Journal of Contemporary Management
Volume 14

The role of demographics and Facebook activities in users' concerns about online privacy

Y JORDAAN *
Department of Marketing Management, University of Pretoria
*yolanda.jordaan@up.ac.za * corresponding author*

TN NDHLOVU
Department of Marketing Management, University of Pretoria
thinkwell.ndhlovu@up.ac.za

Abstract

Online social networking sites, such as Facebook, have become an integral part of society –mainly due to a need for social engagement. Unfortunately, cyber-related crimes have increased owing to individuals displaying their personal information so freely online. The reported inconsistencies in terms of the associations of different users and user activities in terms of their levels of online privacy served as an impetus for this study.

Against the backdrop of the uses and gratifications theory and the reported inconsistencies from previous studies, the purpose of this study is to investigate how certain socio-demographic variables and activities of Facebook users are associated with concerns about information privacy on Facebook. Data was collected through 210 self-administered questionnaires.

Results suggest that females are less likely than males to provide accurate personal information on Facebook. Furthermore, there was a positive correlation between internet experience and a Facebook user's privacy concerns. The value of this study lies in understanding the balance between privacy concern and sharing personal information, as well as to assist Facebook practitioners in terms of dealing with the issue of privacy for different Facebook users. Privacy concerns also have an impact on a user's likelihood of implementing advanced privacy settings, and the results from this study may be able to assist Facebook practitioners to minimise the negative consequences of future Facebook interactions.

Key phrases

Facebook, internet experience, online privacy, personal information, privacy concerns

1. INTRODUCTION

People all over the world are communicating on social networking sites on a daily basis and, as a result, social networks have become a significant part of consumers' daily lives. Facebook, Twitter and Instagram have become sites where users express themselves, communicate with their families and friends and also build new relationships while sustaining existing ones (Mohamed 2010:75). In South Africa, Facebook is still the most popular networking site with 14 000 000 users of which 85% of these users use mobile devices (Goldstuck & Du Plessis 2017: Internet). The statistics on social network penetration in South Africa show that 27% of the population is active in social network sites (Statista 2016:Internet), with the average daily usage of social media channels around 2.7 hours per day (Statista 2015:Internet).

Establishing and engaging in social networks require social network users to reveal a great deal of personal information online. Revealing personally identifiable information puts users at risk of a breach in their privacy (Acquisti & Gross 2006:2). It is said that the full utilisation of Facebook by users is hampered by privacy concerns and subsequent privacy protection behaviour.

Protective behaviour includes giving inaccurate information and changing privacy settings (Hunt 2009:46), making it difficult for Facebook practitioners to harness the full potential that this social network site offers. One associated risk when sharing personal information is the possible unauthorised use of information by third parties, causing the user to fall victim to cyber-crime (Debatin, Lovejoy, Horn & Hughes 2009:86). This creates a dilemma for social network users since they have to balance sharing personal information with protecting their privacy.

The uses and gratifications theory is often cited to explain how social network users balance sharing personal information and protecting their privacy. The theory suggests that individuals fulfil their needs for entertainment, relationships and identity construction through the use of social network systems, and that these needs override their privacy concerns (Debatin *et al.* 2009:89; Malik, Dhir & Nieminen 2016:130). Simply put, the assumption is made that for users of social networks such as Facebook, the need for social engagement is more important than protecting their own privacy.

Several international studies have considered gender and/or ethnicity in terms of information privacy concerns and behaviour in an online environment. More specifically, there is evidence that user socio-demographics and prior internet experience are differentiators when it comes to

privacy concerns of social network users, which ultimately leads to privacy protection behaviour (Bellman, Johnson, Kobrin & Lohse 2004:313; Cho, Rivera-Sánchez & Lim 2009:397; Fogel & Nehmad 2009:159; Hoy & Milne 2010:33; O'Neil 2001:19).

However, very few studies report on the role of these demographics amongst South African Facebook users. This warrants further investigation, especially in terms of the perceptions of different ethnic groups, because South Africa is known for its ethnic diversity. In this regard, ethnic diversity may extend to Facebook usage and identify valuable pockets of potential for social network managers. Even Facebook has indicated that one of their goals is to understand how different ethnic groups use this platform (Marlow 2009:Internet).

In addition, previous studies (Bellman *et al.* 2004:321; Choi & Land 2016:871; Park & Jang 2016:625; Mohamed 2010:86) reported mixed results in terms of the relationship between information privacy concerns and Internet experience or accurate disclosure of personal information on Facebook. On the one hand, some studies report that users' level of online privacy concern decreases as the level of their Internet experience increases (Bellman *et al.* 2004:321; Mohamed 2010:86).

Other studies again, report a positive correlation between users' level of online privacy concern and their Internet experience levels. This positive relationship occurs when these experienced users become more aware of how their personal information is used, and thus become more concerned (Beldad, De Jong & Steehouder 2011:2239; Singh & Hill 2003:644). These same inconsistencies are reported in terms of users' levels of online privacy concerns and their likelihood to provide accurate personal information (Tufekci 2008:20; Young & Quan-Haase 2009:265). Consequently, further studies on these afore-mentioned relationships are required to uncover the balance between privacy concern, personal information sharing and the usage of the Facebook platform by South Africans.

Also contributing to this study, is Facebook's recent change in privacy settings (Kovach 2014:Internet). This sparked the need for research to determine which privacy settings South African Facebook users choose and its relation to their privacy concerns.

The purpose of the study is therefore to examine how Facebook users differ based upon socio-demographic variables (gender and ethnicity) and prior internet experience with respect to privacy concerns in a South African context. A self-administered survey was conducted

amongst Facebook users and the results revealed significant differences in privacy concerns based upon some of the variables.

This study contributes to the uses and gratifications theory by understanding the balance between sharing personal information and the value users receive from Facebook. Furthermore, the results can enable practitioners to segment their Facebookstrategies according to the needs of different demographic groups, as well as be proactive in their management of privacy issues on Facebook.

The rest of this article commences with a review of the literature relating to online social networks, online privacy and privacy concerns. Next, the methodology adopted for the study is described, after which the findings are presented and discussed. Lastly, the article presents the managerial implications, limitations and recommendations for future research.

2. LITERATURE REVIEW

2.1 Online social networks and Facebook

Researchers agree that a social network site is essentially a way for users to construct their social lives online (Boyd & Ellison 2008:211; Lareau 2007:3). Social networking sites such as Facebook and others have become cybernetic gathering places for people of various ages and walks of life, to connect with others, "hang out," and feel part of a community (Boyd & Ellison 2008:210; Ellison, Vitak, Gray & Lampe 2014:855; Hoy & Milne 2010:28).

In these cybernetic gathering places, users can interact with online friends, view photographs and videos, and chat in a virtual world that is a reconstruction of real-life interactions with people they know. The individual's name, contact information, demographic data and a picture is provided to distinguish individual users (Hoy & Milne 2010:2; Kaplan & Haenlein 2009:63).

Facebook is a social network system that facilitates communication in a virtual world, between people who know each other, or those who are meeting for the first time. Worldwide, Facebook has the highest number of members with 2 000 000 000 (Aslam 2017:Internet), followed by Whatsapp and YouTube with over 1 000 000 000 users (Statista 2017:Internet). Facebook is also the most popular social networking site in South Africa with 14 000 000 users (Worldwide Worx & Fuseware 2017:Internet). The dominant use of the Facebook social networking system

in South Africa provides an opportunity to examine users' privacy concerns relative to patterns of information disclosure (Acquisti & Gross 2006:3).

2.2 Privacy in an online context

Hunt (2009:12) believes that privacy in an online context consists of control and access. In this context, control is the extent to which information about a user is communicated, how and to whom it is communicated, as well as how much is revealed. Users' control over their own personal information helps to manage their level of intimacy and define their relationships with others (Hunt 2009:12). Access refers to the magnitude, to which a user's information is available to others, the extent to which others know about the user and the degree of attention others give the user. Limited or no accessibility to others provide users with perfect privacy (Hunt 2009:12).

In general, concern is considered to be a multifaceted belief, surrounding personal independence, democratic participation, identity management and social coordination (Mohamed 2010:76). For this study, concern about online privacy is defined as any individual online social network user who has the desire to keep information out of the hands of undesirable others (Hunt 2009:16).

Therefore, individuals who are concerned about online privacy, express a discernible interest in safeguarding their personal information online, and may view the issues dealing with online privacy with uncomfortable apprehension. Issues of concern can typically include who has access to an individual's personal information, identity theft, and surveillance of users' online behaviour, unauthorised third party use, and even unwanted contact, such as stalking (Debatin *et al.* 2009:84). The extent of an individual's privacy concern can be attributed to the sensitivity of the information to be shared (Kim 2016:399).

According to Acquisti and Gross (2006:1), privacy concerns as a single characteristic is not enough to predict an individual's membership to Facebook, nor his/her concern for personal information. However, factors such as gender, ethnic background and internet experience could be seen as the driving forces behind users' varying degrees of privacy concerns on Facebook. These aspects are associated with concerns about online information privacy and have an effect on the way in which a user may interpret privacy or take precautions to protect it.

The theoretical approach of this study is based on the uses and gratifications theory. The theory suggests that individuals fulfil their needs for entertainment, relationships and identity construction through the use of social network systems, and that these needs override their privacy concerns (Debatin *et al.* 2009:89). Prior research revealed that uses and gratifications on Facebook differed according to user demographics (Park, Kee & Valenzuela 2009:729), and the various needs of users (Ozanne, Navas, Mattila & Van Hoof 2017:9; Raacke & Bond-Raacke 2008:172).

2.2.1 The role of demographics in privacy concerns and information disclosure on Facebook

Marketers often tailor their offerings to meet the needs of specific demographic groups, including gender and ethnicity. With regard to gender, several previous research studies report that females are more concerned about their online privacy than males (Cho *et al.* 2009:397; Hoy & Milne 2010:28; Mohamed 2010:74; Rowan & Dehlinger 2016:340). Interestingly, females also tend to be more concerned than males in taking action, such as making use of Facebook's privacy settings, which protect their privacy (Hoy & Milne 2010:28; Mohamed 2010:74).

Therefore, gender differences may determine whether South African female Facebook users have higher concerns for information privacy than their male counterparts. It is therefore hypothesised that:

H1: Females are more concerned about information privacy on Facebook than males.

A study by Raacke and Bond-Raacke (2008:172), found that uses and gratifications on social networks sites varied between males and females, with females prone to divulging more personal information. In line with the findings by Fogel and Nehmad (2009:159) and females' purported increased concern for privacy, it is hypothesised that:

H2: Females are less likely to provide accurate personal information on Facebook in comparison with males.

Segmenting markets according to ethnicity is another approach that marketers can follow in an attempt to meet the specific needs and wants of users. One prior research study found no ethnic differences in uses and gratifications amongst Facebook users (Raacke & Bond-Raacke 2008:169). However, there is evidence from several other previous research studies (Hofstra,

Corten and Van Tubergen 2016:619; Litt & Hargittai 2014:10; Singer *et al.* in O'Neil 2001:19) that the effects of confidentiality and privacy concerns vary between individuals of different ethnic groups. In one study, Black respondents expressed higher levels of concern about privacy than White respondents (Singer *et al.* in O'Neil 2001:19). In another study the level of concern varied by ethnic origin, where Whites and Blacks were very concerned with privacy, as opposed to Asians who were the least likely to show concern (O'Neil 2001:20). Based on this discussion, it is hypothesised that:

H3: Ethnic groups differ in terms of their concerns about information privacy on Facebook.

2.2.2 Internet experience and Facebook privacy concerns

The high level of uses and gratification means that Facebook has become part of users' lives and users are engaged in friendly yet unpredictable activities (Debatin *et al.* 2009:101). It can be deduced from the uses and gratifications theory that, high levels of use and gratification override users' privacy concerns (Debatin *et al.* 2009:89). Several studies have been conducted to examine the correlation between individuals' experiences with the internet and their information privacy concerns (Bellman *et al.* 2004:313; Cho *et al.* 2009:397; Dinev & Hart 2005:7; Liao, Liu & Chen 2011:702; Singh & Hill 2003:634).

Internet experience can be described as the length and frequency of internet use (Cho *et al.* 2009:397). The length of use refers to the time span (in months or years) that an individual has been active on Facebook. Frequency refers to the rate at which an individual logs in to Facebook over a certain period of time. Many previous research studies report that an internet user's concerns about online privacy diminishes with internet experience, suggesting that online privacy concern should fall gradually as a user's online internet experience rises (Bartsch & Tobias 2016:147; Bellman *et al.* 2004:321; Livingstone 2008:408).

However, other research findings report that as a result of increased expertise, internet users who are more skilled and knowledgeable with the internet, are more concerned about online privacy (Cho *et al.* 2009:397; Sing & Hill 2003:648). Furthermore, this expertise makes individuals more vigilant about internet usage, given that they are more aware of how their information could be collected and used without their consent (Cho *et al.* 2009:397). Based on the afore-mentioned studies, the following hypothesis is proposed:

H4: There is a correlation between users' experience with the internet and their concerns about information privacy on Facebook.

2.2.3 The role of privacy settings in concerns about privacy on Facebook

As previously discussed, the gratifications of Facebook as a social tool seem to override many privacy concerns (Debatin *et al.* 2009:101-102). This inconsistency between being concerned about information privacy, but lacking to behave in a protective manner is often referred to as the privacy paradox (Kokolakis 2017:123).

In a Facebook context, this may mean that users are satisfied with Facebook's default privacy settings, which are those settings that are automatically in place when a user creates a Facebook account. If the user does not alter these initial privacy settings in any way, they remain default settings.

Advanced privacy settings refer to any adjustments made to the default privacy settings on Facebook (Hunt 2009:7). Changing the default settings allow users to regulate the access that their friends and the public have to their personal information, helping to protect against unwanted access by others. Advanced privacy settings essentially allow users to dictate and manage their personal privacy boundaries, as well as their levels of intimacy with others (Hunt 2009:16).

Facebook users are increasingly utilising private settings and this could be due to various factors that include: accessibility to advanced privacy settings; users' growing expertise with settings and controls; and an increase in awareness of privacy risks on social network sites (Stutzman, Gross & Acquisti 2012:22). It is therefore hypothesised that:

H5: There is a significant difference between the privacy concerns of those Facebook users who implement advanced privacy settings and those who use default privacy settings.

2.2.4 Accurate personal information and concerns about privacy on Facebook

A Facebook user's personal information can include an email address, home address, contact number, date of birth, relationship status, hobbies or interests (Mohamed 2010:77). Disclosing personal information on a social network system places a user at greater risk of cyber and physical stalking, surveillance and even identity theft (Young & Quan-Haase 2009:265). High

gratifications and usage patterns on Facebook have resulted in users developing a lax attitude towards privacy concerns (Debatin *et al.* 2009:83); therefore users disclose a great deal of accurate personal information.

Previous research uncovered that users disclose accurate personal information without regard or concern for online privacy (Tufekci 2008:20). However, one study reports that users with low levels of concern about information privacy (thus not concerned that their information may potentially be used for harmful purposes), tend to be forthcoming and more likely to provide accurate personal information on Facebook (Young & Quan-Haase 2009:266).

In addition, those users who believe that privacy is only a concern once it has been breached or lost, also tend to perceive the benefits of using social networks as greater than the potential privacy risks (Young & Quan-Haase 2009:266). The opposing view is that concerns about information privacy on Facebook have an effect on the information revelation behaviours of users (Pew in Young & Quan-Haase 2009:266).

A Pew internet survey reports that of the 45% of individuals who have not provided accurate personal information to access a social network, 61% of them consider themselves to be "hard-core privacy defenders" (Pew in Young & Quan-Haase 2009:266). Based on the aforementioned discussion, it is hypothesised that:

H6: There is a correlation between concerns about information privacy on Facebook and a user's likelihood of providing accurate personal information.

3. RESEARCH METHODOLOGY

3.1 Sampling and data collection

The target population for the study consisted of students at the Hatfield campus of the University of Pretoria in South Africa. An accurate and suitable sampling frame was not available from which to draw a probability sample and therefore a non-probability (convenience) sampling method was applied to the study. The sampling attempted to include an equal spread of gender and ethnic groups. Also, only students with an active Facebook account were included. The equal gender spread was an attempt to mirror the South African Facebook

population, where 50% of Facebook users are male and 50% are female (Worldwide Worx & Fuseware 2015:Internet).

Data for the study was collected by means of campus intercepts, using a self-completion questionnaire. The questionnaire was pre-tested using a convenience sample of 12 selected undergraduate and postgraduate students at the same university. The final realised sample included a total of 210 usable questionnaires, consisting of an equal number of female and male respondents (105 each). Three of the four main population groups, as categorised by Statistics South Africa, were equally represented, namely Black (70), White (70) and Indian/Asian (70). The Coloured ethnic grouping was not included because of the limited number of Coloured students enrolled at the specific university.

3.2 Measures

Concern about information privacy was measured by 10 items using a 7-point Likert-type response format (ranging from 1 = Strongly disagree to 7 = Strongly agree) adapted from Malhotra, Kim and Agarwal (2004:351). For this scale, high scores indicate a greater level of concern about online privacy.

Internet experience of a Facebook user was also measured by 3 items using a 7-point Likert-type response format taken from Dinev and Hart (2005:14); where higher scores indicate greater internet experience of the user (Dinev & Hart 2005:14). The Cronbach's alpha value reported by Dinev and Hart (2005:16) was 0.87.

In order to establish what current privacy settings a respondent has implemented on Facebook, a dichotomous question from Hunt (2009:28) was used. The question contained two options: (1) I am using default (original) privacy settings and have not adjusted the privacy settings on my Facebook account, or (2) I am using customised (stricter) privacy settings because I have adjusted the privacy settings on my Facebook account.

The likelihood of providing accurate personal information was measured using a 3-point rating scale (Acquisti & Gross 2006:14; Mohamed 2010:82). Respondents were given a list of nine information categories (birthday, cell phone number, home phone number, partner's name, personal address, political views, religion, university name and sexual orientation), each containing the options: (1) I do not provide this information, (2) I provide this information, but it is

intentionally not complete or accurate, and (3) I provide this information and it is complete and accurate.

4. RESULTS AND DISCUSSION

4.1 Descriptive statistics

The results indicate that 60% of respondents have customised their privacy settings, with 40% of respondents still using the default (original) privacy settings. On average, the overall internet experience of respondents was relatively high (M = 5.72, SD = 1.05). With regard to respondents' privacy concerns, the results indicated that it was very important for respondents to be aware of and knowledgeable about how their personal information was used online (highest mean score: M = 6.53, SD = 1.10). Respondents were less concerned about giving their personal information to many online companies (lowest mean score: M = 5.38, SD = 1.53).

A total of 80% of respondents were more likely to provide their complete and accurate birthday compared to only 6% who are willing to provide their complete and accurate home phone number. The majority of respondents (89%) are willing to provide their complete and accurate university name, whereas only 10.5% provide their complete and accurate home address.

4.2 Validity and reliability

The two constructs used in the hypothesis analyses were subjected to reliability and validity testing. Table 1 indicates the factor loadings of each construct, together with the Cronbach's alpha, average variance extracted and composite reliability of each construct.

Table 1 indicates acceptable internal consistency in that the Cronbach's alpha values were 0.89 and 0.71 for the respective constructs (Bagozzi & Yi 1988:79). Discriminant validity was evident in that each construct exhibited a clear single factor structure (Cole, Cho and Martin 2001: 94). From Table 1 it is evident that the constructs showed convergent validity in that all the results were above the suggested cut-off norms: factor loadings within each construct were above 0.50 (Hildebrandt 1987:35), the average variance extracted was above 0.5 (Fornell & Larcker 1981) and the composite reliability was above 0.7 (Hair, Anderson, Tatham & Black 1998:302).

TABLE 1: Reliability and validity assessment

Items	Information privacy concern (IPC)	User internet experience (UIE)
(IPC3) I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.	0.599	
(IPC4) Companies seeking information online should disclose the way the data are collected, processed, and used.	0.591	
(IPC5) A good consumer online privacy policy should have a clear and visible disclosure.	0.656	
(IPC6) It is very important to me that I am aware and knowledgeable about how my personal information will be used.	0.699	
(IPC7) It bothers me when online companies ask me for personal information.	0.731	
(IPC8) When online companies ask me for personal information, I think twice before providing it.	0.866	
(IPC9) It bothers me to give personal information to so many online companies.	0.821	
(IPC10) I am concerned that online companies are collecting too much personal information about me.	0.700	
(UIE2) Managing virus attacks		0.501
(UIE3) Communicate through instant messaging		0.849
(UIE4) Downloading files from internet		0.817
Cronbach's alpha	0.89	0.71
Average variance extracted (AVE)	0.51	0.53
Composite reliability (CR)	0.89	0.76

For information privacy concern, two items were deleted to improve the average variance extracted and, for users' internet experience, one item was deleted. Following the reliability and validity testing of information privacy concern and users' internet experience, the research objectives could be addressed by means of hypothesis testing.

4.3 Hypothesis tests

4.2.1 Hypothesis 1

Hypothesis 1 focused on the difference between genders in terms of their concern about information privacy on Facebook. The non-parametric Mann-Whitney U test was used to test Hypothesis 1 owing to the violation of normality. The Mann-Whitney U test revealed no significant differences in the privacy concern levels of males (*Md* = 6.1, n = 105) and females (*Md* = 6.1, n = 105), U = 5272, z = -0.547, p = 0.146 one-tailed, r = 0.04. There was thus no support for Hypothesis 1, which differs from most previous research that reported females being more concerned about their online privacy than males (Cho *et al.* 2009:397; Hoy & Milne 2010:28; Mohamed 2010:74).

4.2.2 Hypothesis 2

Hypothesis 2 dealt with the difference between genders in terms of their likelihood of providing accurate personal information on Facebook. Again, the non-parametric Mann-Whitney U test was used to test the hypothesis due to the violation of normality. The results of the Mann-Whitney U test revealed significant differences in the likelihood of males (*Md* = 117, n = 105) and females (*Md* = 93, n = 105) to provide accurate information (U = 4294, z = -2.822, p = 0.0025 one-tailed). Despite the small effect size (r = 0.2), the results show support for Hypothesis 2. This finding is consistent with previous research investigating the two genders and reporting that females have a lower likelihood of providing accurate personal information (Fogel & Nehmad 2009:159).

4.2.3 Hypothesis 3

Hypothesis 3 dealt with the difference between ethnic groups in terms of their concerns about information privacy on Facebook. With respect to the assumptions underlying the use of a one-

way between-group analysis of variance (ANOVA), the normality violation resulted in a decision to use the Kruskal-Wallis test as the non-parametric alternative.

The results of the Kruskal-Wallis test revealed a statistically significant difference in respondents' concerns about information privacy on Facebook across the three different ethnic groups: χ^2 (2, 210) = 8.68, p = 0.013. The White group recorded the highest median score (*Md* = 122.49), followed by the Black group (*Md* = 100.47) and then the Indian/Asian group (*Md* = 93.54).

Follow-up Mann-Whitney U tests were performed between the pairs of groups to determine where the significance occurred. A Bonferroni adjustment to the alpha values was applied to control for Type I errors. Since three tests were used to compare the different groups, the Bonferroni adjustment of the p-value led to a cut-off point (p-value) of 0.0167 instead of 0.05 (Pallant 2013:243).

The Mann-Whitney U test revealed only one significant difference in the privacy concern levels of the Indian/Asian group (*Md* = 6, n = 70) and the White group (*Md* = 6.2, n = 70), U = 1784, z = -2.778, p = 0.005, r = 0.23.

There was thus support for Hypothesis 3. This finding is the opposite of the results reported in a study where Black respondents expressed higher levels of concern about privacy than White respondents (Singer *et al.* in O'Neil 2001:19). It does, however, coincide with results from a study where Whites were more concerned with privacy issues as opposed to Asians (O'Neil 2001:20).

4.2.4 Hypothesis 4

Hypothesis 4 dealt with the relationship between Facebook users' experience with the internet and their concern for information privacy on Facebook. Preliminary analyses were performed to ensure no violation of the assumptions underlying the Pearson product-moment correlation test. Owing to the violation of normality, the relationship between respondents' internet experience and their information privacy concerns was investigated using Spearman's rank order correlation coefficient.

The results indicated a small, positive correlation between the two variables, *rho* = 0.282, n = 210, p < 0.00, with internet experience being positively associated with information privacy

concerns. The results provided support for Hypothesis 4, which is in line with a previous study conducted by Cho *et al.* (2009:397).

4.2.5 Hypothesis 5

Hypothesis 5 focused on the difference between respondents who use the default privacy settings versus those who use advanced privacy settings in terms of their concern about information privacy on Facebook.

Again, the non-parametric Mann-Whitney U test was used to test Hypothesis 5 due to the violation of normality. The Mann-Whitney U test revealed a significant difference in the privacy concern levels of the group using the default privacy settings (*Md* = 6, n = 82) versus the group using the advanced privacy settings (*Md* = 6.2, n = 124), U = 4043, z = -2.488, p = 0.013, r = 0.17.

Despite the small effect size (r = 0.17), there was support for $H_{5,}$ which is in support of a finding by Hunt (2009:17) and more recently by Kim (2016:400) in a mobile phone involvement context.

4.2.6 Hypothesis 6

The relationship between Facebook respondents' privacy concerns and their subsequent likelihood of providing accurate personal information was measured in Hypothesis 6. The non-parametric Spearman's rank order correlation was used to test the hypothesis due to a violation in normality.

The results were insignificant, with a small, negative correlation between the two variables, rho = -0.126, n = 210, p = 0.068. The negative correlation was as expected, in that respondents would be less willing to provide accurate information if their privacy concerns increased.

However, the results do not show support for Hypothesis 6. This is not in line with findings from a study by Tufekci (2008:20), which also indicated no relationship between online privacy concerns and information disclosure on Facebook.

Table 2 summarises the main statistical results and hypotheses outcomes.

TABLE 2: Summary of hypotheses results

Hypothesis	Hypothesis result	Support for hypothesis
H1: Females are more concerned about information privacy on Facebook than males	Mann-Whitney U test: U=5272, z=-0.547, p=0.146 one-tailed, r=0.04; males/females *Md*=6.1, n=105	Not supported
H2: Females are less likely to provide accurate personal information on Facebook in comparison with males	Mann-Whitney U test: U=4294, z=-2.822, p=0.0025 one-tailed, r=0.2; males/females *Md*=117/93, n=105)	Supported
H3: Ethnic groups differ in terms of their concerns about information privacy on Facebook	Kruskal-Wallis test: $\chi^2(2, 210)=8.68$, p=0.013; Indian/Asian group (*Md*=6, n=70), White group (*Md*=6.2, n=70), U=1784, z=-2.778, p=0.005, r=0.23	Supported
H4: There is a correlation between users' experience with the internet and their concerns about information privacy on Facebook	Spearman's rank order correlation coefficient: *rho*=0.282, n=210, p<0.00	Supported
H5: There is a significant difference between the privacy concerns of those Facebook users who implement advanced privacy settings and those who use default privacy settings	Mann-Whitney U test: U=4043, z=-2.488, p=0.013, r=0.17; default group(*Md*=6, n=82), advanced setting group *Md*=6.2, n=124	Supported
H6: There is a correlation between concerns about information privacy on Facebook and a user's likelihood of providing accurate personal information	Spearman's rank order correlation coefficient: *rho*=-0.126, n=210, p=0.068	Not supported

5. THEORETICAL AND MANAGERIAL IMPLICATIONS

From a theoretical point of view, if one considers the uses and gratifications theory, this finding suggests that female users are active on Facebook because of the gratification it provides. However, in order to get this benefit, they have to provide personal information, and so they provide inaccurate personal information. In other words, the "gratification" does not override their concerns, but rather that they adapt the "use" to enable them to get the gratification. The challenge to researchers and practitioners are thus to determine the drivers behind the behaviour of providing inaccurate personal information, and what this behaviour tries to protect or communicate.

The finding in this study that females are less likely than males to provide accurate personal information on Facebook poses an interesting managerial challenge for online communication practitioners. One consequence of this behaviour may be that online communication activities directed towards females may prove to be less successful owing to the fact that females do not provide accurate personal information (Fogel & Nehmad 2009:159). This is because incorrect information can mislead companies that execute communication strategies on Facebook, since targeted advertisements are based on the user's profile information provided. As a result, misdirected advertisements may prove to be an inefficient use of communicative resources.

What is interesting from a managerial point of view, is the finding that females are not necessarily more concerned about information privacy on Facebook than their male counterparts. This raises the question as to why females feel the need to provide inaccurate personal information on Facebook. This is an important question, especially since there is evidence that Facebook users' level of privacy concerns is negatively associated with their willingness to provide accurate personal information (Young & Quan-Haase 2009:265).

The varying degree by which ethnic groups exhibit privacy concerns as found in this study and by O'Neil (2001:19), may lead to Facebook communication practitioners having to rethink their advertising strategies based on pre-established ethnic profiles. For instance, the findings in this study indicated that White Facebook users are more concerned about their privacy on Facebook than Black users. This may signal to online communication practitioners that the aforementioned ethnic group of Facebook users may be less trusting of communication received from Facebook. Online communication practitioners will need to determine whether

advertisements on Facebook are seen as a breach of privacy, or whether it may be other actions that constitute a privacy breach.

What is of concern is that as Facebook users gain more experience with the internet their information privacy concerns increase – albeit slightly. This suggests that more activity in an online environment leads to more problems, and therefore higher privacy concerns. This provides food for thought for online communication practitioners and poses a challenge on how to create a more trusting online environment.

On the positive side, there is evidence that online shopping as a whole is growing in South Africa (Goldstuck 2011). If this form of shopping does not protect shoppers' personal information, it may be the very reason why the result in this study (namely the positive relationship between privacy concern and internet experience) was found. However, the researchers are cognisant of the fact that whether internet experience through online shopping actually increases users' privacy concerns is yet to be determined.

The findings of this study also show that as information privacy concerns increase, so does privacy protective behaviour in terms of setting advanced privacy settings. This, at least, provides a mechanism for Facebook users to protect their personal information. Online communication practitioners may want to consider communicating this self-protection more clearly to enable Facebook users to take charge of their level of protection.

6. LIMITATIONS AND RECOMMENDATIONS FOR FUTURE RESEARCH

The most significant limitation of this study was the convenience sampling method used to select participants as well as the small sample size of 210 respondents. Furthermore, this study did not represent all of the major population groups in South Africa as it only focused on three of the four major population groups in the country. As mentioned before, the Coloured grouping was not included because of the limited number of Coloured students enrolled at the university from which the sample was drawn.

Future studies can include respondents from a wider geographic area, as well as respondents from a wider age group. Also, the context of this study was limited to Facebook and future

studies might consider including other social network platforms, such as LinkedIn, Instagram, Twitter and Snapchat.

Even though this study did not find a relationship between Facebook respondents' privacy concerns and information disclosure on Facebook, the negative correlation (namely that respondents would be less willing to provide accurate information if their privacy concerns increased) should be noted. Future studies can consider applying the privacy calculus approach to get a deeper sense of Facebook users' evaluation of risks and benefits on this platform (Trepte, Reinecke, Ellison, Quiring, Yao & Ziegele 2017:1). This may provide more meaningful insight into Facebook users' willingness to engage in disclosures on Facebook.

Future studies can consider using an online privacy concern scale that focuses more directly on the privacy issues within Facebook. The disconnect between respondents' privacy concerns and their provision of accurate personal information hints at a better understanding of the actual drivers behind the behaviour of providing inaccurate personal information on Facebook. Future research may thus want to consider whether this decision is because of personal factors, factors related to the online environment, or factors relating directly to Facebook as a platform.

7. CONCLUSION

This study investigated how certain socio-demographic variables (gender and ethnicity) and user activities of Facebook are associated with concerns about information privacy on Facebook. Considering the uses and gratifications theory, this finding suggests that female users are more active on Facebook because of the gratification it provides.

However, in order to get this benefit, they have to provide personal information and as such they provide inaccurate information. One of the reasons why female users provide inaccurate information on Facebook could be that cyber-related crimes have slowly increased in South Africa owing to the fact that individuals display their personal information so freely online (Dlamini & Modise 2012:101). Online communication practitioners should be proactive in their management of privacy issues on Facebook and provide protection for users.

The proposed study's results will add to the limited available knowledge on Facebook privacy amongst South African users. It also provides value to social network practitioners in terms of

dealing with the issue of privacy for different Facebook users, with the aim of minimising the negative consequences of future Facebook interactions.

Data collection support by Ms CT Baggeröhr and Mr DJ Lecluse is hereby acknowledged.

REFERENCES

ACQUISTI A & GROSS R. 2006. Imagined communities: awareness, information sharing, and privacy on the Facebook. *Journal of Computer Science* 4258:1-22.

ASLAM S. 2017. Facebook by the numbers: stats, demographics and fun facts. [Internet: https://www.omnicoreagency.com/facebook-statistics/; downloaded on 2017-07-21.]

BAGOZZI RP & YI Y. 1988. On the evaluation of structural equation models. *Journal of the Academy of Marketing Science* 16(1):74-84.

BARTSCH M & TOBIAS D. 2016. Control your Facebook: an analysis of online privacy literacy. *Computers in Human Behaviour* 56(2016):147-154.

BELDAD A, DE JONG M & STEEHOUDER M. 2011. I trust not therefore it must be risky: determinants of the perceived risks of disclosing personal data for e-government transactions. *Computers in Human Behavior* 27(6):2233–2242.

BELLMAN S, JOHNSON EJ, KOBRIN SJ & LOHSE GL. 2004. International differences in information privacy concerns: a global survey of consumers. *The Information Society* 20(5):313-324.

BOYD DM & ELLISON NB. 2008. Social network sites: definition, history and scholarship. *Journal of Computer-Mediated Communication* 13(2008):210-230.

CHO H, RIVERA-SÁNCHEZ M & LIM SS. 2009. A multinational study on online privacy: global concerns and local responses. *Journal of New Media and Society* 11(3):395–416.

CHOI BCF & LAND L. 2016. The effects of general privacy concerns and transactional privacy concerns on facebook apps usage. *Information and Management* 53(2016):868-877.

COLE DA, CHO S & MARTIN JM. 2001. Effects of validity and bias on gender differences in the appraisal of children's competence: results of MMTM analyses in a longitudinal investigation. *Structural Equation Modelling* 8(1):84-107.

DEBATIN B, LOVEJOY JP, HORN AK & HUGHES BN. 2009. Facebook and online privacy: attitudes, behaviours and unintended consequences. *Journal of Computer-Mediated Communication* 15:83-108.

DINEV T & HART P. 2005. Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce* 10(2):7-29.

DLAMINI Z & MODISE M. 2012. Cyber security awareness initiatives in South Africa: a synergy approach. Seattle, WA: Academic Conferences International. (7th International Conference on Information Warfare and Security; 22-23 March.)

ELLISON NB, VITAK J, GRAY R & LAMPE C. 2014. Cultivating social resources on social network sites: Facebook relationship maintenance behavior and their role in social capital processes. *Journal of Computer-Mediated Communication* 19(2014):855-870.

FORNELL C & LARCKER DF. 1981, Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research* 18(1):39-50.

FOGEL J & NEHMAD E. 2009. Internet social network communities: risk taking, trust, and privacy concerns. *Journal of Computers in Human Behaviour* 25(1):153-160.

GOLDSTUCK A. 2011. Online sales accelerate in SA. [Internet: http://www.worldwideworx. com/online-sales-accelerate-in-sa/; downloaded on 2016-11-17.]

GOLDSTUCK A & DU PLESSIS T. 2017. SA social media landscape 2017. [Internet: http://www.worldwideworx.com/wp-content/uploads/2016/09/Social-Media-2017-Executive-Summary.pdf/; downloaded on 2017-07-21.]

HAIR JF Jr, ANDERSON RE, TATHAM RL & BLACK WC. 1998. Multivariate data analysis. 5th ed. London: Prentice Hall International.

HILDEBRANDT BF. 1987. Introduction to numerical analysis. 2nd ed. New York, NY: Dover Publications.

HOFSTRA B, CORTEN R & VAN TUBERGEN F. 2016. Understanding the privacy behaviour of adolescents on Facebook: the role of peers, popularity and trust. *Computers in Human Behavior* 60(2016):611-621.

HOY MG & MILNE G. 2010. Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising* 10(2):28-45.

HUNT JA. 2009. Saving Face(book): the influence of technical knowledge on predicting college students' use of privacy settings within the Facebook online social network site. Alabama, South Alabama: University of South Alabama. (Masters' thesis.)

KAPLAN AM & HAENLEIN M. 2010. Users of the world unite! The challenges and opportunities of social media. *Business Horizons* 53:59-68.

KIM H. 2016. What drives you to check in on Facebook? Motivations, privacy concerns, and mobile phone involvement for location-based information sharing. *Computers in Human Behavior* 54:397-406.

KOKOLAKIS S. 2017. Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. *Computers & Security* 64:122–134.

KOVACH S. 2014. Facebook's privacy policy is changing and you're going to get a long email about it. [Internet: http://www.businessinsider.com/facebook-privacy-policy-change-2014-11; downloaded on 2016-10-28.]

LAREAU LSC. 2007. Understanding online self-disclosure through emerging privacy concerns and norms: a mixed-method approach. Lafayette, Indiana: Purdue University. (Masters' thesis.)

LIAO C, LIU CC & CHEN K. 2011. Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: an integrated model. *Electronic Commerce Research and Application* 10:702-715.

LITT E & HARGITTAI E. 2014. Smile, snap and share? A nuanced approach to privacy and online photo-sharing. *Poetics* 42(2014):1-21.

LIVINGSTONE S. 2008. Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media and Society* 10(3):393-411.

MALHOTRA NK, KIM SS & AGARWAL J. 2004. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Journal of Information Systems Research* 15(4):336-355.

MALIK A, DHIR A & NIEMINEN M. 2016. Uses and gratifications of digital photo sharing on Facebook. *Telematics and Informatics* 33:129–138.

MARLOW C. 2009. How diverse is Facebook? [Internet: https://www.facebook.com/notes/facebook-data-science/how-diverse-is-facebook/205925658858/; downloaded on 2017-03-19.]

MOHAMED AAA. 2010. Online privacy concerns among social networks' users. *Journal of Cross Cultural Communication* 6(4):74-89.

O'NEIL D. 2001. Analysis of internet users' level of online privacy concerns. *Journal of Social Science Computer Review* 19(1):19-21.

OZANNE M, NAVAS AC, MATTILA AS & VAN HOOF HB. 2017. An investigation into Facebook "liking" behavior an exploratory study. *Social Media + Society*:1–12, Apr-Jun.

PALLANT J. 2013**.** SPSS survival manual. 5th ed. New York, NY: McGraw-Hill.

PARK YJ & JANG SM. 2016. African American internet use for information search and privacy protection tasks. *Social Science Computer Review* 34(5):618-630.

PARK N, KEE KF & VALENZUELA S. 2009. Being immersed in social networking environment: Facebook groups, uses and gratifications, and social outcomes. *CyberPsychology and Behavior* 12(6):729-733.

RAACKE J & BONDS-RAACKE J. 2008. My space and Facebook: applying the uses and gratifications theory to exploring friend-networking sites. *CyberPsychology and Behavior* 11(2):169-174.

ROWAN M & DEHLINGER J. 2014. Observed gender differences in privacy concerns and behaviors of mobile device end users. *Procedia Computer Science* 37 (2014): 340-347.

SINGH T & HILL ME. 2003. Consumer privacy and the internet in Europe: a view from Germany. *Journal of Consumer Marketing* 20(7):634-651.

STATISTA. 2015. Average numbers of hours per day spent by social media users on all social media channels as of 4th quarter 2015, by country. [Internet: http://www.statista.com/statistics/270229/usage-duration-of-social-networks-by-country/; downloaded on 2016-10-13.]

STATISTA. 2016. Penetration of leading social networks in South Africa as of 4th quarter 2016. [Internet: https://www.statista.com/statistics/284468/south-africa-social-network-penetration/; downloaded on 2017-03-14.]

STATISTA. 2017. Most famous social network sites worldwide as of January 2017, ranked by number of active users (in millions). [Internet: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/; downloaded on 2017-02-28.]

STUTZMAN F, GROSS R & ACQUISTI A. 2012. Silent listeners: the evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality* 4(2):7-41.

TREPTE S, REINECKE L, ELLISON NB, QUIRING O, YAO MZ & ZIEGELE M. 2017. A cross-cultural perspective on the privacy calculus. *Social Media + Society* 1–13, Jan-Mar.

TUFEKCI Z. 2008. Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin *of Science, Technology and Society* 28(20):20-36.

WORLDWIDE WORX & FUSEWARE. 2015. South African social media landscape 2015. [Internet: http://www.worldwideworx.com/wp-content/uploads/2014/11/Exec-Summary-Social-Media-2015.pdf; downloaded on 2016-09-21.]

WORLDWIDE WORX & FUSEWARE. 2017. South African social media 2017. [Internet: http://www.worldwideworx.com/wp-content/uploads/2016/09/Social-Media-2017-Executive-Summary.pdf; downloaded on 2017-02-28.]

YOUNG AL & QUAN-HAASE A. 2009. Information revelation and internet privacy concerns on social network sites: A case study of Facebook. University Park, Pennsylvania: C&T. (4th International Conference on Communities and Technologies; 25-27 June.)