Journal of Information Privacy & Security

JIPS

An official publication of the Global Business Resource Center at the University of Wisconsin-Whitewater

Volume 9, Issue 4, 2013

ILP

Ivy League Publishing
P.O. Box 680392
Marietta, Georgia 30068, USA
Ph: (770) 649-6718
Fax: (770) 565-4721
E-mail: admin@ivylp.com
http://www.ivylp.com

Editor-in-Chief

Kallol Bagchi , Ph.D
The University of Texas at El Paso

Journal website
http://jips.utep.edu

Journal of Information Privacy and Security (JIPS)

Volume 9, Issue 4, 2013

Table of Contents

An Empirical Investigation of Privacy Awareness and Concerns on Social Networking Sites

Sunil Hazari (corresponding author), Richards College of Business, University of West Georgia Carrollton, GA 30118, USA, shazari@westga.edu

Cheryl Brown, Richards College of Business, University of West Georgia Carrollton, GA 30118, USA, cbrown@westga.edu

ABSTRACT

Privacy affects every user who exchanges information over the Internet. In the past few years, the growth of information on social networks (such as Facebook, Twitter, LinkedIn) has increased exponentially. Companies are harvesting this information with and without the knowledge of individuals. While the exchange of information and seamless interaction between individuals and groups has become an easy task, issues related to this exchange, such as information privacy and security, have created new challenges. This study investigated respondents' attitudes towards privacy on social networking sites. In addition, the study sought to ascertain whether socio-demographic variables and knowledge of privacy issues influence attitudes and privacy concerns towards using social computing sites. Data analysis includes descriptive profile analysis, and statistical validation of attitudes and privacy concerns by means of correlation, regression, and cluster analysis. There was a significant relationship between privacy awareness and knowledge based on information provided by respondents. Most socio-demographic variables did not show significant effects on information privacy concerns. Implications of the findings are discussed. Further research is needed to investigate individual concerns on specific information that is being collected, stored, and shared on popular social networking sites.

KEYWORDS

Social Media, Social Networking, Privacy Knowledge, Attitudes & Concerns

INTRODUCTION

The digital age has made it possible to generate and collect large amounts of data with minimum effort. Data collection has been facilitated by open social networks where information flows at a rapid pace. For example, Marketing professionals use social networks to communicate with customers, monitor metrics, observe competitors, and for information analysis concerning brands, products, and company image (Rinaldo, Tapp, & Laverie, 2011). The ease with which information can be collected and

processed by companies, marketers, and web site operators has raised concern for the information age (Smith, Dinev, & Xu, 2011). Purcell, Brenner, and Rainie (2012) report that most users disapprove of personal information being collected for search results or for targeted advertising. However, looking at the content being posted and the number of searches being conducted every second, users are willing to give up information in return for customized information to fulfill a need to seek information, communicate, interact, or complete a transaction. Companies are collecting information from users and selling this information to other stakeholders, often disregarding the privacy aspect under which data were collected in the first place. Social networking sites such as Facebook, YouTube, Twitter, Google Plus, and LinkedIn have transformed the way in which consumers generate, share, and interact with information (Patterson, 2012). Using technical enablers of accessing services via mobile phones, tablets, netbooks, and desktop computers, social computing has enabled real-time interactions between individuals, groups, and businesses. Information is being stored and collected via cloud computing, Radio Frequency Identification (RFID), Near Field Communication (NFC), and biometric systems. Privacy on social networking sites is different from privacy when browsing the web because social networking sites have identity as well as demographic information that can be associated with users when they are logged in and browse for products and services displayed on social networking sites.

The millennial generation has grown up with texting, sharing photos, posting on blogs, and interacting on social media sites from their laptops and mobile devices (Alsop, 2008). This form of communication is their preferred mode as compared to the older generation who grew up with voice calls and e-mails. Technology has become user friendly, and as a result, individuals are volunteering more information about themselves when they interact with friends, acquaintances, and strangers on social networking sites. Although most web browsers include a 'do not track' button, this feature is seldom used because the feature is not automatically activated by default. Consumers are not aware that there is constant data collection underway on social networking sites (Shilton, 2009). Tweets, blogs, wikis, and videos are full of information about an individual's attitudes and opinions over a range of personal and professional topics. Information about individuals is openly available on the Internet. Companies are looking to collect browsing data from individuals to target advertisements that may be of potential benefit to the user. Information privacy is a complex concept that has been studied from many perspectives to include psychology, marketing, management, and information systems (Pavlou, 2011). Unfortunately, issues associated with social computing interaction, such as security and privacy, have taken a back seat to the ease with which information can be exchanged or compromised. There is therefore a strong need to study information privacy in relation to individuals who use social networking sites.

Purpose of the Study

The current generation of students is growing up in a social environment that is progressively interactive and communication intensive (Li, Greenberg, & Nicholls, 2007). Interaction in social media and networking environments gives rise to issues such as privacy and security. The issue of privacy has been studied from an

organizational perspective (Bessen, 1993; Milberg, Smith, & Burke, 2000) as well as individual perspective (Malhotra, Kim, & Agarwal, 2006), but these studies have not addressed attitudes towards privacy specific to social computing. For the purpose of this study, the term "Social Computing" is used to indicate user interaction on Web 2.0 and Social Media sites such as Facebook, YouTube, Twitter, LinkedIn, Pinterest and Google Plus.

More empirical investigation is needed from an individual point of view because interactions on social networking sites are mostly done by individuals from personal accounts. Hazari, Hargrave, and Clenney (2008), in their study related to information security behavior, called for more research on socio-demographic factors that affect user behavior towards information security and privacy. Individuals who use social computing sites range from those who are extremely concerned about privacy issues, to those who would not hesitate to provide any personal information if requested by the site. This difference in attitude towards privacy may be attributed to various socio-demographic factors such as age, gender, and/or behavioral factors such as previous experience in using social computing. There is evidence to suggest that gender and age may influence attitude towards privacy (Sheehan, 1999). Graeff and Harmon (2002) found that privacy concerns vary by age, income, and gender. Their research showed that younger consumers were more aware of data collection practices while older consumers were more likely to be concerned about financial privacy. Some studies have also reported constructs such as trust (Eastlick, Lotz, & Warrington, 2006), ethics (Culnan, & Williams, 2009), and cultural values (Milberg, Burke, Smith, & Kallman, 1995) are also related to privacy concerns.

While of the focus of previous studies have been mostly in relation to purchasing behavior, there is a strong need to study information privacy in relation to individuals who use social networking sites. Stutzman (2006) stated that social networking profiles for an individual ranges from the relatively innocuous (favorite book or movie) to the potentially invasive (such as sexual orientation, political views, and photos). This data could be harvested for ancillary purposes such as target marketing or compromised as a result of identity theft. Although the Stutzman study provided direction to other researchers, it used a very small sample so the findings cannot be generalized even across the college student population which was the selected demographic for the study. Also, only one of the three social networking sites used in that study exists today as a popular destination for social interaction. There is a need to provide updated information on privacy concerns of young adults who frequent popular social networking sites. This study investigated attitudes towards social computing privacy, and socio-demographic factors that may be related to these attitudes. A Privacy Awareness Score was computed based on survey responses. Investigating attitudes and preferences can provide deeper insights into actual behavior (Ajzen & Fishbein, 1977; Melone, 1990). In this study the attitude survey was designed to include cognitive, affective, and behavioral responses that are typically used when measuring attitude (Bagozzi & Burnkrant, 1979; Gonzalez, 1992). A survey instrument was developed to explore business students' attitudes toward online privacy on social networking sites, as well as their knowledge, understanding and preferences towards online privacy issues.

SOCIAL COMPUTING ENVIRONMENT

On social computing sites, companies have partnered with the sites to offer incentives (such as coupons) and get more information about the user to the sites. This information may be sold to other third party vendors who build a profile of the user based on aggregated data from multiple sites. The web has grown from static to an interactive medium. It is now accessible via mobile devices that are ubiquitous for the digital generation as can be seen from this study which found that a majority of respondents access sites from their smartphones. More research is needed to explore specific characteristics that may affect privacy as it relates to the use of social media sites.

For example, Geolocation and behavioral targeting are becoming very sophisticated and integrated into web advertising networks (Wang, Burgener, Kuzmanovic, & Maciá-Fernández, 2011). In the Web 2.0 world, most consumers expect some tracking is done by companies so data and personal information is always at a risk of exposure. Contextual or behavioral advertising generates the revenue stream for companies that are collecting a lot of data. This revenue stream supports free content that consumers expect to be available to them. Marketers are interested in collecting information from consumers because they want granular information on consumers so they can tailor advertising in a personalized way. This is done by knowing more about the tastes, behaviors and fears of the target market (Chaney, 2009).

Consumers are prepared to reveal personal information in exchange for rewards such as coupons, promotions and incentives. The privacy paradox has been reported in literature as the willingness by users to provide information despite acknowledging their concern for privacy issues (Acquisiti & Grossklags, 2005; Barnes, 2006). Further, the privacy calculus takes into account the value placed on certain pieces of personal information which are relinquished in exchange for promotional items (such as coupons), but other information which is considered more valuable is retained and protected from marketers (Varian, 2006). Privacy has a technical as well as a behavioral component, but it is up to the user to be aware of the differences between these types of controls. Using technical controls, privacy can be controlled by using in-browser privacy protection (Chen & Rea, 2004). A privacy policy should be clear in explaining data that will be collected when visitors use the website. Related to data and information gathering, companies are expected to disclose the terms of service on how the data collected will be stored, used, and shared. Belanger and Crossler (2011) have called for more studies that investigate user input and profiles into information privacy practices followed by companies. With the exponential growth of social computing, there is a demonstrated need to study which variables affect aspects of information privacy when consumers visit social networking sites.

Legal issues related to Privacy

On the Internet, there is a tradeoff between personal information and service, and legal issues arise as a result of accessing information over the Internet. Over the years there have been many laws related to electronic communication that have addressed data and information access. For example, the Electronic Communications Privacy Act was passed in 1986, before the Internet became an essential means of communication.

This law stated that if information is stored on a server, the law makes it easy for law enforcement or the government to access it via a subpoena. The CAN-SPAM Act of 2003 attempted to regulate commercial email messages. The law did not just apply to bulk email as it also included any commercial message where a commercial product or service is promoted. Regulations that govern privacy are essential to support open exchange of information between individuals, businesses, and networks. There are other types of laws that govern information exchange between companies and users on websites and social computing sites. Few individuals are aware of how these laws affect use of social media sites. In 1998 the Child Online Privacy Protection Act (COPPA) legislation was introduced to protect minors. The legislation required parents' permission before kids less than thirteen years of age could give out personal information on websites. If a web user was under thirteen years old, he/she was not required to provide any personal information. The COPPA legislation is dated since it was introduced 15 years ago and the generation of web innovation since then has seen rapid changes in the ways the web has evolved.

There has been a shift from individual marketing to group marketing as is evidenced by popularity of social networking sites such as Facebook and Twitter. Previously the model for Internet digital marketing was one-to-one which targeted individuals who were web users. Today, companies are not only trying to influence individuals but also connect with other contacts of that individual. The Federal Trade Commission has requested updates to privacy laws for kids on the web, but getting product advertisers, privacy advocates, and web operators to agree on ground rules is not always easy. These laws are needed for the protection of individuals who interact on social computing sites (Foster & Greene, 2012). For example, the use of real names on social networking sites (especially Facebook and LinkedIn) makes individuals vulnerable to identity theft. This is because in addition to the name, other personal information such as birthdate, hometown, and phone number is also available for view if the privacy control is not set. Triangulating this information with other public (and publicly available) information such as property records, tax assessor files, court files, and professional and business licenses would allow digital profiling which could be used to perpetuate identity theft.

Privacy issues of social computing sites

The launch of any new social computing site usually raises questions and concerns regarding privacy. For example, in 2010, when Google announced its new service that would share users' information it led to lawsuits and complaints to the Federal Trade Commission. While the Internet provides a venue for instant exchange of communication and information, it also invites ways in which data and privacy can be compromised by using websites, apps, and services that hold user information which can include usernames, passwords, addresses, phone numbers, credit card numbers, and transaction history. The nature of the social computing site may determine the amount of privacy given to a user of that service. For example, on Twitter, tweets are by default open to the public and can be read by any Twitter user. On the other hand, Facebook provides the user better privacy by having the user set controls on who can view the content. However, Facebook has been known to change its Terms of Service which affects how information can be shared which may be different from what a user

had agreed to in the past (Mckeon, 2010). Often users skip reading the new Terms of Service or making changes based on how the new policy may affect their posts.

With over 1 billion users, Facebook is the largest social media site. Most young people have an insatiable appetite for the social nourishment provided by social media sites such as Facebook (Patterson, 2012). Extensive data collection takes place on Facebook as it generates revenue by selling user data to advertisers. The collection and sale of data is achieved by using Facebook apps as well as third-party plug-ins that may collect consumer information such as IP number location, search keywords, user's web history and browser type. For the digital generation this is normal activity in the way they connect, communicate and relate to their friends. Individuals are on their own to decipher complicated privacy policies when interacting with companies. A typical Facebook user does not typically think about business models or data collection. Regarding changing privacy settings, it is not uncommon to find that users have left the settings at the default level when they first joined the site. This is typical behavior as Human Computer Interaction research has reported that users tend not to change default settings (Mackay, 1991).

Facebook has been struggling over the years with trying to define an optimum privacy policy that would be acceptable to users and businesses. In 2009 Facebook made personal information such as the Friends List public without informing users of this change. They also retained information of deleted accounts which included photos and videos associated with those accounts when it was active. Facebook settled with the FTC and agreed to allow independent auditors to come in every six months for the next 20 years to review their privacy policy compliance (Sengupta, 2011). The FTC has negotiated similar agreements with other social media sites such as Google and Twitter. There have been many concerns raised over Facebook privacy but this has not detracted from the number of users interacting daily on the website to communicate with friends, relatives, associates, and companies. As users spend more time connected to social media sites, the amount of information being shared and stored on these sites is increasing daily. Communication in Facebook is done by using the timeline, mail, photos, videos, chat, pages, groups, and third party apps. Any of this information can be retained by Facebook and can potentially be divulged to third parties. The exchange of information is governed by Facebook privacy policies that users agree to when signing up for a new account. However these policies have been tweaked over time and users are expected to abide by the new policies. A user's basic default privacy setting can be controlled under the Privacy Settings page but under this page are additional settings that control who can find the user on Facebook. Some other privacy settings can also include Timeline and Tagging where others can see portions of your timeline and identify you in photos and videos. Additional privacy can be set by allowing Facebook applications and third party access to the user's account including making their page appear on Google results and Public searches. Block lists can be used to prohibit certain users from accessing user information and a user may also choose to secure the account by enabling logins from known devices and sending alerts if the user account is accessed from an unknown device. As can be

seen from these options, the privacy and security settings can be overwhelming to a typical user.

The changes to Facebook privacy policies have been well documented. Opsahl (2010) provides a historical look at aspects of Facebook privacy policy over the years. For example, in 2005, the Privacy Policy stated:

No personal information that you submit to Facebook will be available to any user of the Web Site who does not belong to at least one of the groups specified by you in your privacy settings.

In 2007 this changed to:

Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, school name, and profile picture thumbnail will be available in search results across the Facebook network unless you alter your privacy settings.

In 2010 this was further changed to:

When you connect with an application or website it will have access to General Information about you. The term General Information includes your and your friends' names, profile pictures, gender, user IDs, connections, and any content shared using the Everyone privacy setting. ... The default privacy setting for certain types of information you post on Facebook is set to "everyone." ... Because it takes two to connect, your privacy settings only control who can see the connection on your profile page. If you are uncomfortable with the connection being publicly available, you should consider removing (or not making) the connection.

Facebook is today the leader in the digital marketing landscape (Holzner, 2008) and the largest social networking site. Opsahl (2010) believes that the shift from user control of their personal information during the initial stages of Facebook (i.e. when it was first launched in 2004) to gradually allowing more access to user information by advertising and business partners, has been a sign of times as a result of increasing growth, competition, and business focus which has limited users' option to control their own information.

Previous studies on Privacy

Previous research studies have investigated privacy related issues for individuals under different conditions such as study of purchasing behavior, loyalty cards, banking, and social networking. A summary of significant studies related to privacy is shown in Table 1.

Table 1: Previous Privacy Research

Source	Focus	Sample	Environment
Castañeda & Montoro (2007)	Trust, Purchase Decision, Intent to buy, Intent to provide information	Undergrad Business Students	Web Transactions
Graeff & Harmon (2002)	Discount Cards Loyalty Cards Supermarket Cards	Consumers	Retail
Stutzman (2006)	Student Data Information Disclosure	University Students	Social Network Communities
Lallmahamood (2007)	Security	Customers	Internet Banking
O'Brien & Torres (2012)	Technology Banking	Facebook Users	Facebook
Youn (2009)	Information Disclosure	Young Adolescents	Web Sites
Tan, Qin, Kim, & Hsu (2012)	Privacy concern User acceptance	Undergrad Business Students	Social Networking Sites

While the contributions of the above studies are significant, there are gaps that emerge which could provide additional insight into privacy issues and concerns of consumers, especially in studies that used social networking sites. With technology related to data collection expanding rapidly (e.g. Near Field Communication, Radio Frequency Identification, and mobile advertising), researchers need to periodically assess how attitudes related to privacy have evolved as individuals get more comfortable and accepting of technology use. Since social media sites are used on various devices such as laptops, tablets, and smart phones, useful information can be gained from users who are considered to be the main demographic (i.e. young adults) and who use social media on a regular basis. This study used the dimensions of behavior, trust, policies, and technology to understand attitudes and concerns towards privacy. Data collected and analysis conducted as a result of this study can be used to validate previous findings and/or provide a pathway for further research as social media sites add new features that may impact individuals' privacy awareness or concerns (such as notification on changes in terms of use policies).

THEORETICAL FOUNDATION & RESEARCH QUESTIONS

This study was based on elements of the framework provided in the Ajzen-Fishbein Theory of Reasoned Action (1980). The TRA theory, which had resulted from attitude research of the Expectancy Value Model, posits that a person's intention to perform a behavior is related to the actual performance of the behavior. Using the theory in the context of this study, an individual who has a positive attitude that a social computing site is protecting his/her privacy would be more intent to use the site over a longer

term. Acceptance behavior can be influenced by several factors such as individual differences (in age, gender, experience), beliefs, attitudes, as well as situational influences (Agarwal, 2000). According to TRA, a person's behavior will be determined by attitude toward the behavior, beliefs about outcomes of behavior, value of these outcomes, social impact of other people, and the person's motivation to adhere to opinion of others. Personal attitude towards a behavior will determine the intent to adopt a given behavior. The construct of attitude and how it affects behavior was the main focus of the study. Deaux and Wrightsman (1988) had further investigated the types of attitude that can impact behavior, and found three components of attitude: (1) the cognitive aspect which affects what an individual consciously thinks and believes; (2) the affective component which includes emotions involved with a product or service (e.g. "I love Facebook"); and (3) the behavioral component which refers to actions that people may have performed in the past. Although the Theory of Reasoned Action provided the primary framework in this study because it engages in the effect of attitudes as antecedents of intension, another dimension of the study was addressed by the Unified Theory of Acceptance and use of Technology (UTAUT) that was also applicable to the factors of privacy concerns in this study. UTAUT provides an extensive review of literature on age, experience, and gender as moderating effects of relationship between a system's expectations and behavior intention (Venkatesh, Morris, Davis, & Davis, 2003). The questionnaire used in this study was developed using variables identified in the Theory of Reasoned Action and Unified Theory of Acceptance and use of Technology.

The following research questions were investigated in this study:

1) What are the attitudes of business students towards privacy when using social computing sites?
2) How do socio-demographic variables (e.g. gender and age) impact attitude toward privacy? How do socio-demographic variables impact knowledge about privacy issues?
3) Is there an association between work experience and longevity of use of social computing sites towards privacy concerns?
4) Can socio-demographic variables predict high versus low knowledge about privacy?

METHOD

This study used attribute independent variables which are often investigated in social sciences and education research. The variables broadly include any predictors, antecedents or presumed causes or influences under investigation in the study. According to Gliner, Morgan, and Leech (2009), attributes of participants, as well as active independent variables, fit within this definition. Quantitative data were gathered through a questionnaire-based survey of business students enrolled at a university in the South East United States. The questionnaire had three parts: Part One was a Likert Scale attitude survey that had sixteen items related to Privacy Behavior, Trust, Policies, and Technology. Table 2 summarizes previous research sources of questionnaire items under each subscale.

Table 2: Sources of questionnaire items

Subscale	Sources
Behavior	Castañeda & Montoro (2007) Hazari, Hargrave & Clenney (2009) Kim, Ferrin, & Rao (2008) Tsai, Egelman, Cranor, & Acquisti (2011)
Trust	Belanger, Hiller, & Smith (2002) Bart, Shankar, Sultan, & Urban (2005) Dwyer, Hiltz, & Passerini (2007) Olivero & Lunt (2004)
Policies	Jensen & Potts (2004) Tsai, Egelman, Cranor, & Acquisti (2011)
Technology	Brown & Muchira (2004) Debatin, Lovejoy, Horn, & Hughes (2009) Fogel & Nehmad (2009) Milne & Culnan (2006) Venkatesh, Morris, Davis, & Davis (2003)

The five-point Likert response scale ranged from "Strongly Disagree" to "Strongly Agree". These items captured preferences related to social computing privacy attitude in the cognitive, affective, and behavioral domain. A Privacy Awareness Score (PAS) was associated with this section of the questionnaire. A high score in this section indicated more awareness and concern towards social computing privacy. It is accepted practice to measure privacy concerns using self-reported scales (Stewart & Segars, 2002; Malhotra, Kim, & Agarwal, 2004). Part Two was a knowledge quiz related to privacy controls where respondents were asked to answer True/False statements that tested their general knowledge about privacy. Appendix A shows questionnaire items of Part One and Two along with identification of items under each of the four subscales that were used in the survey. Part Three asked for demographic information. Prior to administration of the survey, it was pilot tested with a group of respondents that included faculty and students (not counted in the actual sample). Feedback from the group was incorporated in the final version of the survey that was given to 157 respondents included in this study. Content validity of survey items was established by two faculty members in the Information Systems and Marketing departments in the College of Business. As shown in Table 3, most respondents in this study ranged from 18-25 years which is typical of the social computing demographic

Table 3 Socio-demographic characteristics of the sample (n= 157)

Measure	Items	Frequency	Percent
Gender	Male	73	46.5
	Female	84	53.5
Age	18-21 yr	71	45.2
	22-25 yr	58	36.9
	26-30 yr	9	5.7
	> 30 yr	19	12.1
Employment	Not Employed	56	35.7
	Part-time	76	48.4
	Full-time	25	15.9
Social Media Sites Most Used	Facebook	111	70.7
	Twitter	39	24.8
	LinkedIn	2	1.3
	Pinterest	5	3.2
Social Media Sites Used how long?	< 1 yr	10	6.4
	1-2 yr	25	15.9
	> 2 yr	122	77.7
Social Media Sites How most accessed?	Smartphone	84	53.5
	Laptop	62	39.5
	Desktop	10	6.4
	Tablet	01	0.6

RESULTS

The instrument assessed individuals' attitudes toward privacy along four hypothesized subscales. Reliability of the instrument was calculated before proceeding with data analysis. Cronbach alpha, which is the measure of internal consistency (or Reliability), was calculated for the scale and was found to be 0.69. Nunnally (1978) and Thorndike (1996) have stated that overall Cronbach alpha of 0.70 is considered acceptable criterion for internally consistent scales. Although the reliability of the overall scale was acceptable, two subscales exhibited lower coefficient of reliability (possibly due to the small number of items in the subscales). Due to this limitation, additional individual analysis specific to subscales was not conducted and all questions were treated as unidimensional. Further research can look into modifying the items in the individual subscales to improve reliability of individual subscales.

Descriptive data analysis was conducted on attribute variables. A multi-variate analysis of variance (MANOVA) was used to examine Privacy Awareness and

Knowledge Score as the dependent variables with gender, age, and employment status as independent variables. A one-way MANOVA was calculated examining effect of gender on privacy awareness score and knowledge score. No significant effect was found (Lambda (2,154) = .993, $p > .05$). Neither the privacy awareness score nor knowledge score were significantly influenced by gender. A one-way MANOVA was calculated examining effect of age on privacy awareness score and knowledge score. No significant effect was found (Lambda (6,304) = .926, $p > .05$). Neither the privacy awareness score nor knowledge score were significantly influenced by age. A one-way MANOVA was calculated examining effect of employment status (not employed, employed full-time, employed part-time) on privacy awareness score and knowledge score. A significant effect was found (Lambda (6,304) =.931, $p < .05$). Follow-up univariate ANOVA indicated that Privacy Awareness score was not significantly influenced by employment status ($F(2,154) = .949$, $p > .05$). Knowledge scores, however were significantly influenced by employment status ($F(2,154) = 3.673$, $p < .01$).

An independent-samples t test was calculated comparing the mean Privacy Awareness scores of males and females. No significant difference was found ($t(155) = .223$, $p > .05$). The mean score of males ($m = 59.38$, $sd = 8.224$) was not significantly different from the mean score of females ($m = 59.13$, $sd = 5.886$). An independent-samples t test was calculated comparing the mean knowledge (percent) scores of males and females. No significant difference was found ($t(155) = .894$, $p > .05$). The mean of males ($m = 67.71$, $sd = 20.07$) was not significantly different from the mean score of females ($m = 64.80$, $sd = 20.62$).

A Pearson correlation coefficient was calculated to investigate the relationship between users' privacy awareness and knowledge score. A weak negative correlation that was significant was found ($r(157) = -.257$, $p < .001$) between the two variables. A linear regression was calculated to predict a users' knowledge score based on their privacy awareness score. A significant regression equation was found ($F(1,155) = 10.968$, $p < .001$), with an R2 of .066. Users' predicted knowledge score is equal to 110.135 - 0.742 * (Privacy Awareness Score).

The average Privacy Awareness score and average Knowledge score (percentage of items correctly answered) of users under each group is shown below in Table 4.

Table 4 Privacy Awareness and Knowledge scores

Measure	Items	Knowledge Score (Percent)	Privacy Awareness Score
Gender	Male	67.71	59.38
	Female	64.80	59.13
Age	18-21 yr	62.57	59.06
	22-25 yr	65.27	59.41
	26-30 yr	76.19	60.00
	> 30 yr	77.44	59.11
Employment	Not Employed	65.05	58.30
	Part-time	63.72	59.54
	Full-time	76.00	60.48

Spearman correlation was used to examine the relationship between age groups and associated privacy awareness scores. A weak correlation that was not significant was found ($r_s(155) = .036$, $p > .05$). For the age group and knowledge score, a weak correlation that was significant was found ($r_s(155) = .220$, $p < .05$). Although the Privacy Awareness Score across all age groups were similar, the older age groups exhibited a higher knowledge score.

One-way ANOVA was computed comparing the knowledge scores of users under different age groups. A significant difference in knowledge scores was found among the age groups ($F(3,153) = 3.621$, $p < .05$). Tukey's HSD was used to determine the nature of the differences between the age groups. This analysis revealed that only users who were >30 years scored significantly higher than users 18-21 years. The 22-25 and 26-30 year groups were not significantly different from either of the other two groups.

As previously mentioned, user awareness about privacy may result in better informed decisions when surfing the web and using social media sites. To test this hypothesis, a seven-item knowledge quiz related to privacy controls was given to

respondents who were asked to answer True/False statements that tested their general knowledge about privacy issues. Cluster analysis (Kaufman & Rousseeuw, 2009) helped determine the difference between knowledge levels of respondents and form cluster groups based on knowledge results. Using a Hierarchical Cluster Analysis of finding two clusters by using the nearest neighbor method, it was found for a two cluster group, the "low knowledge" group cluster consisted of 30 respondents with a mean score of 2.47 (35.28%) and a "high knowledge" group of 127 respondents with a mean score of 5.14 (73.43%). Logistic regression (Field, 2009) was conducted to assess whether the predictor variables of gender, age, and employment status could predict whether a respondent could be placed in a low or high knowledge group. When all three predictor variables were considered together, they were not able to significantly predict high or low knowledge group membership (χ^2=1.952, df=3, N=157, p >.05).

LIMITATIONS

This study has some limitations associated with the nature of the study and the general topic of privacy. The questionnaire included items that could have self-reported answers which may be consistent with tendencies of socially desirable answering patters (such as negative aspects associated with sharing of passwords and creating accounts under fictitious names). By filling out the questionnaire for this study, some respondents may have thought more about privacy issues that they take for granted when interacting on social computing sites. Respondents may have read news items or blogs related to privacy and security breaches and may have responded to general beliefs related to privacy on the Internet (i.e. subjective norm as defined in Ajzen-Fishbein theory of reasoned action). The Privacy Awareness Scale in this study was considered to be unidimensional. Future studies could try to isolate individual dimensions that may emerge from the scale for additional insight and development of a multidimensional privacy awareness scale (which currently does not exist). The survey respondents were located at a single institution. However, multiple sections of different classes were used to collect data thereby providing a slightly more diverse sample. Not all individual subscales of the questionnaire exhibited high internal consistency so the questionnaire items were analyzed not based on subscales, but as a holistic representation of privacy issues. It is assumed that the privacy awareness metric used in this study is an accurate reflection of privacy concerns of individuals who took part in this study.

DISCUSSION

Individuals form attitudes and beliefs as a result of experiences they may have had in the past. An individual who believes their privacy has been compromised on social computing websites would be more cautious when sharing personal information on social networking sites. Conversely, Joinson et. al. (2010) found that people may be inclined to relinquish privacy concerns when dealing with a trusted organization or website. Given that the majority (77.7%) of our sample consists of individual who

have used social media sites for more than two years, it is possible that they have grown to accept limitations of these sites in terms of issues regarding their privacy or compromise of personal information. Junglas (2006) investigated demographic variables including personality traits in perceptions of privacy and found these related to usefulness, risk, and trust to explain behavioral intentions that affect privacy. There was a significant correlation between privacy awareness scores and knowledge scores which were the two dependent measures in this study. Use of multiple measures provided a better understanding towards privacy issues as a relationship could be established between what an individual knows about privacy and his/her attitudes towards privacy issues. This study found that gender differences did not have an effect on privacy awareness and knowledge about privacy issues. This is consistent with findings of Nowak and Phelps (1992) who reported that concerns about personal privacy did not vary between men and women, and there are no differences in actions men and women take to protect their privacy in a direct marketing context. This study also found for the sample under study, age did not have an effect on privacy awareness and knowledge about privacy issues. Hoofnagle, King, Li, and Turow (2010) had similarly found that no significant differences towards online privacy exists between younger and older adults. The employment status of respondents did show a significant effect on privacy awareness and knowledge scores. This may have been due to exposure related to information awareness training programs in formal settings where employees are made aware of acceptable use policies in work place settings and where they may have had to agree to these policies. Moreover, it is possible that those who are working are more conscious of the potential implications that certain information on social media sites could have negative consequences in the workplace; therefore, the need to fully understand the sites' privacy policies could be more important for those who are employed.

CONCLUSION

Given the global adoption of social media sites as documented in this study, the relevancy of the subject can be considered to be important and popular for scholarly and professional attention. Despite the concerns about privacy on social computing sites, social media continues to thrive as evidenced by the number of users joining social networks. According to Gross and Acquisti (2005), the rapid increase in participation on social media sites has been accompanied by a progressive diversification and sophistication of purposes and usage patterns across a multitude of different sites. For this trend to continue, site owners, advertisers, and marketers must make their users comfortable in sharing personal information. There needs to be a level of trust established that information gathered about an individual will not be used in violation of the privacy policy. Perception of violation of trust may impact willingness to share data, which in turn may affect targeted advertising to individuals. This research has implications for individuals, businesses, regulators, and business schools who teach students about issues privacy and social networking.

Milne, Rohm, and Bahl (2004) found that an individual's concern for privacy is a strong predictor of safe online behavior. Although there is legislation that protects

privacy to a certain extent, what is missing is baseline consumer privacy legislation that protects all users. Attitudes toward privacy can impact use of social computing sites. Owners of social computing sites should take an active role in being transparent about their privacy policies and how collected data will be used. This would influence continued use of the site by visitors, especially where personal information and credit card data is exchanged between users, vendors, and third party apps. Users must be made to believe that social computing sites have the highest regard for security and privacy similar in comparison to sites such as ecommerce and banking. This would encourage frequent visits, more interaction, and clicking of ads, which are essential to the revenue stream of social computing sites. For users to feel comfortable when giving up their information over social networks, and be confident that their privacy rights are protected, there is a strong need for further research on privacy issues in the legal, economical, ethical, social and technical disciplines. Future research can look at identifying antecedents towards privacy related behavior on social computing sites. Other research can also study relationships between information privacy and related constructs of how companies can establish social trust, and community building that can mutually benefit both the consumers as well as the company's brand.

This study investigated privacy issues related to social computing use. The demographics of the sample can be considered representative of typical users of social media sites, which are young adults regularly accessing sites such as Facebook from their smartphones (Brenner, 2013). Further research can investigate additional demographic differences based on cultural or ethnic background. With advertisers facing stiff challenges from competing brands who are using aggressive marketing to attract customers, privacy of social computing has become more important because of issues such as credit card scams and identity theft. The quest for gathering phone numbers, email addresses and other personal data for better target marketing has led to unscrupulous practices such as ignoring the privacy flag set in browsers. Belanger and Crossler (2011) have identified opportunities for technical solutions to address privacy concerns. The next generation of social media apps, products, and web services need to have more transparent privacy policies so users can be better informed on how the data collected during interaction with the service will be used. A business needs to be trusted and valued by users for sustained interaction. The results of this study show that individuals are concerned about their privacy, and would like to control their digital reputation as it can directly impact long term business relationships or employment prospects. From an educational perspective, there needs to be more awareness training provided by institutions to make students aware of privacy issues when dealing with social computing sites. This can reinforce behavior that contributes to maintaining privacy and security in personal lives as well as in the workplace. The rights of business versus rights of the consumer are in conflict; there must be a balance between the two. Until that happens, individuals will have to take responsibility to safeguard their online behavior.

REFERENCES

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE Security & Privacy, 3(1), 26-33.

Agarwal, R. (2000). Individual acceptance of information technologies. In R. W. Zmud (Ed.), Framing the domains of IT management: Projecting the future through the past, 85-104. Pinnaflex: Cincinnati, OH,

Alsop, R. (2008). The trophy kids grow up: How the millennial generation is shaking up the workplace. NJ: Jossey-Bass.

Ajzen, I. & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. Psychological Bulletin, 84, 888-918.

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall.

Bagozzi, R. P., & Burnkrant, R. E. (1979). Attitude organization and attitude-behavior relationship. Journal of Personality and Social Psychology, 37, 913-929.

Barnes, S. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9).

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. Journal of Marketing, 133-152.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. The Journal of Strategic Information Systems, 11(3), 245-270.

Belanger, F. & Crossler, R. E. 2011 (2011). Privacy in the digital age: A review of information privacy research in information systems MIS Quarterly, 35(4), 1017-1041.

Bessen, J. (1993). Riding the marketing information wave. Harvard Business Review, 71(5), 150-160.

Brenner, J. (2013, February 14). Pew Internet: Social Networking. Retrieved from http://pewinternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx

Brown, M. R., & Muchira, R. (2004). Investigating the relationship between internet privacy concerns and online purchase behavior. Journal of Electronic Commerce Research, 5(1), 62-70.

Castañeda, J. A., & Montoro, F. J. (2007). The effect of Internet general privacy concern on customer behavior. Electronic Commerce Research, 7(2), 117-141.

Chaney, P. (2009). The digital handshake: Seven proven strategies to grow you business using social media. New Jersey: John Wiley & Son.

Chen, K. & Rea, Jr., A. I. (2004). Protecting personal information online: A survey of user privacy concerns and control techniques. The Journal of Computer Information Systems, 44(4), 85-92.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational

privacy: Lessons from the ChoicePoint and TJX data breaches. MIS Quarterly, 33(4), 673-687.

Deaux, K., & Wrightsman, L. (1988). Social psychology. Pacific Grove, CA: Brooks/Cole.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication, 15(1), 83-108.

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007, August). Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. In AMCIS (p. 339).

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. Journal of Business Research, 59(8), 877-886.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. Computers in Human Behavior, 25(1), 153-160.

Field, A. (2009). Discovering statistics using SPSS. CA: Sage Publications.

Foster, T. N., & Greene, C. R. (2012). Legal issues of online social networks and the workplace. Journal of Business & Ethics, 18, 131.

Gliner, J. A., Morgan, G. A., Leech, N. L. (2009). Research methods in applied settings: An integrated approach to design and analysis (2nd ed.). New York, NY: Routledge.

Gonzalez, V. E. (1992). On human attitudes: Root metaphors in theoretical conceptions. Goteborg, Sweden: Vasastadens Bokbinderi AB.

Graeff, T. R., & Harmon, S. (2002), Collecting and using personal data: consumers' awareness and concerns, Journal of Consumer Marketing, 19(4), 302-318.

Gross, R., & Acquisti, A. (2005, November). Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society (pp. 71-80). ACM.

Hazari, S., Hargrave, W., & Clenney, B. (2009). An Empirical Investigation of Factors Influencing Information Security Behavior. Journal of Information Privacy and Security, 4(4), 3-20.

Holzner, S. (2008). Facebook marketing: Leverage social media to grow your business. New York: Que Publishing.

Hoofnagle, C., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies?.Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864

Jensen, C., & Potts, C. (2004, April). Privacy policies as decision-making tools: an evaluation of online privacy notices. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 471-478). ACM.

Joinson, A. N., Reips, U., Buchanan, T., & Schofield, C. (2010). Privacy, Trust, and Self-Disclosure Online. Human-Computer Interaction, 25, 1-24.

Junglas, I. (2006). Personality traits and privacy perceptions: An empirical study in the context of location-based services. Proceedings of the International

Conference on Mobile Business, p. 36. doi: 10.1109/ICMB.2006.40

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision support systems, 44(2), 544-564.

Kaufman, L., & Rousseeuw, P. J. (2009). Finding groups in data: An introduction to cluster analysis. NJ: Wiley.

Lallmahamood, M. (2007). An examination of individual's perceived security and privacy of the Internet in Malaysia and the influence of this on their intention to use e-commerce: Using an extension of the Technology Acceptance Model. Journal of Internet Banking and Commerce, 12(3), 1-25.

Li, T., Greenberg, B. A., & Nicholls, J. A. F. (2007). Teaching experiential learning: Adoption of an innovative course in an MBA marketing curriculum. Journal of Marketing Education, 29(1), 25-33.

Mackay, W. E. (1991, March). Triggers and barriers to customizing software. In Proceedings of the SIGCHI conference on Human factors in computing systems: Reaching through technology (pp. 153-160). ACM.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, 15(4), 336-355.

Mckeon, M. (2010). The evolution of privacy on Facebook. Retrieved from http://www.mattmckeon.com/facebook-privacy/

Melone, N. P. (1990). A theoretical assessment of the user-satisfaction construct in information systems research. Management Science, 36(1), 76-91.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. (1995). Values, personal information privacy, and regulatory approaches. Communications of the ACM, 38(12), 65-74.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. Organization Science, 11(1), 35-57.

Milne, G. R., Rohm, A. J., Bahl, S. (2004). Consumers' protection of online privacy and identity. Journal of Consumer Affairs, 38(2), 217-232.

Milne, G. R., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. Journal of Public Policy & Marketing, 238-249.

Nowak, G. J. & Phelps, J. (1992). Understanding privacy concerns: As assessment of consumers' information related knowledge and beliefs. Journal of Direct Marketing, 6(4), 28-39.

Nunnally, J. C. (1978). Psychometric theory. New York: McGraw-Hill.

O'Brien, D, and Torres, A. (2012). Social networking and online privacy: Facebook users' perceptions. Irish Journal of Management, 16(14), 63-97.

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. Journal of Economic Psychology, 25(2), 243-262.

Opsahl, K. (2010, April 28). Facebook's eroding privacy policy: A timeline. Retrieved from https://www.eff.org/deeplinks/2010/04/facebook-timeline

Patterson, A. (2012). Social-networkers of the world, unite and take over: A meta-introspective perspective on the Facebook brand. Journal of Business Research, 65(4), 527-534.

Pavlou, P. A. (2011). State of information privacy literature: Where are we now and where should we go? MIS Quarterly, 35(4), 977-988.

Purcell, K., Brenner, J. & Rainie, L. (2012, March 9). Search engine use 2012. Retrieved from http://pewinternet.org/Reports/2012/Search-Engine-Use-2012.aspx

Rinaldo, S. B., Tapp, S., & Laverie, D. A. (2011). Learning by Tweeting using Twitter as a pedagogical tool. Journal of Marketing Education, 33(2), 193-203.

Sengupta, S. (2011, November 29). FTC settles privacy issue at Facebook. The New York Times. Retrieved from http://www.nytimes.com

Sheehan, K. B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. Journal of Interactive Marketing, 13(4), 24-38.

Shilton, K. (2009). Four billion little brothers? Privacy, mobile phones, and ubiquitous data collection. Communications of the ACM, 52(11), 48-53.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An interdisciplinary review. MIS Quarterly, 35(4), 989-1015.

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

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

Tan, X, Qin, L, Kim, Y, and Hsu, J. (2012). Impact of privacy concern in social networking web sites. Internet Research, 22(2), 211-233.

Thorndike, R.M. (1996). Measurement and evaluation in psychology and education (6th ed.). Upper Saddle River, NJ: Prentice Hall.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. Information Systems Research, 22(2), 254-268.

Varian, H. R. (2006). Economic aspects of personal privacy. Retrieved from http://people.ischool.berkeley.edu/~hal/Papers/privacy

Wang, Y., Burgener, D., Kuzmanovic, A., & Maciá-Fernández, G. (2011, June). Understanding the network and user-targeting properties of web advertising networks. In Distributed Computing Systems (ICDCS), 2011 31st International Conference on (pp. 613-622). IEEE.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. The Journal of Consumer Affairs, 43(3), 389-418.

AUTHOR BIOGRAPHY

Dr. Sunil Hazari is Associate Professor in the Department of Marketing & Business Education at the Richards College of Business, University of West Georgia. His teaching and research interests are in the areas of Social Media Collaboration & Communication, Information Security, Web Usability, and Organizational aspects of e-Learning. He has authored several peer-reviewed journal publications in Information and Instructional Technology areas, and has presented papers at national conferences. He serves on editorial board member of several journals. Further information is available from http://www.sunilhazari.com/education

Cheryl O'Meara Brown is Senior Lecturer in the Department of Marketing at the Richards College of Business, University of West Georgia. Her teaching and research interests are in Marketing Research and Digital Marketing. She has served as a consultant to several organizations.