Data Privacy: Are We Accidentally Sharing Too Much Information?

Adnan A. Chawdhry
chawdhry_a@calu.edu
California University of Pennsylvania
California, PA

Karen Paullet
paullet@rmu.edu

David M. Douglas
douglas@rmu.edu

Robert Morris University
Moon Township, PA

Abstract

We are living in a world in which we are surrounded by technology. With the conveniences of technology also come nuisances. People are exposing personally identifiable information (PII) about themselves without realizing the consequences of this action. Many users of social network sites are aware of the possible pitfalls of failing to secure their personally identifiable information using the privacy settings of the site. However, what about the personally identifiable information placed in the photos that individuals place online? What about accidentally sharing information by clicking "reply all" to an email that was meant for only one recipient or attaching the wrong document in an email? With the increased deployment of electronic devices that connect us around the world, we often unintentionally share personal information with those we do not know or whom we did not intend to disclose the private details. The oversharing of information, how it is collected, and who collects it can be a source of power. As users of these communication channels, we need to be aware of how information can be accidentally shared with those we did not intend and the negative effects it can have on the user. To the best of the researcher's knowledge, this is the first attempt to measure accidental sharing of information via mobile devices, email, public Wi-Fi and text messaging. This 2013 exploratory study investigates how students at a mid-Atlantic University willingly and unwillingly share personal information and the potential effect this sharing has on their digital lives.

Keywords: Privacy, Information Technology, Social Networking, Email, Texting

1. INTRODUCTION

Society has found new ways to communicate and share information, which has allowed civilization to develop and society to grow and prosper. Over the masses of humanity, the retention of information has been the source of collective control. As we connect to the world with mobile and stationary electronic devices through social networking sites, we share information.

©2013 EDSIG (Education Special Interest Group of the AITP)

We have all heard information is power. Today, even the most trivial piece of personal information is worth money to someone. In 2012, several break-ins occurred in the Portland, Oregon area. The burglar retrieved information from the victims personal profile status. The homeowners simply posted their vacation status on a social networking site, which then triggered the series of events (Hanrahan and Cook, 2012). More often than not, we are unaware whom we are sharing our information with or which entity collects our digital data. Much can be gained from the bits and pieces of information that are accidentally shared using today's communication channels.

Accidentally sharing information can easily be used to damage a person's reputation or steal a lifetimes worth of savings. For the purposes of this study, accidental is defined as "happening without intent or through carelessness and often with unfortunate results" (Mish, & et al. 1983, p. 49).

How often do we accidentally share information each day? Do we click send on an email message only to regret it a second later? Or do we unwittingly agree to terms and conditions of a mobile phone application (App) only to feel distress a moment later especially when we find out what we agreed to in our haste in order to have the "latest and greatest application at our fingertips.

Indeed, the results of our haste and impulses can beget unintended consequences that reach far out into the future of our digital dossiers. Regardless of the consequences that may result from the accidental sharing of our digital lives, cyberspace does not delete, forgive, or forget.

2. LITERATURE REVIEW

With more than 100 million Americans who use smart phones, privacy and unintentional sharing of information is a concern. Smart phones not only connect to the Internet, but can also be used to pay for goods and services, check personal finances, and act as an electronic boarding pass at transportation terminals. Additionally, we routinely send and accept text messages and photos from our smart phones. However, we seldom consider that our connectivity just might be jeopardizing our privacy. For instance, Apple and Google have the ability to track users activities based on a person's phone location and unique identification (CR Investigates, 2013). Smartphones have become a convenience for end users. We are able to complete our banking, make travel arrangements or even purchase a pair of shoes with the click of a button. As we take advantage of the technologies, end users must be aware of the privacy and security risks associated with such behavior. For example, when banking, do we know if we are connecting to a secure network or are we connecting to public Wi-Fi?

As mentioned by Makesjki, et.al. (2011), studies have found that users have a difficult time completing basic access control management tasks, including determining who has access to which resources such as social media and email, and making changes to an existing policy (Reeder, R.W., 2008; Lipfort, H.R., et.al, 2008; Madden and Smith. 2010). File sharing mechanisms tend to be so difficult to use that many users prefer to share documents as email attachments. As people share attachments comes the risk of attaching the wrong document or sending the information to the incorrect recipient.

Personally Identifiable Information (PII), as defined by Johnson (2005) is "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." Krishnamurthy & Willis (2009) analyzed PII leakage via online social network sites such as Facebook, LinkedIn, Twitter, and Xanga. When filling out social network profiles users include their first and last name, location (city), zip code, street address, email address, telephone numbers, and photos. Other pieces of information included in profiles which can be linked directly to the user are gender, birthday, age, schools, employer(s), friends and activities. Their study revealed that it is possible for third parties to link PII, which is leaked via social network sites, with user's actions both within the site and elsewhere to include third party applications and tracking cookies.

Applications, also known as "Apps," also raise concerns for privacy and the unintentional sharing of information. It has been estimated that there are over one million apps available for

smart phones. Since many of these apps are free or low-cost, they are tempting to install on your device with little or no afterthought (CR Investigates, 2013). When downloading free apps end users are not always aware that by doing so they are permitting third parties to access their personal information. Individuals can take simple steps to protect personal data that require little effort or time. "On average, Americans spend 127 minutes a day on their smartphones, using 41 apps. There are more than 1 million apps available. An app displays its permissions—the information it will access—the millisecond prior to download. Do you, like everyone else, glance down and hit the button" (Silmore, 2013, p. 28)? First, make sure you install apps with caution and use reputable sources such as Google Play or Amazon Appstore. Second, beware of unsecured Wi-Fi networks. Open Wi-Fi networks can easily be intercepted. Third, watch out for text spam. Text spam can contain links to websites that automatically download malicious software to your phone. Fourth, disable or turn off location tracking. Turn it on only when needed, for instance when in need of directions. Fifth, when recycling or selling an older phone remember to remove memory cards, restore factory settings, and delete all sensitive data (CR Investigates, 2013).

Digital dossiers set the person apart from the masses and confirm a person's individual passions and proclivities. These in turn could be used by the state to predict a person's future behavior (good or evil) and by businesses to determine individual spending habits (Vaidhyanathan, 2008). Automatic identification and data collection (AIDC) systems are changing the world and altering how the concept of privacy is being interpreted by businesses, governments, and people.

Pinchot and Paullet (2012) conducted a study of 146 college students to determine if Facebook profile data has a direct link to personal security questions. The study revealed that 63% of students share their date of birth and 76% reveal their hometowns in their profile settings. Together, these two pieces of information could be used to determine a person's social security number (Debtain, et.al, 2009). On its own, hometown could be used as an educated guess to answer a popular personal security question such as "In what city were you born?" In the study, 21% of females reported that they share their maiden name on Facebook in order for past acquaintances to be able to recognize their profile. Additionally, 85% of respondents indicated that they share the name of their high school in their profile. Another related security question that can be linked to a person's profile is "What was your high school mascot?" which can be easily determined from this information.

A Carnegie Mellon University (CMU) study conducted by Gross and Acquisit (2006) surveyed over 4000 students in regards to privacy on Facebook. The researchers searched all CMU Facebook members using the website's advanced search feature to extract their profile IDs. Their findings revealed that 90% of profiles contained an image, 88% of users provided their date of birth, 40% listed their phone numbers to include cell phone numbers, and 50% listed their current residence. It must be mentioned that Facebook profiles can be fully identifiable by participants providing their first and last names in their profile. To evaluate whether or not students provided a real name and date of birth the researchers analyzed a subset of 100 profiles randomly accessed from the initial 4000 students for accuracy. Facebook users in 89% of the profiles analyzed used their real first and last name and 98% provide their actual date of birth to include the month, day and year even though they are not required to do so. Facebook only requires a first name and the month and year of birth. Very few users chose to limit access to their profile to just friends.

Paullet and Pinchot (2012) conducted a study in regard to the oversharing of information on social networks. The study revealed that participants reveal information that can map directly back to the answers of security authentication questions that they set up for personal accounts. For instance, 41% of participants provided the name of the street they grew up on in their profiles, 44% provided their childhood place of birth, 32% provided the name of their favorite sports team, 46% provided the name of their favorite pet and 60% provided their mother's maiden name. If one looks at some of the security questions used to set up a new account and compare them to information people reveal in their photos or profiles, one will be able to find the answers to many of the security questions by looking at the photos posted.

3. RESEARCH METHODOLOGY

With the advent of newer technologies and social networking sites throughout the world, individuals are finding more convenient ways of completing tasks and sharing information. However, these conveniences provide a need for data privacy awareness so that individuals understand the benefits and risks of using these technologies and websites. The purpose of this study was to determine personal characteristics and social networking site affiliations that affect individuals sharing private details. The study explores the following two research questions:

> RQ1: What are common scenarios where individual's accidentally overshare information?
>
> RQ2: How could users modify their online behavior to protect against accidentally oversharing information?

The study examined students at a small mid-Atlantic University during the period of February 2013 through April 2013. The research utilized a quantitative methodology to assess the students' awareness and desire to modify their behavior. The population chosen for this study was comprised of undergraduate and graduate students enrolled in on-campus and online programs of study. Undergraduate students and graduate students were surveyed in order to gather data from students 18 years of age and older. A total of 138 respondents completed the survey. The survey was designed to obtain information on the respondents' affiliations with various social networking sites in addition to providing scenarios to assess if the respondents shared private information. The survey was conducted using Survey Monkey, an online tool, to gather and organize data. The data was imported into SPSS for further analysis. This study used Chi-square with a statistical significance at the .05 margin of error with a 95% confidence level to determine students' awareness and willingness to modify behavior. The study was a convenience sample surveying students from all departments within the university which included the School of Arts and Humanities, Business, Science and Math, Engineering, Computer Science, Information Technology, Criminal Justice and Psychology.

The survey instrument consisted of 28 closed-ended questions and one open ended question for further understanding of participant comments and responses. The first four questions focused on student demographics; which included gender, age, education, and degree program. Questions 5 through 18 asked students if they were aware of the capabilities associated with mobile devices, GPS linked photos from cameras or cell phones, and RFID. They were then asked a follow up question in regard to their willingness to change their behavior based upon 5 choices (Very Likely, Somewhat likely, Neutral, Somewhat Unlikely, Not Likely). The next 10 questions discussed a student's understanding of privacy risks associated with using technology. Students were provided with three scenarios to help answer the questions. The final question asked the students about their willingness to change their behavior after completing their survey and, if so, how they are planning to modify their behavior.

4. RESULTS

The survey responses were analyzed according to how respondents accidentally overshare information. Of the respondents, it was determined that 90.30% were members of some social networking site that included Facebook, Twitter, YouTube, Foursquare, LinkedIn, and Google+. The respondents ranged in age from 18 – 62 years old. Approximately 64% of the sample that responded they were members of a social networking site falls between the ages of 19-22. A further breakdown of age versus their response to being a member of a social networking site can be seen in the Appendix Table 1.

Each of the participants who responded "Yes" to having a membership to a social networking site were also asked to choose their membership from a list of predefined social networking sites to include Facebook, Twitter, YouTube, Foursquare, LinkedIn, and Google+. Facebook, Twitter, and YouTube were used by over 50% of the participants with Facebook being the most widely used social networking site. Additionally, Google+ and LinkedIn had a strong presence among 19 to 23 year olds. A little over 29% of respondents belong to LinkedIn and 22% are members of Google+. Additional details of this analysis can be found in Table 2 of the Appendix.

Respondents' age was used in evaluating several variables. Specifically when using social networking sites was compared to the general age of the respondents to determine any

correlation. When comparing age to the respondents' social networking site association, the analysis produced a chi-square value of 42.157 with 44 degrees of freedom and a statistical significance value of .551. This value was well beyond the threshold of .05 and therefore no statistical significance was present within these two variables. Social networking usage was then evaluated which showed a chi-squared value ranging from 12.895 to 43.313 with 22 degrees of freedom. Facebook and Twitter both produced statistically significant data of .005 and .004, respectively, in the categories of social networking and age. The remaining choices of social networking members showed no statistical significance. Additional details of this analysis can be found in the Appendix Table 3.

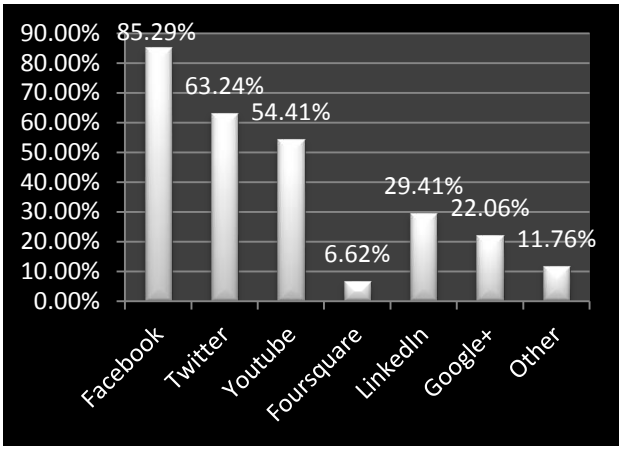

Figure 1: Bar chart of social networking sites

The researchers asked a series of 10 questions/statements that proposed different scenarios of accidental oversharing. These questions were:

- When replying to an email, I have hit "Reply All" to an email that was intended for one recipient and shared information I should not have.
- When attaching a document, photo, or other file to an email, I have sent the incorrect attachment to an email and shared information I should not have.
- When sending or replying to a SMS message (text message), I have sent personal information to the wrong person.
- When sending or replying to a MMS message (multimedia message), I have sent the incorrect attachment and shard information I should not have.
- I have posted a private message on a public wall on a social media site.
- I have posted information about my friends and families that do not want to participate in social networking?
- When filling out online forms (e.g. to sign up for an account) I provide more information that is necessary?
- When filling out online forms, I provide accurate information in the profile?
- I take the time to read the terms of service agreements on (social networking sites, online purchases, etc.) before accepting?
- I connect to publicly available Wi-Fi and transmit personal information such as my name, user names, and passwords while checking my bank account, email or updating my social media status.

In most cases, the majority of respondents claimed they did not accidentally overshare information. Sharing private information over a public Wi-Fi was one of the scenarios where the majority of the respondents, approximately 54%, claimed they have or currently share information. Additionally, 76.3% of the respondents stated that they provided accurate information when completing forms. Of the respondents, 40% stated that they shared private information over an SMS text to the wrong person. Each of the remaining scenarios resulted in less than 30% of respondents stating they accidentally shared too much information. The remaining responses in order of highest accidental information sharing to lowest includes reading the terms of service agreement, providing accurate information online, posting information about one's family or friends, accidentally hitting "Reply to All," posting more information than necessary, incorrect email attachment, incorrect MMS attachment, and posting private messages on a social networking page. A detailed breakdown of these results can be found in the Appendix Table 4.

Additionally, the researchers compared four variables (Age, Gender, Education Level, and Program of Study) with the 10 scenarios of accidentally sharing information in order to determine any statistical significance. Age produced chi-square values ranging from 40% (Attachment) to 78% (Accurate Information). Additionally, a statistical probability beyond the .005 threshold was calculated to illustrate

statistical significance. This value was calculated and ranged from 0.00, or 0.00%, to 0.64. In relation to age, providing accurate information online (0.00%), providing details about a family or friend online (5%), or accidentally sending an MMS to the wrong person (3%) were considered statistically significance. All of the other scenarios were outside of the 5% margin of error and 95% confidence interval. Gender had chi-square values from 139.67 to 143.82. All of the accidental information sharing scenarios illustrated statistical significance with gender having a value of 0.00%. The chi-square value of Education level ranged from 141.10 to 158.34. Similar to Gender, all of the accidental information sharing scenarios calculated a statistical significance with Education Level having a value of 0.00%. Lastly, the Program of Study had chi-square values of 146.13 to 158.46. Each of the accidental sharing information scenarios yielded values of 0.00% showing a statistical significance with Program of Study. Further analysis of these values can be seen in the Appendix Table 5.

The final question asked if the participants would change their online behavior based on what they read in survey. Approximately 44.44% responded that they would change their behavior while 55.56% stated they would not modify their behavior. Those who responded yes to this question were also asked a follow up open-ended question to further clarify how they would modify their online behavior. As expected, respondents answering in the affirmative became more cautious and proactive of their online activity by not sharing as much information as they have in the past.

A summary of these responses include:

1. Reconsider submitting personal information when connected to public Wi-Fi.
2. No longer posting personal information on social networking sites.
3. No longer using social networking sites.
4. Will be more aware and cautious of their online activity.
5. More careful about what information is posted / given out over the Internet.
6. More careful about where personal data is accessed.
7. More careful about posting pictures on social networking sites.
8. Reduce any unessential activity using social networking sites.

5. DISCUSSION

To the best of the researcher's knowledge, limited research has been done on the accidental oversharing information. Periodically, news headlines appear surrounding the negative outcome of posting information on social networking sites such as, posting your vacation adventures only to find that their home was burglarized or losing a job due to posting an inappropriate comment. Something so simple and innocent can lead to negative consequences for people. Yet, many are constantly connected and are actively posting on social media sites like Facebook, Twitter, and YouTube, which were the most common social networking sites from this study. In an effort to keep people informed, people opt to include their names or specifically tag them in a picture or a post. People might say what harm can a picture really do, but let's not forget the old adage "that a picture is worth a 1,000 words". From a picture we can gather a person's geographic location, whom they were with, and even the time the photo was taken. Examining the meta-data within the photo can provide private details to anyone connected to the site, including those with objectionable intentions.

It is extremely easy to hit "reply to all" on an email or accidentally send an SMS or MMS to the wrong person. Call it simple carelessness, being preoccupied; keeping in mind that sensitive information could be passed into the wrong hands. This study determined that approximately 18% to 40% of the participants shared information that they did not intend to via email, SMS, or MMS. Essentially 1 out of every 5 people accidentally overshares information. For the researchers, these numbers were significant enough to be concerned. Think about the damage that can be done by accidentally sending a message to wrong recipient. Regardless of the negative effects that might arise, the sender can never take it back. It is out there, traveling over the Internet and seen by the recipient.

Sometimes users do not realize that providing too much information, even when intentionally posting information, can have the same negative effects. For example, sites like Facebook attempt to have their subscribers complete their profiles by entering background information like

education details, birthdays, anniversaries, phone numbers, etc. How often do you see these responses being answers to "security questions" that help reset personal accounts? How much sharing can be considered over sharing? This study concluded that on average 1 out of 5 people shared too much information online. This comes to 20% of the population who use technology. The question remains, how much of this information could affect the user or an unintended victim?

Connectivity to public Wi-Fi networks has become easier. Free Wi-Fi is a factor in attracting customers to restaurants and coffee shops. It also saves money for consumers with limits to their data plans. Most, if not all, mobile devices allow the user to select if they want their device to automatically connect to their network when they are within range. For example, AT&T will connect to their own public Wi-Fi connections called "AT&T" at common retail locations like Starbucks. Whether we connect to it on our own or our mobile device connects for us, do we really filter what content we see? Is it that important to respond to personal email using publically available Wi-Fi? In this study, approximately 54% of the respondents connected to public Wi-Fi and shared some private information about themselves or other people. Those numbers were quite shocking but when you take a look at the factors such as high internet speed, limited Internet data allowances, and mere convenience, it isn't so shocking to see why people are connecting to public Wi-Fi connections.

As with any study, the researchers hope to understand more about their participants by analyzing their responses. The data collected about most of the accidental information sharing scenarios had responses of approximately 20%. The study concluded by almost 45% of the respondents saying they would change their behavior online. The general themes surrounding the responses were awareness of the potential risks and becoming more careful when sharing information. Frequently, we fail to see the "potential" risks that await us. Convenience and an "I want it now" attitude blind us to the unintended consequences. Sometimes this "awareness" can be enough to change our behavior and keep us from making costly mistakes. Likewise, just taking the extra step of double checking to whom we are sending messages, what information we post, or who actually owns that information about to be posted on the Internet can make a difference. From the participants' responses to how they can change their behavior, it became clear. They were now aware of some of the harmful effects of oversharing information. Moreover, they now realize they need to be more careful of what they share because we never know who will be hurt by the information exposure.

6. CONCLUSION

The first step to any change is awareness. With any new technology, people often seek out the conveniences and often forget or ignore the potential risk of their actions. This study aimed to understand the level that individuals accidentally overshare information and through what means information are shared. Results for connecting to a public Wi-Fi and accidentally sharing an SMS were as expected. However, the remaining scenarios averaged 1 in 5 respondents oversharing private information was a bit of a surprise. Even though these numbers could seem low to some, one must also remember that this information can include information about another person. So really the effect of accidentally sharing information might reach well beyond the 1 in 5 conclusion. However, given that almost 45% of the respondents stated that they would change their behavior online after completing this survey, one could conclude that after the participants were made aware of the potential risks, they valued their privacy enough to modify their behavior and in turn reduce the potential harmful effects that could result. Overall, one lesson learned is that awareness was very important and even if the participants were not accidentally oversharing information, once they learned of the effects, they felt the necessity to modify their behavior.

7. REFERENCES

CR Investigates. (2013, June). Keep your phone safe: How to protect yourself from wireless threats. Consumer Reports. *78-(6),* 18-22.

Debtain, B., Lovejoy, J., Horn, A., & Hughes, B. (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.

Gross, R., & Acquisit, A. (2005). Information revelation and privacy in online social networks. *Proceedings of WPES'05* (pp. 71-80). Alexandria, VA: ACM.

Hanrahan, M., and Cook, K. (2012). Police: burglars watched facebook statuses to find victims. Retrieved on June 25, 2013 from http://www.king5.com/video/featured-videos/Police-Burglars-watched-Facebook-statuses-to-find-victims-170703716.html

Krihnamurthy, B., & Willis, C.E. (2009). On the leakage of personally identifiable information via online social networks. ACM. Retrieved on June 15, 2013 from http://conferences.sgcomm/org/sigcomm/2009/workshops/wosn/papers/p7.pdf

Lipford, H.R., Besmer, A., & Watson, J. (2008). Understanding privacy settings in facebook with an audience view. *UPSEC'08: Proceedings of the 1st Conference on Usability, Psychology, and Security.* Berkeley, CA.

Madden, M., & Smith, A. (2005). Reputation management and social media. Retrieved on June 25, 2013 from http://pewinternet.org/Reports/2010/Reputation-Management.aspx

Madjeski, M., Johnson, M., Bellovin, S. (2011). The failure of online social network privacy settings. Department of Computer Science, Columbia University. Accessed July 2, 2013 from http://academiccommons.columbia.edu/catalog/ac:135406

Mish, F., C. & et.al. (Eds. 1983). Webster's ninth collegiate dictionary. (1st ed). Springfield, MA. Merriam-Webster.

Paullet, K., & Pinchot, J. (2012). Cybercrime: The unintentional effects of oversharing information on facebook. CONISAR Proceedings, New Orleans, LA.

Pinchot, J., & Paullet, K. (2012). What's in your profile? Mapping facebook security profile data to personal security questions. *Issues in Information Systems, 13(1),* 284-293.

Reeder, R. W., Kelley, P.G., McDonald, A.M., & Cranor, L.F. (2008). A user study of the expandable grid applied to P3P privacy policy visualization, *WPES'08: Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society,* ACM, 45-54.

Silmore, M. (2013, July). Appetite for information. *Carnegie Mellon Today, 10(3),* 26-29.

Vaidhyanathan, S. (2008, February 15). Naked in the nonopticon: Surveillance and marketing combine to strip away our privacy. *The Chronicle Review,* B7-B10.

Appendices and Annexures

Table 1: Age versus Member of a Social Networking Site

Age	Member Yes?	Member No?	Total
18	1.5%	0.00%	1.49%
19	12.7%	0.00%	12.69%
20	24.6%	1.49%	26.12%
21	14.2%	0.00%	14.18%
22	12.7%	2.24%	14.93%
23	7.5%	1.49%	8.96%
24	1.5%	0.00%	1.49%
25	1.5%	0.00%	1.49%
27	1.5%	0.00%	1.49%
28	2.2%	0.00%	2.24%
31	0.7%	0.00%	0.75%
35	1.5%	0.75%	2.24%
36	1.5%	0.75%	2.24%
37	0.0%	0.75%	0.75%
42	0.7%	0.75%	1.49%
44	0.7%	0.00%	0.75%
51	1.5%	0.00%	1.49%
52	0.7%	0.00%	0.75%
54	0.0%	0.75%	0.75%
56	0.7%	0.00%	0.75%
57	1.5%	0.75%	2.24%
62	0.7%	0.00%	0.75%
Total	**90.30%**	**9.70%**	**100.00%**

Table 2: Age versus Social Networking Site Membership

Age	Facebook	Twitter	YouTube	Foursquare	LinkedIn	Google+	Other
18	1.5%	0.74%	0.74%	0.00%	0.00%	0.00%	0.00%
19	12.5%	11.03%	8.09%	1.47%	0.74%	5.15%	4.41%
20	24.3%	20.59%	16.91%	2.94%	7.35%	6.62%	2.94%
21	14.0%	9.56%	8.82%	0.00%	5.88%	5.15%	1.47%
22	11.0%	9.56%	5.88%	1.47%	2.94%	1.47%	0.74%
23	7.4%	5.15%	5.88%	0.00%	4.41%	2.21%	0.74%
24	1.5%	0.74%	0.74%	0.00%	0.74%	0.00%	0.00%
25	0.7%	1.47%	0.00%	0.74%	0.00%	0.00%	0.00%
27	1.5%	0.00%	1.47%	0.00%	0.74%	0.74%	0.00%
28	1.5%	2.21%	1.47%	0.00%	0.74%	0.74%	0.00%
31	0.7%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
35	1.5%	0.74%	1.47%	0.00%	0.74%	0.00%	0.74%
36	1.5%	0.00%	0.00%	0.00%	0.74%	0.00%	0.00%
37	0.0%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
42	0.7%	0.00%	0.00%	0.00%	0.74%	0.00%	0.00%
44	0.7%	0.00%	0.00%	0.00%	0.74%	0.00%	0.00%
51	1.5%	0.74%	0.74%	0.00%	0.00%	0.00%	0.74%
52	0.7%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
54	0.0%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
56	0.7%	0.00%	0.00%	0.00%	0.74%	0.00%	0.00%
57	0.7%	0.00%	1.47%	0.00%	1.47%	0.00%	0.00%
62	0.7%	0.74%	0.74%	0.00%	0.74%	0.00%	0.00%
Total	**85.29%**	**63.24%**	**54.41%**	**6.62%**	**29.41%**	**22.06%**	**11.76%**

Table 3: Membership versus Social Networking Site Analysis

	Yes/No	Facebook	Twitter	YouTube	Foursquare	LinkedIn	Google+
Value	42.157[a]	40.976[a]	43.313[a]	24.681[a]	12.895[a]	25.591[a]	19.114[a]
df	44	22	22	22	22	22	22
Asymp. Sig. (2-sided)	.551	.008	.004	.313	.936	.270	.638

Table 4:

	Reply All	Attach-ment	SMS	MMS	Private Message	Family Friends	More Info	Accurate Info	Terms	Wifi
Yes	21.64%	18.05%	40.00%	18.52%	14.18%	22.22%	20.15 %	76.30%	26.67%	54.81 %
No	78.36%	81.95%	60.00%	81.48%	85.82%	77.78%	79.85 %	23.70%	73.33%	45.19 %

Table 5:

		Reply All	Attach-ment	SMS	MMS	Private Message	Family Friends	More Info	Accurate Info	Terms	Wifi
Age	Value	48.20	40.09	57.49	62.50	41.11	60.07	54.52	78.62	60.26	61.07
	df	44.00	44.00	44.00	44.00	44.00	44.00	44.00	44.00	44.00	44.00
	Sig.	0.31	0.64	0.08	0.03	0.60	0.05	0.13	0.00	0.05	0.05
Gender	Value	140.19	140.65	140.68	140.02	140.62	139.67	140.49	139.91	140.06	143.82
	df	9.00	9.00	9.00	9.00	9.00	9.00	9.00	9.00	9.00	9.00
	Sig.	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Education	Value	148.48	146.99	141.63	144.68	146.89	141.10	146.84	158.34	145.35	143.83
	df	18.00	18.00	18.00	18.00	18.00	18.00	18.00	18.00	18.00	18.00
	Sig.	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Study	Value	151.36	154.62	158.46	154.44	150.03	146.13	157.72	148.76	148.80	150.48
	df	30.00	30.00	30.00	30.00	30.00	30.00	30.00	30.00	30.00	30.00
	Sig.	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00