# Online privacy-related predictors of Facebook usage intensity

Yolanda Jordaan[1*] & Gené Van Heerden[2]

[1]Department of Marketing Management
Economic and Management Sciences 4-114
University of Pretoria, South Africa
Postal address: Private bag X20, Hatfield, Pretoria 0028, South Africa
**Corresponding author*
Tel no: +27 12 420 2997; Work no: +27 12 420 3349;
Mobile no: +27 82 541 6610; Fax no: +27 12 420 2997
E-mail address: yolanda.jordaan@up.ac.za

[2]Department of Marketing Management
Economic and Management Sciences 4-127
University of Pretoria, South Africa
Postal address: Private bag X20, Hatfield, Pretoria 0028, South Africa
E-mail address: gene.vanheerden@up.ac.za

## Abstract

**Purpose** – The paper aims to assess which aspects of online privacy concern and reported privacy behavior predict Facebook usage intensity.

**Design/methodology/approach** – The data were obtained by collecting 598 surveys via a non-probability, convenience sampling method. A logistic regression was conducted to predict high and low Facebook usage intensity with regard to online privacy-related attributes.

**Findings** – The findings indicated that only five of the 16 online privacy-related items predicted Facebook usage intensity. The top three items related mainly to the control of online privacy.

**Research limitations/implications** – The results of the study identify the most important privacy concern and privacy behavior aspects that Facebook should take note of. The significant predictors of Facebook usage intensity could provide insight into those privacy attributes, which are the most critical to address, when considering the continuous evolution of the online privacy model for Facebook.

**Originality/value** – The uses-and-gratification theory and the third-person theory provide a framework for understanding and describing the empirical results – by referring to the tension experienced between online privacy concerns and online privacy behavior. The value of this study lies in the identification of the online privacy-related attributes that significantly predict Facebook usage intensity.

## 1. Introduction

The founder of Facebook, Mark Zuckerberg, has stated that he believes that privacy is no longer a social norm, as online users have become used to sharing their information online, resulting in lower levels of privacy expectation (Shapshak, 2012). Contrary to this belief, a recent study conducted by Stieger et al. (2013) found that individuals who are quitting Facebook do so because they are concerned about their privacy. In fact, their results indicated that privacy concerns outweigh the perceived advantages of Facebook, and that these concerns have ultimately led these individuals to quit Facebook. This behavior should be particularly important for Facebook as a platform, considering the reported decline in users over the past few years, especially in developed countries (Garside, 2013).

Social networking sites such as Facebook require users to build a personal profile by providing personal information. Thereafter, users are encouraged to post and share personal information as part of their online social interactions in building and maintaining social relations with like-minded people (Bornoe & Barkhuus, 2011; Hoy & Milne, 2010). As expected, the social network environment has led to an increased interest in online information privacy, mainly due to the large number of users actively involved in social network systems, coupled with the amount of personal information revealed on such systems (Debatin et al., 2009).

The reality is that there is an inherent tension for users between their desire for social interaction and connection and the need to disclose personal information to enable these interactions. The result is that a user's personal information can be publicly accessible to both known and unknown audiences (Bateman et al., 2011). The downside is that making personally identifiable information visible puts the users at risk of a breach in their privacy (Acquisti & Gross, 2006). Some of the associated risks of making personal information visible include: unwanted contact (including harassment or stalking); unauthorized use of personal information by third parties; identity theft; and surveillance of users' online behavior (Debatin et al., 2009).

A number of theories have been considered when attempting to understand the inherent tension between the concern for information privacy and the disclosure of personal information (also referred to as the 'privacy paradox'). The uses and gratifications theory asserts that people use social network systems to fulfil their need for entertainment, relationships, and identity construction; and this supposedly overrides their privacy concern (Debatin et al., 2009). The third-person effect theory states that people expect social network systems to have greater consequences on others than on themselves: they do not believe that they are at risk, and as a result their privacy concern diminishes (Debatin et al., 2009). Consequently, these two theories provide a framework to understand the current study better.

The purpose of this study is to assess which aspects of online privacy concern and reported privacy behavior predict Facebook usage intensity. Several previous studies have examined the relationship between Internet experience or usage, and online privacy concerns, with mixed results. On the one hand, a few scholars report that users' level of online privacy concern is not affected by the level of their Internet experience (Mohamed, 2010; Yao et al., 2007). On the other hand, scholars have shown that there is a positive direct relationship between users' Internet experience and their online privacy concern, since they are more aware of how data about them could be collected and used against their wishes (Beldad et al., 2011; Corbitt et al., 2003; Singh & Hill, 2003). Adding to the debate, several scholars have reported that users' online privacy concerns actually diminish as the level of their Internet usage and experience increases (Bellman et al., 2004; Cho et al., 2009; Fogel & Nehmad, 2009).

In addition to the reported inconsistencies in previous research about the relationship between online privacy concerns and Internet experience and/or usage intensity, little attention has been paid to reported online privacy *behavior* and its relevance to usage intensity. Filling this gap is important, as it is relevant to know whether protective online privacy behavior actually relates to users' Facebook usage intensity. Furthermore, we expect that reported behavior would give marketers a greater understanding of users, especially since we know that very few users engage in protective behavior, despite the high levels of privacy concern (Debatin et al., 2009).

Further, none of the scholarly work to date has attempted to predict Facebook group membership in terms of usage intensity as it relates to online privacy concerns and behaviour. This suggests the need for research to identify those privacy attributes that contribute most to Facebook usage intensity. As such, this study contributes to the existing theory by identifying those online privacy-related attributes that significantly predict Facebook usage intensity. The findings advance the knowledge of online information privacy by uncovering which privacy-related aspects contribute to low and high Facebook usage intensity.

The findings have value for both privacy scholars and social network practitioners, in terms of dealing with the issue of online privacy for different Facebook users, with the aim of minimizing the negative consequences of future Facebook interactions. In this context, we conducted a logistic regression by dividing the users into two groups according to their Facebook usage intensity levels.

The paper opens with a review of the literature relating to social network systems in general, as well as Facebook and privacy. Next, the methodology adopted for the study is described, after which the findings are presented and discussed. The paper ends by presenting the managerial implications of its findings.

## 2. Literature review

### 2.1. Online privacy and social network systems

Recent years have seen social network systems becoming increasingly popular, with millions of people around the world accessing these sites on a regular basis (Boyd & Ellison, 2008; Mohamed & Ahmad, 2012). At the most basic level, a social network system can be described as a virtual community in which individuals can interact with others through their personal profiles (O'Brien & Torres, 2012). Users join social network systems primarily for social interaction with people who are part of their extended social network, and with people known only virtually (Boyd & Ellison, 2008; Hoy & Milne, 2010; Strater & Lipford, 2008). The profiles of others are browsed to stay aware of social ties, to learn about new contacts, and for pure entertainment (Bornoe & Barkhuus, 2011). Thus social network systems allow users to present information about themselves and to view information about others. For this very reason, social network systems are in essence publicly accessible virtual spaces (Bateman et al., 2011).

One perspective on the public nature of social network systems is that individuals are driven to disclose information about themselves. Disclosing personal information within a social network system has the benefit that it forms and maintains social capital (Ellison et al., 2007). Social capital is the result of the interpersonal relationships and friendships that are created and maintained by social network-system users (Bateman et al., 2011; Debatin et al., 2009), and as such, social capital is not possible without some degree of information disclosure.

Information disclosure on social network systems has received much attention due to the privacy concerns it brings to the fore (Buchanan et al., 2007; Yaakop, 2013). For example, when individuals create their personal profiles online, they decide and modify how much information about themselves is disclosed, or not disclosed, as part of managing their own identity (Strater & Lipford, 2008). In one study, 18 per cent of respondents revealed that they did not disclose their real names when they created their profiles (Fogel & Nehmad, 2009).

However, most users do disclose personal information on the social network systems, as it is needed to build relationships (Christofides et al., 2009; Cho et al., 2009). As such, there is evidence that people disclose large amounts of personal information, even if they are concerned about their online privacy (Acquisti & Gross, 2006; Debatin et al., 2009). This introduces the privacy paradox, which refers to the disconnection between individuals' desire to protect their privacy and their lack of protective behavior (Acquisti & Gross, 2006; Stutzman, 2006; Barnes, 2006). Put in another way, it is when users of social network sites say that they are concerned about their online privacy, yet still disclose detailed personal information on their profiles.

A number of studies have examined the relationship between online privacy concerns and behavior, and mixed results have been reported (Acquisti & Gross, 2006; Buchanan et al., 2007; Dinev & Hart, 2004; Dwyer et al., 2007; Mohamed, 2010; Nov & Wattal, 2009; Tavani, 2008; Young & Quan-Haase, 2009). Some of the studies found that, even though people are concerned about their online privacy, they still participate in social network systems and disclose personal information (Acquisti & Gross, 2006; Dwyer et al., 2007). On the other hand, other studies have indicated that when Internet users have privacy concerns, they are likely to engage in privacy protective behavior (Cho et al., 2009; Fogel & Nehmad, 2008; Hoy & Milne, 2010; Mohamed, 2010; Rustemli & Kokdemir, 2001).

More specifically, a few studies have reported that people with high levels of online privacy concern disclose less personal information on Facebook (Buchanan et al., 2007; Mohamed, 2010; Young & Quan-Haase, 2009). From the afore-mentioned research studies, it may be deduced that a focus on the privacy concerns of online users produces an incomplete picture, since other factors play an important role. Thus it is also necessary to investigate online privacy behavior – including the actions, if any, that people take to safeguard their privacy – in order to get a better understanding and a more holistic picture.

For the purpose of this study, online privacy concern can be described as the process whereby individuals alter their online privacy behavior in order to keep their personal information protected from unwanted viewers (Strater & Lipford, 2008:111). In the Facebook context, online privacy behavior can be defined as the technical protective behaviors undertaken by users to protect their personal information from being disclosed online (Buchanan et al., 2007). Technical protective measures available on Facebook include opting-out of unwanted communications.

A number of theories have been used to interpret online information privacy. An article by Li (2012) reviewed no fewer than fifteen theories. For the purpose of the present study, two media theories were explored in an attempt to understand the inherent tension or privacy paradox phenomenon within the context of the social media systems.

The first is the uses-and-gratifications theory that asserts that people use social network systems to meet their need for entertainment, relationships, and identity construction (Debatin et al., 2009). This theory originated in the 1940s, when early communications research studied the gratifications that attracted audiences (Schramm, 1949). On the basis of this theory, it is speculated that users may consider the trade-off between the merits of a media type (in this case, social networking) versus the potential consequences. In other words, the use of the social media network, together with the gratification received from interacting socially in an online environment, outweighs any privacy concerns that users might have (Hann et al., 2007; Laufer & Wolfe, 1977).

The second theory to be considered is the third-person effect, which states that people expect social network systems to have greater consequences on others than themselves. The third-person effect was first presented by Davison (1983), followed by numerous studies on the influence of the media on the individual and on others (Antonopoulos et al., 2015; Paul et al., 2000; Paradise & Sullivan, 2012; Schweisberger et al., 2014; Zhang & Daugherty, 2010). In principle, the third-person effect has two components: perceptions (in our case, online privacy concerns) and behavior (online privacy-protective behavior). Thus, for the purpose of this study, social network users have lower online privacy concerns and protective behaviors, since they do not believe that they are at risk, thereby underestimating the social media effects on themselves (Debatin et al., 2009; Golan & Banning, 2008).

Against the backdrop of the afore-mentioned media theories, the next section puts online privacy and Facebook usage in perspective.

## 2.2. Online privacy and Facebook usage

In the eleven years since its founding in 2005, Facebook has become an ideal platform for personal socialization. For prospective users to kick-start their personal socialization on Facebook, they have to register a profile. As part of the registration process, Facebook offers the opportunity for the inclusion of personal details such as telephone numbers, home addresses, religious views, and one's relationship status. The platform also allows a user to add friends, share photographs, join groups, and send private or public messages (Strater & Lipford, 2008).

Building a Facebook profile and engaging with others on this platform thus requires a prospective user to divulge personal information – which is counter-intuitive to privacy protection. Facebook began with a network-centric approach to privacy where users decided with whom they wanted to share their information. However, when Facebook evolved into a site that became open to third parties, the settings to allow users to determine which third parties could access their content became very complex. Facebook does offer a basic default setting to create a profile for a new user, but very few users seem to adjust the privacy settings in this default setting (Light & McGrath, 2010).

Many studies have investigated the effectiveness of Facebook’s privacy settings. Govani and Pashley (2005) found that Facebook users either do not make use of their privacy settings, or they willingly accept unknown people as ‘friends’ (Debatin et al., 2009). More recently, following the negative publicity that Facebook received because its default privacy settings were public, they added more privacy setting options for users. These were supposed to enable them to manage their own profiles more effectively (Taraszow et al., 2010).

Nevertheless, if users fail to modify their privacy settings, it effectively means that they are sharing their content with every other Facebook user (Liu et al., 2011). Facebook's default privacy settings are usually set at their lowest; thus users need to be proactive in protecting their privacy. It is clear, then, that while Facebook has presented the world with an entirely new form of communication and means of socializing, it also presents a danger to its users, as their personal information is visible online. In this way, this social network platform makes unauthorized access possible if the user does not take the necessary privacy control measures (Mital & Sarkar, 2011).

Previous research indicates that consumers were found to have a greater trust in Facebook than in other social network systems. In addition, individuals with a Facebook profile have significantly greater risk-taking attitudes than those without one (Fogel & Nehmad, 2009). This raises the issue of whether high-intensity Facebook users have lower online privacy concerns and/or behaviors. The usage of Facebook has been addressed in two ways. First, Facebook usage is described in terms of what the platform itself is used for. Here, a number of studies have examined this form of usage, and their findings show that Facebook is mainly used to search and learn about individuals whom users have met recently, and to stay in touch with friends (Acquisti & Gross, 2006; Fogel & Nehmad, 2009; Strater & Lipford, 2008). The second form of usage – the one that will be considered for the purpose of this study – is where Facebook usage intensity is a measure of a user’s Facebook experience. Besides measuring frequency or duration of usage, Facebook usage intensity also includes the extent to which users are emotionally connected with Facebook, and the degree to which Facebook is integrated into their daily activities (Ellison et al., 2007).

## 3. Research methodology

As noted previously, the purpose of this study is to predict Facebook usage intensity with regard to online privacy concern and protective behavior. Logistic regression allowed us to determine the effect of these two types of privacy-related attributes simultaneously, in order to predict Facebook usage intensity (Pallant, 2011).

### *3.1. Sampling and data collection*

The target population consisted of undergraduate and postgraduate students studying at a large South African university. The unit of analysis was a student cohort who had made use of Facebook during their academic year. Two reasons may be advanced for this choice. First, conducting this study among students is appropriate because this age group represents the majority of active Facebook users in South Africa (Socialbakers, 2014). Second, focusing on Facebook as a social media platform is relevant because Facebook is the biggest and fastest-growing social network system in South Africa. In fact, Facebook is currently the dominant and most-trusted social network system in South Africa, with almost 12 million active users (World Wide Worx & Fuseware, 2015). A non-probability convenience sampling method was used, with an equal distribution between male and female respondents.

The data were collected by means of a survey, using a self-administered questionnaire. The participants were intercepted on campus on a convenience basis. The questionnaire was completed by 598 respondents, and all the responses were usable for analysis.

### *3.2. Measurement instrument*

For the first construct, Facebook usage intensity, six items were measured by using a seven-point Likert-type response format. All the Likert-type response formats used in this study ranged from strongly disagree (1) to strongly agree (7). The Facebook usage intensity scale was taken from Ellison et al. (2007), who reported a Cronbach's alpha value of 0.83. The Cronbach's alpha coefficient for the Facebook usage intensity scale for this study was 0.90.

The second construct, online privacy concern, was also measured by using a seven-point Likert-type response format consisting of 10 items. Malhotra et al. (2004) investigated the Internet users' information privacy concerns scale (IUIPC). For this study, the Cronbach's alpha value was 0.79, which indicates acceptable internal consistency reliability (Nunnally, 1978). Although the IUIPC scale has three sub-dimensions (three privacy control items, three awareness items, and four collection items), each of these items was individually used to meet the purpose of the study. The decision to include the individual items in the logistic regression would allow for better insight into the role that each privacy-related item played, as opposed to privacy dimensions.

Lastly, online privacy behavior was measured by adapting the scale of Buchanan *et al.* (2006) – another seven-point, six-item Likert-type response format. The internal consistency reliability of the scale revealed that the item "I block messages/e-mails from people I do not want to hear from" had a relatively low item-to-total correlation; once it had been deleted, the Cronbach alpha value increased slightly from 0.70 to 0.72. The study of Buchanan *et al.* (2006) reported a Cronbach's alpha value of 0.74.

### *3.3. Data Analysis*

A direct logistic regression was conducted for this study, to predict the outcome category for individual cases by using the most parsimonious model. A logistic regression provides this study with knowledge of the relationships and strengths among the online privacy-related items for the Facebook usage intensity groups (Pallant, 2011). A direct logistic regression was performed with a dichotomous dependent variable – Facebook usage intensity (measured by six items) – where the binary logistic procedure was used. Online privacy concern (measured by 10 items) and online privacy behavior (measured by six items) were the independent variables. This study thus used each of the 16 online privacy-related items to assess how well these items predicted Facebook usage intensity. A forced entry method was used, in which all the predictor variables were tested in one block to evaluate their predictive ability, while controlling for the outcomes of the other predictors in the model (Pallant, 2011).

## 4. Research results

### *4.1. Descriptive statistics*

The sample contained an equal proportion of male and female respondents. The majority of the respondents (89 per cent) were between the ages of 18 and 22 years of age, with the remaining 11 per cent being between 23 and 30 years of age.  The mean for the overall age groups is 20.64 years of age with a standard deviation of 1.67. The median age is 20 years. Table 1 outlines the descriptive statistics of the age sample, including the percentage of gender representation within each age group.

With regard to Facebook usage intensity, the results indicated that 61 per cent of the respondents feel that Facebook is a part of their everyday activities, with 51 per cent of the respondents believing that Facebook has become a part of their daily routine. A total of 35 per cent of the

**Table 1. Descriptive statistics of the Age and Gender groups.**

| Age | Age frequency | Age % | Age % within males | Age % within females |
|---|---|---|---|---|
| 18 years | 14 | 2.3 | 1.3 | 2.3 |
| 19 years | 154 | 25.8 | 26.2 | 25.7 |
| 20 years | 151 | 25.3 | 24.5 | 25.2 |
| 21 years | 126 | 21.0 | 23.2 | 21.0 |
| 22 years | 89 | 14.9 | 13.8 | 14.9 |
| 23 years | 35 | 5.9 | 5.7 | 5.8 |
| 24 years | 20 | 3.3 | 4.0 | 3.3 |
| 25 years | 2 | 0.3 | 0.7 | 0.3 |
| 26 years | 2 | 0.3 | 0.3 | 0.3 |
| 27 years | 1 | 0.2 | 0 | 0.2 |
| 28 years | 2 | 0.3 | 0 | 0.3 |
| 29 years | 0 | 0 | 0 | 0 |
| 30 years | 2 | 0.3 | 0.3 | 0.3 |
|  | 598 | 100 | 100 | 100 |

respondents indicated that they have no preference (neutral) in telling people that they have a Facebook account. Furthermore, the results showed that 61 per cent of the respondents feel out of touch when they have not logged on to Facebook for a while, and 73 per cent of the respondents agreed that they feel a part of the Facebook community. The majority of the respondents (67 per cent) indicated that they would be sad to see Facebook shut down.

The respondents’ number of Facebook friends ranged from 0 to 2 350, with an average number of 475 Facebook friends. A total of 25 per cent of respondents have 200 or fewer Facebook friends, whereas 50 per cent of the respondents had 334 friends or fewer. In terms of the amount of time respondents spend on Facebook daily, the results indicated that the majority of the respondents (63 per cent) spend between zero and 30 minutes a day on Facebook.

### *4.2. Logistic regression*

The first step for the binary logistic regression was to create two mutually-exclusive groups: a high Facebook usage intensity group and a low Facebook usage intensity group. The decision to categorize the two groups was based on the respondents’ level of agreement. For our purposes, only those respondents who agreed or strongly agreed with all the statements were included in the high-usage intensity Facebook group, with the remainder being classified as low-intensity Facebook users.

As noted earlier, logistic regression was conducted to predict Facebook usage intensity, based on 10 online privacy concerns and six online privacy behavior items. At this stage, the baseline results – without any of the online privacy concern or online privacy behavior variables – show that the overall percentage of correctly classified cases is 64.2 per cent. The full model was tested against a constant only model, which was statistically significant, indicating that the predictors, as a set, reliably distinguished between high- and low-intensity Facebook usage ($\chi 2$ (df = 16, N = 598) = 59.37, $p < 0.001$). The overall model explained between 9.5 per cent (Cox and Snell R squared) and 13.3 per cent (Nagelkerke R squared) of the variance in Facebook usage intensity, and correctly classified 71.6 per cent of cases (93.7 per cent for low Facebook usage intensity, and 23 per cent for high Facebook usage intensity), which is an improvement over the 64.2 per cent of the baseline model. Table 2 reports on all the items, and highlights the five items (in bold print) that made a unique statistically-significant contribution to the model.

**Table 2: Logistic regression predicting Facebook usage intensity**

| **Online privacy concern items** | **B** | **S.E.** | **Wald** | **df** | **Sig.** | **Odds ratio** |
|---|---|---|---|---|---|---|
| Right to exercise control over decisions about how information is collected, used, and shared. | 0.234 | 0.109 | 4.581 | 1 | **0.032** | **1.264** |
| Consumer control of personal information lies at the heart of consumer privacy. | 0.239 | 0.115 | 4.340 | 1 | **0.037** | **1.270** |
| Online privacy is invaded when control is lost as a result of a marketing transaction. | 0.279 | 0.103 | 7.370 | 1 | **0.007** | **1.322** |
| Companies should disclose the way the data are collected, processed, and used. | 0.094 | 0.111 | 0.711 | 1 | 0.399 | 1.098 |
| A good consumer online privacy policy should have a clear and visible disclosure. | -0.146 | 0.141 | 1.075 | 1 | 0.300 | 0.864 |
| I should be aware and knowledgeable about how my personal information will be used. | -.147 | 0.122 | 1.454 | 1 | 0.228 | 0.863 |
| It bothers me when online companies ask me for personal information. | 0.046 | 0.101 | 0.206 | 1 | 0.650 | 1.047 |
| I think twice before providing personal information when companies ask for it. | -0.180 | 0.114 | 2.499 | 1 | 0.114 | 0.835 |
| It bothers me to give personal information to so many online companies. | 0.040 | 0.124 | 0.105 | 1 | 0.746 | 1.041 |
| I am concerned that online companies are collecting too much personal information about me. | 0.068 | 0.091 | 0.565 | 1 | 0.452 | 1.071 |
| **Online privacy behavior items** | **B** | **S.E.** | **Wald** | **df** | **Sig.** | **Odds ratio** |
| I watch for ways to control what people send me online. | 0.084 | 0.077 | 1.180 | 1 | 0.277 | 1.088 |
| I remove cookies from my Internet browser. | 0.023 | 0.063 | 0.130 | 1 | 0.718 | 1.023 |
| I use a pop-up window blocker on my Internet browser. | -0.012 | 0.062 | 0.039 | 1 | 0.844 | 0.988 |
| I check my computer for spyware. | -0.177 | 0.059 | 9.074 | 1 | **0.003** | **0.837** |
| I clear my Internet browser history regularly. | -0.032 | 0.058 | 0.303 | 1 | 0.582 | 0.968 |
| I block messages from people I do not want to hear from. | 0.126 | 0.054 | 5.457 | 1 | **0.019** | **1.135** |
| Constant | -3.866 | 0.859 | 20.250 | 1 | 0.000 | 0.021 |

From Table 1, Facebook usage intensity’s strongest predictor was that Facebook users believe that online privacy is invaded when control is lost, with an odds ratio of 1.32. This indicated that respondents who believe that online privacy is invaded when control is lost were 1.32 times more likely to have high Facebook usage intensity than those who did not believe that online privacy is invaded when control is lost, controlling for all other factors in the model. The second-strongest predictor of Facebook usage intensity was the control of personal information. In this case, respondents with control of their personal information were 1.27 times more likely to have high Facebook usage intensity than those who did not have control of their personal information.

Next, respondents who exercised control over their information decisions were 1.26 times more likely to have high Facebook usage intensity than those who did not exercise control over information decisions. It is interesting to note that the three strongest predictors relate to online privacy concern items, while the remaining two predictors relate to online privacy behavior.

Respondents who block information from unknown people were 1.14 times more likely to have high Facebook usage intensity than those who did not block information from unknown people. Finally, the odds ratio of 0.84 for those respondents checking their computers for spyware was less than 1, indicating that for every additional spyware check-up, the respondents were 0.84 times less likely to have high Facebook usage intensity, controlling for all other factors in the model.

## 5. Discussion and conclusions

This study has considered online privacy concern, and it has reported online privacy protective behavior in terms of two media theories related to the social network environment. These theories were considered against the backdrop of the privacy paradox, where users report concern about their privacy within the social environment but do not apply these concerns to their usage behavior (Norberg et al., 2007). The uses-and-gratifications theory encompasses the need for entertainment, relationships, and identity construction, which, in this case, can override Facebook users' privacy concerns.

In this study, the majority of the respondents indicated that Facebook is a part of their lives and daily routine, and that it would be sad if Facebook were to shut down. The majority of the respondents agreed that: a) they are proud to tell people they are on Facebook (96 per cent); b) they feel part of the Facebook community (73 per cent); and c) they feel out of touch when they are not logged on to Facebook (61 per cent). These findings highlight the fact that Facebook contributes to users' identity construction, entertainment, and relationship value.

One of the gaps identified in this study was the lack of knowledge of how well online privacy concern and online privacy behavior predict Facebook usage intensity. From the realized sample of 598 student respondents, a direct logistic regression was conducted to identify the privacy-related items that were of importance to high-intensity and low-intensity Facebook users. The findings of the logistic regression showed that five of the 16 privacy-related items predicted the likelihood that the respondents would have high Facebook usage intensity.

The findings of this study have several implications for privacy researchers and Facebook developers and/or marketers. For privacy academics, this study fills the research gap of knowing which privacy concerns and behaviors contribute most to Facebook usage intensity. Previous studies of privacy in social network systems have dealt with privacy concern and Internet usage, but the findings were mixed. Also, not many studies have dealt with privacy-protective behaviors, especially with regard to the intensity levels of Facebook users.

The findings from the logistic regression revealed that three privacy-concern items and two privacy-behavior items were powerful predictors of Facebook usage intensity. The results of this study indicated that the issue of control seems to be one of the main issues for low-intensity Facebook users. This is evident in that control was identified as the top three predictors of Facebook usage intensity: online privacy is invaded when control is lost; wanting control of personal information; and finally, one's right to control decisions on personal information.

The control issue relates to the feeling that users believe they have lost control when engaging in marketing transactions. As a result they feel that they have a right to control the way their information is used. This highlights the importance of the control issue to Facebook, since the site should clearly communicate to users when third-party individuals have access to users' personal information. This concern about control can escalate as a result of Facebook's latest changes, which now include tracking users' browsing and shopping habits. For example, Facebook tracks online browsing habits to provide users with more targeted advertisements. Also, when users purchase from a Facebook advertisement or promotion, Facebook shares this purchase information with the advertisers. Thus, in reality, if users do not actively set the opt-out function in their Facebook privacy settings, tracking of their browsing and shopping behavior will continue, and personal information will be shared with third parties (Facebook, 2015).

It is important, therefore, that Facebook explicitly informs users of these recent changes, and communicates to users that they should opt-out if they do not want this sharing to take place. The ideal is probably for Facebook to prompt users before sharing information with third parties. It thus seems that, if users perceive that they have control over the quality and accessibility of their own personal information – their preferred way to manage their privacy – this might reduce their online privacy concern. This is in line with the findings of other studies (Acquisti & Gross, 2006; Tavani, 2008).

The two reported privacy behavior items that showed significance related to privacy protection by blocking messages or checking for spyware to eliminate the monitoring of online activities. However, the only protection within Facebook currently is for Facebook users to manage their own privacy settings. This might be an issue that Facebook should address by involving the users either through developing a gamification element that will engage users in an entertaining way in managing their privacy settings, or by providing stricter guidelines for third parties when entering the Facebook environment.

Another suggestion is that it might be worthwhile for Facebook to educate users in managing and controlling their own privacy settings. In this regard, Facebook has recently added a ‘privacy basics page’ with answers to frequently-asked questions (Kovach, 2014) as well as a new ‘privacy check-up tool’ to help users manage their Facebook settings (Guynn, 2014). This tool allows users to review the privacy aspects of their profiles, and their visibility to others. This should assist users to manage their privacy settings; and in so doing, they should feel more in control of their personal information.

Facebook could also think of involving its users by asking them for innovative ideas for dealing with the issue of online privacy. This might create a sense of ownership in addressing the privacy issue, and put users in better control of their information.

Facebook could also consider annual reminders on users’ Facebook pages to update the existing privacy settings, and to inform users of any changes or new settings available. At least Facebook has recently reduced the privacy policy from 9 000 words to only one page of 2 700 words, with design improvements and clearer explanations to make it easier for users to read (Facebook, 2015).

## 6. Limitations and future recommendations

This study has employed a cross-sectional survey as the primary research method, using a convenience sample. As such, the findings of this study cannot be generalized to all Facebook users. It is suggested that future studies include different adult populations, given some evidence that different generations deal with Facebook, and privacy, differently (Dries et al. 2008; Helsper, 2010). Future research may also want to compare users from developed versus developing countries, in order to explore whether privacy needs differ according to the level of social network usage in the different countries. This may yield interesting results – considering that, for example, Facebook is growing strongly in South Africa, but is declining in many other countries (World Wide Worx & Fuseware, 2015).

The context of this study was limited to Facebook, which might affect the results, as different privacy aspects might be more or less important in different social network systems. Future studies might consider conducting a similar study on a different social network platform, to investigate whether different aspects related to privacy are deemed more or less important than those highlighted in this study.

For this study, perceptions on online privacy concern and behavior were investigated among Facebook users in general. A more specific group fan page might have presented different results. This could also be an interesting avenue for future research. What might also provide interesting insight is to use data mining techniques to analyze Facebook usage and to align this with the privacy concern and behavior of users. Another suggestion for future researchers is to consider an experimental design through which one could create different Facebook conditions, in order to observe the effect that the changes have on users' protective privacy behavior.

## References

Acquisti, A. & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Privacy Enhancing Technologies*, 4258, 1-22. http://dx.doi.org/10.1007/11957454_3.

Antonopoulos, N., Veglis, A., Gardikiotis, A., Kotsakis, R. & Kalliris, G. (2015). Web third-person effect in structural aspects of the information on media websites. *Computers in Human Behavior*, 44, 48-58. http://dx.doi.org/10.1016/j.chb.2014.11.022.

Bateman, P.J., Pike, J.C. and Butler, B.S. (2011). To disclose or not: Publicness in social networking sites. *Information Technology & People*, 24(1), 78-100. http://dx.doi.org/10.1108/09593841111109431.

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. http://dx.doi.org/10.1016/j.chb.2011.07.002

Bellman, S., Johnson, E.J., Kobrin, S.J. & Lohse, G.L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society: An International Journal*, 20(3), 312-324. http://dx.doi.org/10.1080/01972240490507956.

Bornoe, N. & Barkhuus, L. (2011). Privacy management in a connected world: Students' perception of Facebook privacy settings. *Workshop on Collaborative Privacy Practices in Social Media*, 19-23 March, Hangzhou, China, http://www.bornoe.org/papers/CSCW2011-Collaborative-Privacy-Workshop-bornoe.pdf (accessed 11 November 2012).

Boyd, D.M. & Ellison, N.B. (2008). Social network sites: Definition, history and scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210-230. http://dx.doi.org/10.1111/j.1083-6101.2007.00393.x.

Buchanan, T., Paine, C., Joinson, A.N. & Reips, U. (2007). Development of measure of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157-165. http://dx.doi.org/10.1002/asi.20459.

Cho, H., Rivera-Sánchez, M. & Lim, S.S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society*, 11(3), 395-416. http://dx.doi.org/10.1177/1461444808101618.

Corbitt, B.J., Thanasankit, T. & Yi, H. (2003). Trust and e-commerce: A study of consumer perceptions. *Electronic Commerce Research and Applications*, 2(3), 203-215. http://dx.doi.org/10.1016/S1567-4223(03)00024.

Christofides, E., Muise, A. and Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *Cyberpsychology & Behavior,* 12(3), 341-345. http://dx.doi.org/10.1089/cpb.2008.0226.

Davison, W.P. (1983). The third-person effect in communication. *Public Opinion Quarterly*, Vol. 47(1), 1-15. http://dx.doi.org/10.1086/268763.

Dinev, T. and Hart, P. (2004). Internet privacy concern and their antecedents – measurement validity and a regression model. *Behaviour & Information Technology*, 23(6), 413-422. http://dx.doi.org/10.1080/01449290410001715723.

Debatin, B., Lovejoy, J.P., Horn, A. & Hughes, B.N. (2009). Facebook and online privacy: Attitudes, behaviours, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1), 83-108. http://dx.doi.org/10.1111/j.1083-6101.2009.01494.x.

Dries, N., Pepermans, R. & De Kerpel, E. (2008). Exploring four generations' beliefs about career: Is 'satisfied' the new 'successful'? *Journal of Managerial Psychology*, 23(8), 907-28. http://dx.doi.org/10.1108/02683940810904394.

Dwyer, C., Hiltz, S. & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. In *Proceedings of the Thirteenth Americas Conference on Information Systems,* Keystone, Colorado. http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1849&context=amcis2007.

Ellison, N.B., Steinfield, C. & Lampe, C. (2007). The benefits of Facebook “friends”: Social capital and college students’ use of online social network sites. *Journal of Computer-Mediated Communication*, 12(4), 1143-1168. http://dx.doi.org/10.1111/j.1083-6101.2007.00367.x

Facebook. (2015). How do we use this information? https://www.facebook.com/about/privacy (accessed 2 February 2015).

Facebook. (2015). Updating our terms and policies: Helping you understand how Facebook works and how to control your information, https://www.facebook.com/about/terms-updates (accessed 2 February 2015).

Fogel, J. & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior,* 25(1), 153-160. http://dx.doi.org/10.1016/j.chb.2008.08.006.

Garside, J. (2013). Facebook loses millions of users as biggest markets peak, *The Guardian, 29 April*, http://www.theguardian.com/technology/2013/apr/28/facebook-loses-users-biggest-markets (accessed 2 February 2015).

Golan, G.J. & Banning, S.A. (2008). Exploring a link between the third-person effect and the theory of reasoned action: Beneficial ads and social expectations. *American Behavioral Scientist*, 52(2), 208-224. http://dx.doi.org/10.1177/0002764208321352.

Govani, T. & Pashley, H. (2005). Student awareness of the privacy implications when using Facebook. Paper presented at the “Privacy Poster Fair” at the Carnegie Mellon University School of Library and Information Science, http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf (accessed 2 February 2015).

Guynn, J. (2014). Facebook rolling out privacy check-up for users, *US Today, 4 September*, http://www.usatoday.com/story/tech/2014/09/04/facebook-privacy-checkup-tool/15067743/ (accessed 2 February 2015).

Hann, I., Hui, K., Lee, S.T. & Png, I.P.L. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, 24(2), 13-42. http://dx.doi.org/10.2753/MIS0742-1222240202.

Helsper, E.J. (2010). Gendered internet use across generations and life stages. *Communication Research*, 20(10), 1-23. http://dx.doi.org/10.1177/0093650209356439.

Hoy, M.G. & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising,* 10(2), 28-45. http://dx.doi.org/10.1080/15252019.2010.10722168.

Kovach, S. (2014). Facebook's privacy policy is changing and you're going to get a long email about it, http://www.businessinsider.com/facebook-privacy-policy-change-2014-11 (accessed 2 February 2015).

Laufer, R.S. & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional, developmental theory. *Journal of Social Issues*, 33(3), 22-42. http://dx.doi.org/10.1111/j.1540-4560.1977.tb01880.x.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, 54(1), 471-481.

Light, B. & McGrath, K. (2010). Ethics and social networking sites: A disclosive analysis of Facebook. *Information Technology & People,* 23(4), 290-311. http://dx.doi.org/10.1108/09593841011087770.

Liu, Y., Krishnamurthy, B., Gummadi, K.P. and Mislove, A. (2011). Analysing Facebook privacy settings: User expectations vs reality. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference,* Berlin, Germany, 61-70. http://dx.doi.org/10.1145/2068816.2068823.

Malhotra, N.K., Kim, S.S. & Agarwal J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information System Research*, 15(4), 336-355. http://dx.doi.org/10.1287/isre.1040.0032.

Mohamed, A.A. (2010). Online privacy concerns among social networks' users. *Cross-Cultural Communication*, 6(4), 74-89. http://dx.doi.org/10.3968/j.ccc.1923670020100604.015.

Mohamed, A.A. & Ahmad, I.H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28, 2366–2375. http://dx.doi.org/10.1016/j.chb.2012.07.008.

Mital, M. & Sarkar, S. (2011). Multihoming behaviour of users in social networking web sites: A theoretical model. *Information Technology & People,* 24(4), 378-392. http://dx.doi.org/10.1108/09593841111182250.

Norberg, P.A., Horne, D.R. & Horne, D.A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), 100-126. http://dx.doi.org/10.1111/j.1745-6606.2006.00070.x.

Nov, O. & Wattal, S. (2009). Social computing privacy concerns: Antecedents & effects. In *Conference on Human Factors in Computing Systems in Boston, 4-9 April,* ACM, New York, 333-336. http://dx.doi.org/10.1145/1518701.1518754.

Nunnally, J. (1978). *Psychometric Theory*, 2nd ed., McGraw Hill, New York, NY.

O'Brien, D. & Torres, A.M. (2012). Social networking and online privacy: Facebook users' perceptions. *Irish Journal of Management*, 31(2), 63-97. http://dx.doi.org/10379/4059.

Pallant, J. (2011). *SPSS Survival Manual*. 4th ed. Allen & Unwin, Australia.

Paradise, A. & Sullivan, M. (2012). (In) visible threats? The third-person effect in perceptions of the influence of Facebook. *Cyberpsychology, Behavior, and Social Networking*, 15(1), 55-60. http://dx.doi.org/10.1089/cyber.2011.0054.

Paul, B., Salwen, M.B. & Dupagne, M. (2000). The third-person effect: A meta-analysis of the perceptual hypothesis. *Mass Communication & Society*, 3(1), 57-85. http://dx.doi.org/10.1207/S15327825MCS0301_04.

Rustemli, A. & Kokdemir, D. (1993). Privacy dimensions and preferences among Turkish students. *Journal of Social Psychology*, 133(6), 807-814. http://dx.doi.org/10.1080/00224545.1993.9713942.

Schramm, W. (1949). The nature of news. *Journalism Quarterly*, 26(3), 259–269. http://search.proquest.com/docview/1290640447?accountid=14717.

Schweisberger, V., Billinson, J. & Chock, T.M. (2014). Facebook, the third-person effect, and the differential impact hypothesis. *Journal of Computer-Mediated Communication*, 19(3), 403-413. http://dx.doi.org/10.1111/jcc4.12061.

Shapshak, T. (2012). Privacy becoming extinct on the net. *Sunday Times*, 4 March, 8. http://www.timeslive.co.za/sundaytimes/2012/03/04/privacy-becoming-extinct-on-the-net.

Singh, T. & Hill, M.E. (2003). Consumer privacy and the Internet in Europe: A view from Germany. *Journal of Consumer Marketing*, 20(7), 634-651. http://dx.doi.org/10.1108/07363760310506175.

Socialbakers. (2014). South Africa Facebook statistics, http://www.socialbakers.com/facebook-statistics/south-africa (accessed 7 March 2014).

Strater, K. and Lipford, H.R. (2008). Strategies and struggles with privacy in an online social networking community. In *Proceedings of the 22nd British HCI Group*, British Computer Society Swindon, UK, 111-119. http://dx.doi.org/10.1023/B:BTTJ.0000047585.06264.cc.

Stieger, S., Burger, C., Bohn, M. & Voracek, M. (2013). Who commits virtual identity suicide? Differences in privacy concerns, internet addiction, and personality between Facebook users and quitters. *Cyberpsychology, Behavior and Social Networking*, 16(9), 629-634. http://dx.doi.org/10.1089/cyber.2012.0323.

Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. *International Digital and Media Arts Journal*, 3(1), 10-18.

Tabachnick, B.G. & Fidell L.S. (2013). *Using multivariate statistics*, 6th ed., Pearson, Upper Saddle River.

Taraszow, T., Aristodemou, E., Shitta, G., Laouris, Y. & Arsoy, A. (2010). Disclosure of personal and contact information by young people in social networking sites: An analysis using Facebook profiles as an example. *International Journal of Media & Cultural Politics*, 6(1), 81-101. http://dx.doi.org/10.1386/macp.6.1.81/1.

Tavani, H.T. (2008). Information privacy: Concepts, theories, and controversies. In Himma, K.E. and Tavani, H.T. (Eds), *The Handbook of Information and Computer Ethics,* Wiley Publishers, New Jersey, 131-163. http://dx.doi.org/10.1002/9780470281819.ch6.

World Wide Worx & Fuseware. (2015). South African social media landscape 2015, http://www.worldwideworx.com/wp-content/uploads/2014/11/Exec-Summary-Social-Media-2015.pdf (accessed 15 December 2015).

Yaakop, A. (2013). Like it or not: Issue of credibility in Facebook advertising. *Asian Social Science*, 9(3), 153-163. http://dx.doi.org/10.5539/ass.v9n3p154.

Yao, M.Z., Rice, R.E. & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, 58(5), 710-722. http://dx.doi.org/10.1002/asi.20530.

Young, A.L. & Quan-Haase, A. (2009). Information revelation and internet privacy concerns on social network sites: A case study of Facebook. In *Proceedings of the Fourth International Conference on Communities and Technologies, Pennsylvania*, ACM, New York, 265-274. http://dx.doi.org/10.1145/1556460.1556499.

Zhang, J., & Daugherty, T. (2010). Third-person effect comparison between US and Chinese social networking website users: Implications for online marketing and word-of-mouth communication. *International Journal of Electronic Marketing and Retailing*, 3(3), 293-315. http://dx.doi.org/10.1504/IJEMR.2010.034833.