are anchored in legislation from various countries and has been adopted by organisations worldwide.

The MMA (2008, p.1) "is the premier global non-profit trade association established to lead the growth of mobile marketing and its associated technologies." The MMA is an "action-oriented organization designed to clear obstacles to market development, establish mobile media guidelines and best practices for sustainable growth, and evangelize the use of the mobile channel" [MMA, (2008), p.1]. The association was established by a group of organisations using mobile marking as a means to promote their products and that felt the need for consumer education and protection. The association has "more than 650 member companies, representing over forty countries around the globe, include all members of the mobile media ecosystem" [MMA, (2008), p.1]. The MMA's "global headquarters are located in the United States and in 2007 it formed the North America (NA), Europe, Middle East and Africa (EMEA), Latin America (LATAM) and Asia Pacific (APAC) branches" [MMA, (2008), p.3].

The 'code of conduct' was, amongst others, also developed by the MMA (2008) to reduce malware and spam and to protect the consumers against unethical Mobile Marketing practices. The 'code of conduct' consists of six ethical values categorised as the 'six C's of privacy' in mobile marketing, specifically:

- *Notice:* "Mobile marketers must provide users with notice." Notice is fairly easy to comprehend and is submitted by the MMA as follows. "Notice should include information sufficient to permit a user to make an informed decision about his or her choices on how that information is used for that marketing program" (MMA, 2008).

  > "Notice is the fundamental principle in the MMA Privacy Code of Conduct and must be enforced at all times. Mobile marketers must inform the user of both the marketers' identity or products and services offered, and the key terms and conditions that govern an interaction between the marketer and the user's mobile device." [MMA, (2008), p.4]

- *Choice and consent:* Consumers have the right to choose the type of product or service as well as the freedom to accept or reject offers. The MMA (2008, p.4) states that:

  > "Mobile marketers must respect the right of users to regulate which mobile messages they receive. This could be done by obtaining users' consent with explicit opt-in and -out options. This can be accomplished via an SMS or MMS opt-in process, a voice response, website registration, other MMA-recognized methods or other legitimate methods. Explanations on how to opt out of multiple messaging programs must be provided on a reasonably frequent basis."

- *Customisation:* "Mobile marketers must ensure that mobile marketing reflects broad customer expectations in any applicable national marketplace" [MMA, (2008), p.4].

  > "Marketing through the mobile channel is most effective when appropriately targeted, and user information collected for marketing purposes should be used to tailor such marketing to the interests of the user when available." [MMA, (2008), p.5]
  >
  > "Mobile marketers must take reasonable steps to ensure that user information they collect for the purpose of delivering targeted advertising is handled responsibly, sensitively and in compliance with applicable law." (MMA, 2008)

- *Constraint:* Mobile marketers "should target and limit mobile messages to that which users have requested. Mobile messages should provide value to the user. Value may be delivered in multiple ways, including: product and service enhancements, reminders, sweepstakes, contests, requested information, entertainment, or discounts" [MMA, (2008), p5].

- *Security:* Mobile marketers must "implement reasonable technical, administrative and physical procedures to protect user information collected in connection with mobile marketing programs from unauthorized use, alteration, disclosure, distribution, or access" [MMA, (2008), p.5].

- *Enforcement and accountability:* The MMA:

  > "Expects its members to comply with the MMA Global Code of Conduct and has incorporated the code into applicable MMA guidelines as they apply to mobile marketers operating around the world, including the MMA Consumer Best Practices (CBP) guidelines, as applicable for certain national markets. Until such time as the code can be enforced effectively by a third party enforcement organization, mobile marketers are expected to use evaluations of their practices to certify compliance with the code. Since mobile marketing involves the use of users' personal information, privacy is pivotal and must be taken into consideration in developing mobile marketing offerings."

  Norris (2003, p.18) recognised when obtaining and processing of location-based data, businesses must be guided by local respective legislations to ensure consumers' data cannot be sourced or utilised prior to the user's consent.

3 Methodology

Quantitative research was found to be more appropriate than a qualitative and was thus selected. The positivist epistemology philosophical foundation was decided to be appropriate and was selected for this study. Subsequently an overview discussion on the various issues on the available research approaches and a justification for the selection of the survey as a research approach was provided. The study therefore involved the use of the survey method. The survey was done in two stages: the pilot study which was distributed to 33 target sample participants to test the validity and reliability of all the questions in the research instrument. The second part was the main survey which was done on 192 male and 192 females or a total of 384 participants.

3.1 Sampling

This study used probability sampling because of its advantage of being unbiased and representative of the entire population (Herbst and Coldwell, 2004) In support of probability sampling (Saunders et al., 2012) suggest that "probability sampling is commonly associated with survey research strategies where you need to make inferences from the sample about a population to answer the research questions." In particular systematic random sampling was used to sample the population. A sample size of 384 consumers were selected from the target population in Windhoek, using a standard formula for a sample size: $SS = Z^2 \times (p) \times (1 - p) / C^2$, which is used for an infinite population (where the population is greater than 50,000 (Freedman et al., 2007) or 10,000.

$$SS = \frac{Z^2 \times (p) \times (1-p)}{C^2}$$

SS sample size

Z *Z*-value (e.g., 1.96 for a 95% confidence level)

P percentage of population picking a choice, expressed as decimal

C confidence interval, expressed as decimal (e.g., 0.05)

$$SS = \frac{1.96^2 \times 0.5 \times 0.5}{0.05^2} = \frac{3.8416 \times 0.25}{0.0025} = 384 \text{ respondents}$$

Therefore, at a confidence level of 95% from a population of 500,000 consumers, the sample for consumers was 384. These were drawn from the Local shopping malls because most of these mobile marketing consumers shop at major shopping malls.

3.2 Research instrument

The research instrument was a self-administered structured questionnaire. Saunders et al. (2012) explain questionnaires as appropriate for case study and experiment strategies but strongly support the use of questioners in the survey research strategy. The questionnaire included a cover letter that briefly introduced the researcher, the study, the purpose of the research and provided an assurance of respondents' confidentiality. The questionnaire consisted of demographics and three sections namely: privacy concerns, sperm and mail ware and permission marketing. Each section consisted of between 4 to 6 closed-ended questions. The questions were measured on a five-point Likert scales. The three basic properties of Likert scales are reliability, validity, and sensitivity and the extent to which research has benefited all three is astonishing (Leung, 2011).

3.2.1 Validity

Saunders et al. (2012) submit "validity is the degree to which a research instrument measures what it is intended to measure. Validity can be carried out using the content, criterion and construct validity approach." Content and construct validity were used during this study. Both content and construct validity were examined through a pre- and post-pilot test for this study.

3.2.2 Reliability

In addition reliability of the scales in the research instrument was tested by using the Cronbach alpha coefficient to determine the degree of internal consistency between the multiple measurements. To further ensure reliability of the research instrument, a pilot study of the research instrument was tested on a sample of 20 random respondents from population of the study. The purpose of the pilot study was to:

1 determine the willingness of the respondents to participate in the study

2 to have pre-knowledge of the reactions of the respondents

3 to determine the suitability and reliability of the research instrument (Christensen et al., 2014).

The results of the pilot study showed that the respondents understood the question items in the questionnaire. This showed that the measuring instrument not only measured what it set out to measure, but that it was consistent in doing so. The reliability test was used to compute the pre-test reliability, and the result proved positive as all variables exceeded the minimum acceptable value of 0.60 (Christensen et al., 2014). After the pilot study, question items in the questionnaire were adjusted and clarified for the final survey.

3.3 Data analysis

The SPSS statistical program descriptive and inferential statistics functions were used to analyse the data collected from the questionnaire. In particular frequency tabulation, measures of distribution, measures of spread, skew and kurtosis from the descriptive functions would be used to give the data description (Zikmund et al., 2013). Descriptive statistics were also used to determine the mean and standard deviation scores of the dimensions and factor influencing attitude. Frequency and percentage distribution were used to analyse the demographic characteristics. Thus inferential statistics were used to assess the strength of the relationship between independent (causal) variables and dependent (effect) variables (Zikmund et al., 2013).

Confirmatory factor analysis "is a statistical tool/technique which was used to verify the factor structure of the observed variables/constructs. It was also used to test whether a specified set of constructs is influencing responses in a predicted way" (Brown, 2014). CFA was used to validity the research instrument.

Furthermore, once CFA AOMS 24 software was used to perform multiple regression analysis in testing the research hypotheses. AMOS is a powerful and graphical, easy-to use structural equation modelling (SEM) software. It "creates much realistic models than standard multivariate statistics or multiple regression models. It is used to estimate, assess, and then present a model in an intuitive path diagram to show hypothesised relationships among variables" (Brown, 2014).

4 Results and findings

This section discusses the findings and draws inferences from statistical findings in the previous chapter. This will include both theoretical and empirical findings. The section begins by introducing a discussion on the research questions, followed by a summary of

the hypothesis test and a synthesis of empirical findings and theoretical findings. Furthermore, implications of findings are expounded which highlights the contribution to body of scientific knowledge.

4.1 Research questions

This study constituted three research questions, which were formulated from the research problem and the preliminary literature review. In addition, three hypothesis were constructed from the research questions and the Literature review. The hypothesis and research questions were subsequently used to develop the research instrument. Based on the following research questions, this study wanted to determine what the privacy concerns of mobile marketing consumers in Namibia were. To what extent malware and spam were a concern for Namibian mobile marketing consumers. The privacy and permission marketing concerns of consumers in Namibia. The results of the hypothesis test were subsequently used to reveal theoretical similarities and differences on the findings of this study and previous studies.

4.2 Hypothesis test

Hypothesis 1 Ho consumers are not aware of privacy concerns in Namibia.

Hypothesis 2 Ho consumers are not concerned about malware and spam in Namibia.

Hypothesis 3 Ho consumers are not concerned about privacy and permission marketing in Namibia.

$\alpha = 0.05$

Critical ratio (CR) threshold 1.96.

Table 1 Regression weights

	Estimate	*S.E.*	*C.R.*	*P*	*Label*
Consumer awareness ← privacy concerns	0.237	0.039	6.060	***	par_1
Consumer concerns ← malware and sperm	0.442	0.043	10.301	***	par_2
Consumer concerns ← privacy and permission	0.209	0.047	4.403	***	par_3

Table 1 illustrates the standard error (SE), CR and p values (P) of the regression weights for privacy concerns, malware and sperm and privacy and permission toward consumer concerns. The p value (***) indicates that all factors are statistically significant towards consumer concerns. In addition the critical values for all factors are greater than 1.96 making them all statistically significant to consumer concerns.

Table 2 Standardised path regression weights

	Estimate
Consumer awareness ← privacy concerns	0.263
Consumer concerns ← malware and sperm	0.448
Consumer concerns ← privacy and permission	0.208

The standardised path regression weights Table 2 indicates the contribution of each factor to consumer concerns. Malware and sperm factor has the highest contribution of 0.448.

Table 3 Squared multiple correlations

	Estimate
Consumer concerns	0.331

The squared multiple correlation Table 3 indicates the variations of all three factors which account for 33% or 0.331 variance of consumer attitudes.

Table 4 Summary of hypotheses test

Variable	*Hypothesis*		*Influence direction*	*Significance*	*Findings*
1	H0	Consumers are not aware of privacy concerns in Namibia.	+	Insignificant	Null hypothesis rejected
2	H0	Consumers are not concerned about malware and spam in Namibia.	+	Significant	Null hypothesis rejected
3	H0	Consumers are not concerned about privacy and permission marketing in Namibia.	+	Significant	Null hypothesis rejected

The findings of this study are summarised in Table 4. According to Table 4 all hypothesis were statistically significant. In addition the table reveals that no differences exist of directional influences of all three hypothesis.

4.3 Discussion of findings

4.3.1 Discussion of Hypothesis 1

This study found that consumers are aware of privacy concerns in Namibia. This is similar to what was found in a study by Culnan and Williams (2009), that a common agreement between retailers and consumers should exist, where "consumers are willing to reveal personal information for economic or social benefits, provided that their personal information will consequently only be used fairly and will not result in negative consequences in the future." For such an agreement to work, Culnan and Williams (2009) also stress it would only be possible for such an agreement to work if retailers are open and honest about their motives for collecting consumer information and not betray consumers' confidence.

4.3.2 Discussion of Hypothesis 2

This study found that consumers are concerned about malware and spam in Namibia, which is a general concern of mobile device users. Spamming and malware are two potential consumer hindrances to the success of mobile marketing. Mobile spam is "unsolicited, unwanted communications in the form of e-mail, text messages and multimedia messages" [Arnold and Becker, (2010), p.13]. Krum (2010) explains that organisations should respect customer's space by not bugging them with non-stop

advertising messages but rather seek to build a cordial relationship with consumers. In the same light, Scott (2007) emphasised that "consumers want participation and not propaganda", hence propaganda messages irritate and make customers become wary of mobile marketing, consumers desire strong relationship with firms based on convenience and choice. Moreover, Scott (2009) recommended that organisations must consider significant issues such as timing, frequency and content of their advertising messages, especially for customers that have subscribed and agreed to receive marketing messages. This may cause un-subscriptions resulting in consumers declining to receive further messages due to becoming overwhelmed by lots of messages received at an inappropriate time or moment (Arnold and Becker, 2010). Watson et al. (2013) propose that permission-based marketing should be applied in the mobile marketing context of mobile marketing for it to be effective.

Users may not become aware when their mobile device has been infected with malware and may assume their device is malfunctioning or simply needs to be replaced. Consumer education on malware can be used to reduce the threat of malware on mobile marketing and also to create awareness and sensitisation on how to curb the effects of malware on privacy intrusion.

4.3.3 Discussion of Hypothesis 3

This study found consumers are not concerned about privacy and permission marketing in Namibia. This also seem to be consistent with what way found in the literature and is a global trend among mobile device users. Carroll et al. (2007) state that permission marketing is focused on nurturing a relationship with customers based on consent to receive and accept information from the businesses. Carroll et al. (2007) stressed that "permission marketing is a two-way mobile communications process between the customer and the mobile marketer" (business).

In the context of mobile marketing, institutional trust is frequently denoted as consumers' media perception of the marketing organisation (Kautonen et al., 2007). The media has the ability to positively or negatively influence the trust consumers can have on innovations such as mobile marketing. Media reports should therefore emphasise both the benefits and drawbacks of mobile marketing on consumers and how these drawbacks can be overcome. It is therefore critical that consumers' education about security devices such as anti-spam, malware and viruses are also advocated through the media. This will reduce the threat on institutional trust and consumer perception marketing organisations as well as allow consumers to have an open-minded approach to mobile marketing and safely enjoy its benefits.

Most studies provide controverting views on the importance of the two trust variables. For example Amir et al. (2013) and Welter and Kautonen (2005) advise that categorically personal trust play a more important role compared to institutional in mobile marketing as a whole experience. While Jayawardhena et al. (2009) suggest "institutional trust as the most important variable of mobile marketing permission compared to personal trust".

Furthermore, firms must manage two critical aspects to ensure the success of a permission-based marketing programme: the customer's opt-in and opt-out timing (Kumar et al., 2014).

5 Conclusions and recommendations

A synopses of the study highlights key theoretical and empirical findings. All three research questions were answered. The researcher suggests that contrary to traditional marketing channels, the great advantage of marketing on mobile devices is that retailers can target a specific audience in a direct and personal manner. By developing a database, mobile marketing adverts on promotional and relational content should be personalised according to customers' profiles. Furthermore, the interest of the consumer must be investigated properly to send adverts more precisely. Privacy concerns and awareness, spam, malware should become the prerequisites for mobile marketing to be effective. A further recommendation is that the result of this study should be used by retailers and marketers to better understand the variables and factors that contribute to consumers' Privacy concerns and awareness, spam, malware challenges in receiving and responding to advertisements on mobile devices.

The government, through its law-making arm called the national council and the telecommunication policy regulator known as the Communications Regulatory Authority of Namibia (CRAN) should enact a law guiding the use of unsolicited electronic messages to mobile phone devices, in order to ensure consumers' privacy and security of consumer data and information. The legislation must include all electronic messages being sent as text or pre-recorded voice messages between mobile devices for the purpose of marketing, advertising, promoting or offering goods, services, business opportunities or from organisations to the consumers' or mobile phone user must be permission-based.

5.1 Future research recommendations

Since Namibia was the focal point of this study research conducted in Namibia excluded other countries in the region, additional research could be carried out continent-wide so as to include the opinions of consumers from other countries.

In addition, the repetition of this study in other countries focusing on regional differences could be studied.

a A longitudinal study to observe trends in changes in consumer attitude as a result of the mobile technology advancement could be carried out in the further.

b Imminent research could be done to aid mobile application developers and organisations in developing more effective and safe mobile device applications.

c Research exploring factors influencing attitude towards mobile marketing affects purchase behaviour can be undertaken.

d Additional research can be carried out on the influence of mobile marketing on other areas of the marketing such as relationship marketing and international marketing.

e Future research on mobile marketing content could be done to determine effective ways to communicate to a wider audience.

f Since mobile marketing is invasive future research can be done to assist firms to develop strategies to circumvent privacy issues.

g Mobile marketing research could also done to determine effective strategies to communicate to educational institutions where participants may be minors.

h Consumers consent should first be pursued by entities through permission-based marketing before marketers can broadcast mobile messages to users on mobile marketing platforms.

i To drive consumer acceptance of marketing messages, the risk associated with credibility of mobile advertisement must be minimised. This can be done through permission-based marketing and ensuring customers that the content of the messages are trustworthy and credible through a short clause in the message.

References

Amir, B., Pejman, J. and Farhad, G. (2013) 'Consumer rights in Iran's telecom: investigation effective drivers on permission base mobile marketing', *European Online Journal of Natural and Social Sciences*, Vol. 2, No. 3, pp.1800–1811.

Arnold, J. and Becker, M. (2010) *Mobile Marketing for Dummies*, John Wiley & Sons Publishing, New Jersey.

Barnes, S. and Scornavacca Jr., E. (2008) 'Mobile marketing: the role of permission and acceptance', *Proceedings of the Second International Conference on Mobile Business*, Vienna, Austria.

Basheer, A.A.A. and Ibrahim, A.A. (2010) 'Mobile marketing: examining the impact of trust, privacy concern and consumers' attitudes on intention to purchase', *International Journal of Business and Management*, Vol. 5, No. 3, p.28.

Brown, T.A. (2014) *Confirmatory Factor Analysis for Applied Research*, Guilford Publications, New York.

Büscher, M., Urry, J. and Witchger, K. (2010) *Mobile Methods*, Routledge, London.

Carroll, A., Barnes, S.J., Scornavacca, E. and Fletcher, K. (2007) 'Consumer perceptions and attitudes towards SMS advertising: recent evidence from New Zealand', *International Journal of Advertising*, Vol. 26, No. 1, pp.79–98.

Chittenden, L. and Rettie, R. (2003) 'An evaluation of e-mail marketing & factors affecting response', *Journal of Targeting, Measurement & Analysis for Marketing*, Vol. 11, No. 3, pp.203–217.

Christensen, L.B., Johnson, B., Turner, L.A. and Christensen, L.B. (2014) *Research Methods, Design, & Analysis*, Pearson Education, Nottingham.

Culnan, M.J. and Williams, C.C. (2009) 'How ethics can enhance organizational privacy: lessons from the choicepoint & TJX data breaches', *MIS Quarterly*, Vol. 8, No. 2, pp.673–687.

Damopoulos, D., Menesidou, S.A., Kambourakis, G., Papadaki, M., Clarke, N. and Gritzalis, S. (2012) 'Evaluation of anomaly - based IDS for mobile devices using machine learning classifiers', *Security & Communication Networks*, Vol. 5, No. 1, pp.3–14.

Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B.G., Cox, L.P., Jung, J., McDaniel, P. and Sheth, A.N. (2014) 'Taint Droid: an information-flow tracking system for realtime privacy monitoring on smartphones', *ACM Transactions on Computer Systems (TOCS)*, Vol. 32, No. 2, p.5.

Felt, A., Chin, E, Hanna, D.S. and Wagner, D. (2011a) *Android Permissions Demystified*, Technical Report No. UCB/EECS-2011-48, University of California, Berkeley.

Felt, A.P., Finifter, M., Chin, E., Hanna, S. and Wagner, D. (2011b) 'A survey of mobile malware in the wild', in *Proceedings of the 1st ACM Workshop on Security & Privacy in Smartphones & Mobile Devices*, ACM, October, pp.3–14.

Felt, A., Greenwood, K. and Wagner, D. (2012) 'The effectiveness of application permissions', in *WebApps'11*, Berkeley, CA, USA.

Freedman, D., Pisani, R. and Purves, R. (2007) *Statistics (International Student Edition)*, 4th ed., 720pp., WW Norton & Company, NY, USA.

Goasduff, L. and Pettey, C. (2012) 'Gartner says worldwide smartphone sales soared in fourth quarter of 2011 with 47 percent growth', 12 April [online] https://www.gartner.com/newsroom/id/1764714 (accessed 26 November 2017).

Herbst, F. and Coldwell, D. (2004) *Business Research*, Juta & Company Ltd., Cape Town.

Jayawardhena, C., Kuckertz, A., Karjaluoto, H. and Kautonen, T. (2009) 'Antecedents to permission based mobile marketing: an initial examination', *European Journal of Marketing*, Vol. 43, Nos. 3/4, pp.473–499.

Kautonen, T., Karjaluoto, H., Jayawardhena, C. and Kuckertz, A. (2007) 'Permission-based mobile marketing and sources of trust in selected European markets', *Journal of Systems and Information Technology*, Vol. 9, No. 2, pp.104–123.

Krishnamurthy, S. (2006) 'Introducing E-MARKPLAN: a practical methodology to plan e-marketing activities', *Business Horizons*, Vol. 49, No. 1, pp.51–60.

Krum, C. (2010) *Mobile Marketing: Finding your Customers no Matter where they are*, Pearson Education, Harlow, India.

Kumar, V., Zhang, X. and Luo, A. (2014) 'Modeling customer opt-in & opt-out in a permission-based marketing context', *Journal of Marketing Research*, Vol. 51, No. 4, pp.403–419.

La Polla, M., Martinelli, F. and Sgandurra, D. (2013) 'A survey on security for mobile devices', *IEEE Communications Surveys & Tutorials*, Vol. 15, No. 1, pp.446–471.

Leino, K.R.M. (2010) 'Dafny: an automatic program verifier for functional correctness', in *International Conference on Logic for Programming Artificial Intelligence and Reasoning*, Springer, Berlin, Heidelberg, April, pp.348–370.

Leontiadis, I., Efstratiou, C., Picone, M. and Mascolo, C. (2012) 'Don't kill my ads!: balancing privacy in an ad-supported mobile application market', in *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications*, ACM, February, p.2.

Leung, S.O. (2011) 'A comparison of psychometric properties & normality in 4-, 5-, 6-, & 11point Likert scales', *Journal of Social Service Research*, Vol. 37, No. 4, pp.412–421.

Marinova, A., Murphy, J. and Massey, B.L. (2002) 'Permission e-mail marketing: as a means of targeted promotion', *The Cornell Hotel & Restaurant Administration Quarterly*, Vol. 43, No. 1, p.6169.

Mobile Marketing Association (MMA) (2008) *Mobile Marketing Guide: Recognizing Leadership & Innovation*, Mobile Marketing Association [online] http://www.mmaglobal.com/mobileapplications.pdf (accessed 20 April 2013).

Norris, S. (2003) 'Make the mobile connection', *Revolution Magazine*, 11 June [online] http://www.revolutionmagazine.com/news/index.cfmfuseactionViewNewsArticle&ID182912 (accessed 16 November 2012).

Persaud, A. and Azhar, I. (2012) 'Innovative mobile marketing via smartphones: are consumers ready?', *Marketing Intelligence & Planning*, Vol. 30, No. 4, pp.418–443.

Saunders, M., Lewis, C. and Thornhill, A. (2012) *Research Methods for Business Students*, 5th ed., Pearson Education, Harlow, India.

Scott, M.D. (2007) *The New Rules of Marketing & PR*, John Wiley & Sons Inc., USA.

Shabtai, A., Kanonov, U. and Elovici, Y. (2010) 'Intrusion detection for mobile devices using the knowledge-based temporal abstraction method', *J. System. Software*, Vol. 83, No. 8, pp.1524–1537.

Smalley, S. (2012) *Middleware MAC for & Android*, August [online] http://kernsec.org/files/LSS2012-MiddlewareMAC.pdf (accessed 25 November 2018).

Tanakinjal, G.H., Deans, K.R. and Gray, B.J. (2010) 'Third screen communication and the adoption of mobile marketing: a Malaysia perspective', *International Journal of Marketing Studies*, Vol. 2, No. 1, p.36.

Tezinde, T., Smith, B. and Murphy, J. (2002) 'Getting permission: exploring factors affecting permission marketing', *Journal of Interactive Marketing*, Vol. 16, No. 4, pp.28–36.

Wang, D., Cheng, H., He, D. and Wang, P. (2016) 'On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices', *IEEE Systems Journal*, Vol. 18, No. 99, pp.1–10.

Watson, C., McCarthy, J. and Rowley, J. (2013) 'Consumer attitudes towards mobile marketing in the smart phone era', *International Journal of Information Management*, Vol. 33, No. 5, pp.840–849.

Welter, F. and Kautonen, T. (2005) 'Trust, social networks & enterprise development: exploring evidence from east & West Germany', *International Entrepreneurship & Management Journal*, Vol. 1, No. 3, pp.367–379.

Zikmund, W.G., Babin, B.J., Carr, J.C. and Griffin, M. (2013) *Business Research Methods*, Cengage Learning, London.