2016

A survey of social media users privacy settings & information disclosure

Mashael Aljohani
Security & Forensic Research Group, Auckland University of Technology, mashaeljohani@gmail.com

Alastair Nisbet
Security & Forensic Research Group, Auckland University of Technology, alastair.nisbet@aut.ac.nz

Kelly Blincoe
Security & Forensic Research Group, Auckland University of Technology, k.blincoe@auckland.ac.nz

DOI: 10.4225/75/58a693deee893
Aljohani, M., Nisbet, A., & Blincoe, K. (2016). A survey of social media users privacy settings & information disclosure. In Johnstone, M. (Ed.). (2016). *The Proceedings of 14th Australian Information Security Management Conference, 5-6 December, 2016, Edith Cowan University, Perth, Western Australia*. (pp.67-75).

A SURVEY OF SOCIAL MEDIA USERS PRIVACY SETTINGS & INFORMATION DISCLOSURE

Mashael Aljohani[1,2], Alastair Nisbet[1,2], Kelly Blincoe[2],
[1]Security & Forensic Research Group, [2]Auckland University of Technology
Auckland, New Zealand
mashaeljohani@gmail.com, alastair.nisbet@aut.ac.nz, k.blincoe@auckland.ac.nz

Abstract

This research utilises a comprehensive survey to ascertain the level of social networking site personal information disclosure by members at the time of joining the membership and their subsequent postings to the sites. Areas examined are the type of information they reveal, their level of knowledge and awareness regarding how their information is protected by SNSs and the awareness of risks that over-sharing may pose. Additionally, this research studies the effect of gender, age, education, and level of privacy concern on the amount and kind of personal information disclosure and privacy settings applied. A social experiment was then run for 3 months that tested SNSs users' reaction to a profile access request by a stranger. The research focused on four different social networks: Facebook, Twitter, Instagram,and Snapchat. The results of the survey and experiment found that there is a significant amount of personal information disclosure, but that the level differs between social networks. It is reveals that gender, age, and education have significant influences on information disclosure and user's privacy settings and that on most sites over 50% of friend requests were readily accepted. These results are a selection from a comprehensive study of some of the more revealing facts about SNS user ship covering 3 months of data collection and almost 500 responses.

Keywords
privacy, security, social networks

INTRODUCTION

Social media and social networking sites (SNS) are now utilised by a large majority of Internet connected people around the world. With the benefit of almost instant communication to potentially billions of other people, the temptation may be to connect as simply and as quickly as possible to enjoy the benefits of social media. With benefits, there are often drawbacks and the recent publicity of privacy breaches, identity theft and the dangers of over-sharing, social media users signing up for and utilising the sites' service should be wary of just how much information they disclose. Of the many SNS's available to consumers, Facebook, Twitter, Snapchat and Instagram are currently the most heavily visited sites. Each site has a user's conditions that are available to be read when a new user creates an account with the site. Often, these agreements may not be fully read or fully understood yet many users agree to the terms and continue to enter personal details to create their account. Some sites have publicly available areas where non-members r general members who have had no prior contact with a user's page can view information posted by the member. At times, this information may be of a personal nature that some members may wish to keep private or may be sufficient information to identify a person, a place of residence or other uniquely identifying feature. It has been argued that advances in communication technology have made people more tolerant and more willing to share information about themselves in a way that renounces the value of privacy in order to be more connected and traceable, specifically among younger generations (Tubaro, Casilli & Sarabi, 2014). Whilst much data exists regarding the numbers of people utilising social media, often on a daily basis, the makeup of the users in relation to their privacy settings and disclosure has been rarely examined.

LITERATURE REVIEW

Technological advancement has become less focused on connecting computers and more concerned about connecting people. A main contributor to this evolution is the use of social networking sites (SNS), which has seen explosive growth in use in the last couple of years (Zheleva, Terzi, & Getoor, 2012). As of August 2016, there are more than 2.22 billion users of SNSs (Statista, 2016). Due to the increasing popularity of SNSs and the drive to reach customers, more than 70% of businesses are now using SNSs (McKinsey Global Institute, 2012). Although SNSs provide a powerful tool to engage people over the web, they can be a source of possible threats to users' privacy and security because users routinely and voluntarily provide personal information (Cross, 2016).

Social networks initially started as websites where users only access to them was with a laptop or a desktop. However, with the advancement of smartphones, social networks released mobile application versions of their sites and other social networks developed mobile standalone applications for access. This development made it easier and more convenient for users to access their online profiles and update more actively and in real time (Aldhafferi, Watson, & Sajeev, 2013). However, the more accessible the social network, the easier it is to be used and the more information the user tends to share (Coyle & Vaughn, 2008). SNSs have unquestionably a strong social impact and the line between a person's virtual and offline life may for some, become blurred.

SNSs have evolved over the years and have gone through many phases of development to reach their current state (Hendricks, 2013). The first recognisable form of SNS that encouraged users to include personal information about themselves for the purpose of social networking emerged in 1997 with a site called SixDegrees (Boyd & Ellison, 2007). It allowed users to open personal accounts and create a list of friends. SixDegrees attracted over a million subscribers at its peak (Chapman, 2009). However, although SixDegrees managed to become popular and attract large numbers of subscribers, the site was not able to maintain its popularity (Boyd & Ellison, 2007). In 2001, SixDegrees.com was shut down. According to the founder of SixDegrees, the failure of his website was due to the fact that SixDegrees was ahead of its time: at that time, not many people had friends who were online and the idea of being online friends with strangers had not yet gained universal acceptance (Prall, 2010).

The concept of creating a virtual SNS inspired other developers (Liu, 2014). In the early 2000s, more people started to have Internet access, hence the target audience became much broader. This helped the success and increased the popularity of SNSs such as Friendster, which has attracted more than 90 million users. It introduced the ability for users to discover their friends and then friends-of-friends, and thus expand their networks and share more information with others.

The vast spread of SNSs started to occur at the start of 2003, initially when Myspace was launched, which grew to be the most popular SNS in the world at that time (Boyd & Ellison, 2007). Myspace differentiated itself from other competitors by giving users the freedom to customise the look of their profiles. In 2004, Facebook was launched initially as a Harvard-only social network and became the most popular SNS in 2008, overtaking Myspace. As of the second quarter of 2015, Facebook has 1.49 billion monthly active users (Statista, 2016). Facebook managed to maintain its success by constantly improving the site and by adding new features (Hendricks, 2013).

At the present time, hundreds of SNSs have emerged, each designed to serve a different audience or have a different style that distinguishes it from other SNSs. Figure 1 shows the vast growth of SNSs from 2006 to 2012.

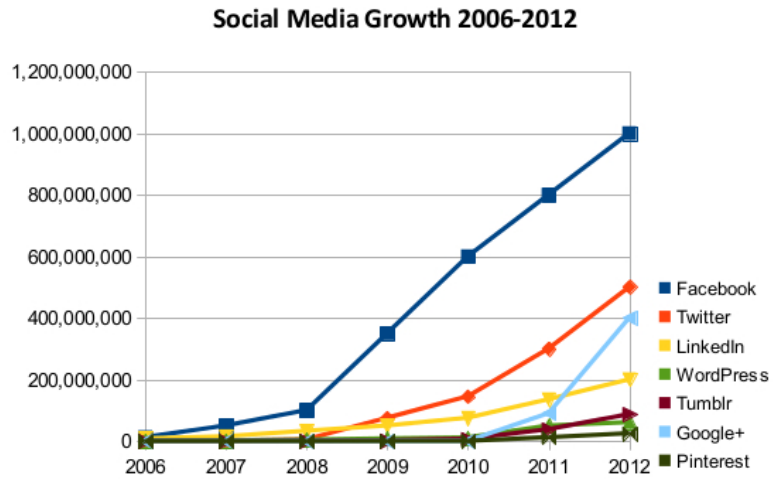

Figure 1: Growth of Online Social Networks, 2006-2012. (Source: White, 2013)

As of August 2016, there are over 2.34 billion social network users globally. This number is expected to increase and reach 2.95 billion social networks users by 2020, which is close to a third of the world's entire population (Statista, 2016). The last decade has witnessed a rapid growth in the number of individuals using SNSs. For instance, as of June 2016, Facebook was regarded as the third most used website globally after

Google and YouTube (Alexa, 2016). Although SNSs provide many benefits for individuals such as keeping in touch with friends and family, privacy and security is regarded as a critical issue that can threaten the users of SNSs (Donath, 2007). This is mainly because SNSs encourage their users to reveal a great deal of personal information about themselves by promising them a better user experience if they do so (Luo, Liu, Liu, & Fan, 2009). For example when users first sign up to Facebook, they will be constantly asked and reminded by Facebook to update their profile with more personal information such as date of birth, hometown, workplace, and/or school in order to find more friends and enjoy the experience better (Lewis, n.d.). The growing popularity of SNSs and the fact that they contain enormous amounts of information make these websites an attractive target for malicious hackers. It is therefore vital that users are aware of the risks of disclosure of personal information and how the information they disclose can be used by unscrupulous individuals to commit crimes such as Fraud and other scams.

The following section discusses the research phases including design of the questionnaire.

RESEARCH DESIGN

The aim of this research is to shed the light on SNS user's personal information disclosure behaviours, their privacy protection settings, privacy policies and users SNS privacy knowledge and awareness. The study was conducted to identify the effect of gender, education status, and age on the degree of personal information disclosure and protective privacy settings applied by the user, using factor analysis. Four most common SNS sites were selected as a cross section of social media sites, each giving a different purpose for the members and viewers of the sites, from primarily text based to primary video and graphics based sites. These sites are Facebook, Twitter, Instagram and Snapchat. An online survey was conducted which aimed to answer the following proposed research questions.

Q1: What are the personal attributes that can have an influence on information disclosure and privacy settings of SNS users?

Q2: Do users' levels of privacy concern have an effect on the amount of information they disclose in social networking sites?

Q3: Are users aware of how their information is protected by SNS providers according to the privacy policies that the users have agreed to?

In addition, a further experiment was conducted to test how users react to stranger's friendship of follow requests. In this experiments, requests were sent to people the requestor had no prior personal knowledge of to ascertain how likely it was that the friend request would be accepted.

Initially an online form was created with the link to the form posted on each of the four sites. In Twitter, for example, the link for the survey was tweeted with trending hash-tags in order to ensure it had wide exposure. In the post, there was a brief description of the survey in order to encourage users to take part in it. For the social experiment, users were selected randomly from their participation in public pages such as newspapers or public figures' pages by either liking a post or commenting on a post. With a population of the four sites combined reaching approximately 1.5 billion users, the confidence level of 95% and margin of error of 5% was found to be appropriate. This meant that a minimum of 385 responses would be required for the survey to have this validity.

Two stages of analysis were used in this research to derive the main findings.

1) Exploratory data analysis (EDA): In this stage, the data files are viewed before completion of the data collection in order to get some ideas about the initial results. The purpose of this stage is that it may indicate further data are required: for instance, there may be more female responses than male responses, which could affect the accuracy of the results. This preliminary stage ensured that any imbalances and limitations in the data were resolved before the end of the data collection period. This stage overlaps with data cleaning because anomalies can become evident. Therefore, in an optimal situation, before the end of this stage, there should be a clean dataset that is ready for the next stage of analysis.

2) Deriving the main findings: This stage generates a summary of the findings, relationships, trends, interpretations and narratives. When analysing the data, the type of questions dictate the type of analysis. However, in general, two tools are used together to analyse the data. The first tool is filtering,

which is provided by Survey Monkey to help break down the results in order to focus on a specific data subset. It allows viewing specific respondents' answers to specific questions. For instance, it allows viewing of all the answers of male respondents who are between the ages of 20-24 years and who answered that they do not trust SNS providers with their information. Secondly, the information is transferred into SPSS in order to analyse it statistically. Factor analysis has been conducted. Separate chi-square tests of contingencies were conducted in order to understand and determine the differences in user privacy setting behaviours and personal information disclosure variables with gender, age, education, and privacy rating for each of the four social networks. All chi-squares were interpreted at a conservative alpha of .01 to control for multiple tests. The chi-square analysis helps to determine whether two discrete variables have any statistical association and whether there is a statistical significance between the variables.

RESULTS

The survey was run from January 2016 to March of that year and 415 people completed the survey. The first question in the survey was: Which of the following Social Networking sites do you currently have an active account with and use? (Check all that apply). The purpose of having this question at the start was to disqualify any non-SNS users and to identify what SNSs the survey participant was currently using. The results revealed that Snapchat was the dominant SNS among the four networks, with a response rate of 69.6%. Snapchat is the newest social network between the other three networks. Facebook, which is one of the oldest SNSs, had the lowest percentage of users in this survey at 55.9%. Table 1 represents the findings and the rankings of the SNSs by the survey participants.

Table 1: Chosen SNSs by the users in the sample

Answer Choices	Responses
Facebook	55.90% N=*232*
Twitter	56.87% N=236
Instagram	60.96% N=253
Snapchat	69.64% N=*289*
None	3.37% N=*14*
Total Respondents: 415	

The next results looked at the membership of the four sites broken down into gender to identify if gender played a role in choice of sites to join. Figure 2 shows that a majority of males (75.52%) in this sample used Facebook; however, females used Facebook the least and Snapchat the most with 79.02%.

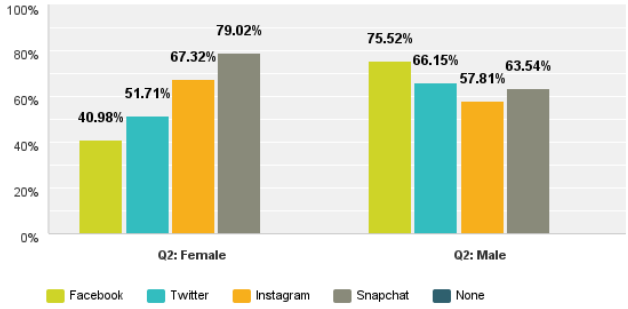

Figure 4.1 Male vs. Female Choice of SNS

One question was designed to determine the reason behind a user becoming a member of the site. With the growing acceptance of SNS's, this question looked at why people joined and was useful for also inferring why many people who are regular Internet users continue to resist joining sites.

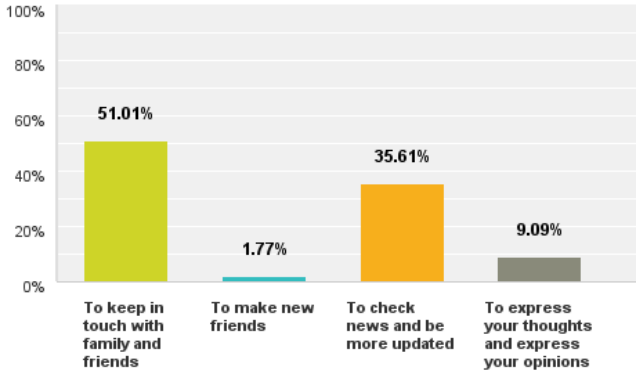

Figure 3: Motivation for using sites

Figure 4 displays the frequency of SNS use by the survey participants. It shows that most of the members are frequent users of SNSs, with 82.9% being daily users.

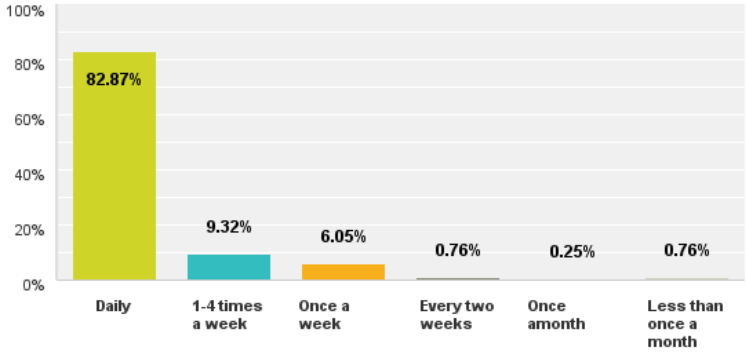

Figure 4: Frequency of site visits

Figure 5 presents the findings of the question "Is the privacy of your information on Social Networking sites a major concern for you?" The purpose of this question was to establish the value of online privacy for the user, which can affect their answers to other questions. For instance, if someone is not very concerned about the privacy of their information online, they will likely not be so stringent in applying protective privacy and security settings to avoid leakage of information. In addition, people who value their privacy and are more concerned about their information will probably not share as much personal information compared to those who are less worried about privacy.

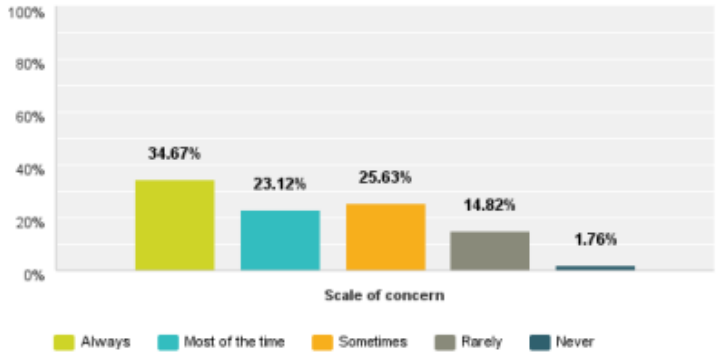

Figure 5:Scale of concern over privacy

The results showed that there was a lack of trust in SNS providers with regard to storage and protection of users' information, as 66.3% of the survey respondents answered that they did not trust their providers with their information. These findings will be used later in this chapter to compare users' actual actions with their levels of

personal information disclosure and examine the ways they apply privacy settings to protect their information and online identity. If users are disclosing personal information, then one method to hinder the use of information by unscrupulous individuals is to use fake or partially fake identities. Figure 6 shows the percentage of members who use their genuine name, fake name or partially fake name such as a genuine first name with a fake surname.

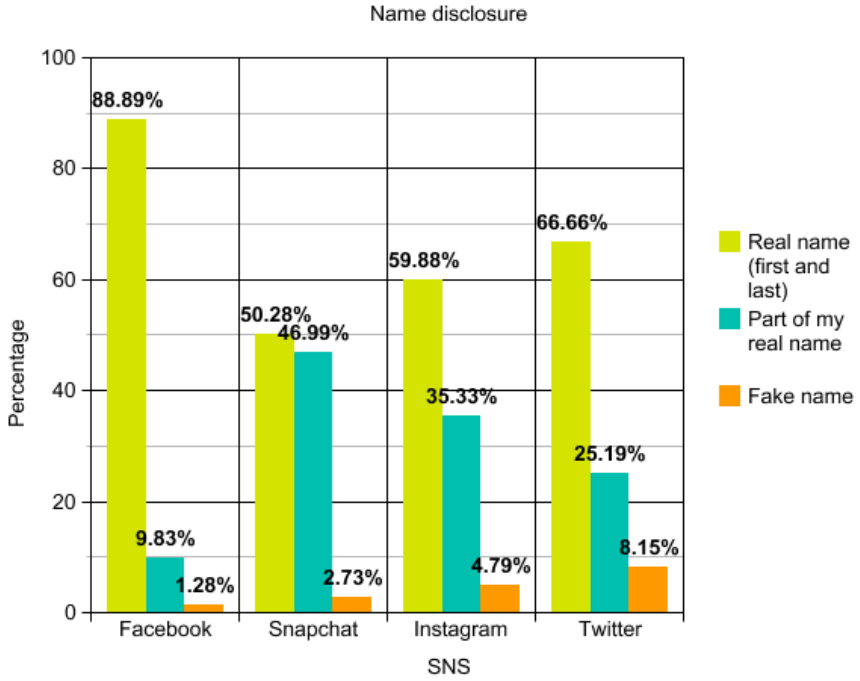

Figure 6: Name disclosure in Facebook, Snapchat, Instagram and Twitter.

The next results looked at the information disclosure and privacy settings members used on the four sites. The Facebook results are indicative of the four sites and indicate the varying level of disclosure people are willing to make. More personal information tends to be kept private on the sites and more generic information such as the city of residence tends to be more freely disclosed.

Table 2: Facebook: Personal information disclosure and privacy settings

	Public	Friends	Customised group of friends	I don't share this information with others	Total Respondents
Hometown	53.9%	36.0%	3.9%	6.1%	228
Current city	52.8%	36.7%	4.8%	5.7%	229
Family members	24.9%	52.8%	7.4%	14.8%	229
Relationship status	29.3%	50.7%	4.8%	15.3%	229
Birthday	41.3%	47.8%	3.5%	7.4%	230
Education	44.5%	45.4%	3.5%	6.6%	227
Events	26.3%	59.2%	5.7%	8.8%	228
Locations visited	24.3%	55.7%	4.3%	15.7%	230
Friends List	26.8%	54.8%	6.6%	11.8%	228
Contact Information	22.2%	50.0%	7.0%	20.9%	230

Instagram is a site dedicated to allowing members to post pictures and videos. The site allows for a brief description of the graphic or video allowing members a choice of how much information about the posting they wish to disclose. Table 3 shows the results for this site.

Table 3: Instagram: Types of personal information posted

	Yes	No	Total
I post pictures/videos of myself	55.7%	44.3%	271
I post pictures/videos of family members/friends	58.7%	41.3%	269
I include the real location of my pictures/videos	69.4%	30.6%	271
Sometimes I post a photo with my house location in the map	39.8%	60.2%	269
I include contact information in my profile	59.6%	40.4%	270
Does your profile picture contain a picture of yourself?	60.0%	40.0%	160

The next series of questions in the survey focuses on the awareness of users of the security policy wordings and the implications of accepting the site's agreements. Much research has been done on users' lack of careful reading of acceptance policies and the results in table 4 indicate that users generally trust that the site will protect their personal information. Careful reading of the policies tends to indicate otherwise in many cases with some sites quite clear that any information, graphics or videos can be reproduced by the site or passed on for any reason without the users permission.

Table 4: Facebook privacy policy awareness question: response frequency

Statement	Proportion of survey participants who do not believe that this statement is true
Collect and use all the information they receive about you to suggest advertisements for you	78 (33.6%)
Track your web surfing anytime you're logged into the site	43 (18.5%)
Use your public information, such as your profile picture, in ads without asking you first and without any compensation to you	45 (19.4%)
Collect information about your device locations, including specific geographic locations, through GPS, Bluetooth, or WiFi signals	59 (25.4%)
None of the above	132 (56.9%)

With the increasing publicity about the risks of over-disclosure of personal information to strangers, many SNS sites are responding by providing much tighter privacy settings for their users. Several sites now prevent graphics searchers to their sites so that a simple search for a picture found on the Internet, even directly downloaded from one of these sites, will often result in no matches on the site. These types of additional security are designed to protect their users from stalking and identity theft. However, these measures only provide greater resistance to these types of criminal acts if users are cautious about whom they permit to view their private information reserved for 'accepted' friends. Table 5 shows the results from setting up a fake profile and then requesting to 'friend' these strangers. Strangers were chosen as randomly as possible by selecting pages during browsing of users' sites. Results show that acceptance rates vary between sites but that 3 out of the 4 sites have greater than 50% acceptance of these fake friends.

Table 5: Acceptance rate for fake profiles on Snapchat, Facebook, Twitter and Instagram

	Users added	Users accepted the add	Frequency of acceptance
Snapchat	400	120	30%
Facebook	400	245	61.25%
Twitter	400	233	58%
Instagram	400	224	56%

The next point of interest was designed to ascertain generilastions from the four sites about whether gender played a significant role in how much personal information was disclosed. As an example which is representative of all sites, Facebook results are shown in table 6. These results indicate that gender does play a role in personal information disclosure with males more likely to disclose personal information than females in

every category. One interesting result from the survey is that in most cases there is no difference between the genders on accepting friend requests. It would appear from this result that the sociability of the members is something accepted by males and females equally.

Table 6: Facebook: Gender Chi-square description of results

Attribute	Results of cross -tabs and Chi Square analysis
Hometown	- Males more likely than females to be public - Females more likely than males to be friends - Females more likely than males to be "don't share
Current City	- Males more likely than females to be public - Females more likely than males to be friends - Females more likely than males to be "don't share"
Family members	- Males more likely to be public than females - Females more likely to "not share' than males
Relationship status	- Males more likely to be public than females - Females more likely to "not share' than males
Birthday	- Males more likely than females to be public - Females more likely than males to be friends
Education	- Males more likely than females to be public - Females more likely than males to be friends - Females more likely than males to "not share"
Events	- Males more likely than females to be public - No difference on friends - Females more likely to "not share"
Locations visited	- Males more likely than females to be public - No difference on friends - Females more likely to "not share"
Friends list	- Males more likely than females to be public - No difference on friends - Females more likely to "not share"
Contact information	- Males more likely than females to be public - No difference on friends - Females more likely to "not share"

Finally, Snapchat results are shown in figure 6 for posting of personal photos and videos. Snapchat promises to permanently delete these photos and videos after a short time but there has been a greater public awareness recently that they are in fact quite easily recoverable from devices that have viewed these items and that the site owners generally retail rights to these often very personal photographs. Results indicate that females are much more likely to post pictures of friends and family members and that younger people tend to be much less concerned by posting these types of personal family and friend pictures and videos.

Table 6: Snapchat Chi-square analysis results for posting pictures/videos that include family members/friends

		Yes	No
Gender	Male	74(56.9%)	56(43.1%)
	Female	122(77.7%)	35(22.3%)
Age	16-24	119(75.8%)	38(24.2%)
	25-34	61(62.9%)	36(37.1%)
	35+	16(47.1%)	18(59.9%)
Education	High school	41(83.7%)	8(16.3%)
	Bachelor	104(68%)	49(32%)
	Masters	42(59.2%)	29(40.8%)
	Doctoral	9(60%)	6(40%)
Privacy	Rarely/Never	42(84.0%)	8(16%)
	Sometimes	46(60.5%)	30(39.5%)
	Mostly	44(67.7%)	21(32.3%)
	Always	64(66%)	33(34%)

CONCLUSION

The results from the survey are a selection of several of the more interesting points taken from the findings. The questionnaire comprised of over 30 different questions with many diverse areas of SNS privacy investigated. This selection of results shows that many factors comprise the profile decisions of users and those who choose to join as members. The publicity over the risks of disclosing private information that may be used to construct fake profiles, stalking and other nefarious activity seems to have had little effect on many SNS users. The desire to be part of a community, often with hundreds of friends, most of which the person will never meet and who themselves may be using fake identities, seems to have only a modest effect on the users' sense of caution. The results indicate that people are generally willing to use real names, disclose personal attributes such as dates of birth and hometown locations and often post personal pictures that could identify themselves, family members and friends. The use of privacy settings where only 'friends' can view posts, videos or pictures is largely negated by the ready acceptance of both males and females to accept friend requests from people whom they have no prior knowledge of and no method to ascertain the genuineness of the identity or desire to follow them. These results indicate that whilst the messages about the risks of over-disclosure are regularly repeated, most social networking site users are making their own decisions about what they wish to disclose and often these decisions are not fully informed by the reading the user agreements and are putting users at risk because of their desire to belong to these communities and share their information with strangers.

REFERENCES

Aldhafferi, N., Watson, C., & Sajeev, A. (2013). Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices. *International Journal of Security, Privacy and Trust Management*, *2*(2), 1-17. doi:10.5121/ijsptm.2013.2201

Alexa. (2016). Alexa Top 500 Global Sites. Retrieved from http://www.alexa.com/topsites

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: definition, history and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210-230. doi:10.1109/EMR.2010.5559139

Chapman, C. (2009, October 7). The history and evolution of social media. Retrieved from http://www.webdesignerdepot.com/2009/10/the-history-and-evolution-of-social-media/

Donath, J. (2007). Signals in social supernets. *Journal of Computer-Mediated Communication*, *13*(1), 231-251. doi:10.1111/j.1083-6101.2007.00394.x

Cross, M. (2014). *Social media security: Leveraging social networking while mitigating risk*. Rockland, MA: Syngress (Elsevier Science).

Lewis, K. (n.d.). How social media networks facilitate identity theft and fraud. Retrieved from https://www.eonetwork.org/octane-magazine/special-features/social-media-networks-facilitate-identity-theft-fraud

Luo, W., Liu, J., Liu, J., & Fan, C. (2009). *An analysis of security in social networks.* Paper presented at the Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 12-14 December, Chengdu. doi:10.1109/DASC.2009.100

Prall, L. (2010, September 20). SixDegrees - social networking in its infancy. Retrieved from http://eziniearticles.com/?SixDegrees---Social-Networking-In-Its-Infancy&id=5064109

Statista. (2015). Facebook: monthly active users 2015 | Statistic. Retrieved from http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Tubaro, P., Casilli, A. A., & Sarabi, Y. (2014). Against the hypothesis of the end of privacy: An agent-based modelling approach to social media. SpringerBriefs in Digital Spaces, DOI: 10.1007/978-3-319-02456-1_1.

Zheleva, E. M., Terzi, E., & Getoor, L. (2012). *Privacy in social networks*. San Rafael, CA: Morgan & Claypool.