Concordia Journal of Communication Research

Volume 8 Article 1

2023

Social Media Use and Awareness of Privacy Concerns

Lola Baldwin
Concordia University, St. Paul, baldwinl1@csp.edu

Jared Gores
Concordia University, St. Paul, goresj@csp.edu

JP Kilbride
Concordia University, St. Paul, kilbridj@csp.edu

INTRODUCTION

Over the past couple of decades, there has been a large rise of mobile phones, and subsequently the rise of social media platforms. While there are numerous studies pertaining to the use of mobile phones, there is limited research on the use of these platforms and attitudes surrounding them. The emergence of these platforms that allow for greater connectivity between individuals has also brought with it, an increase in safety and privacy concerns. Many social media platforms outline their intentions with user information and privacy interests in their terms of service agreements; however, as many of these agreements are pages long and difficult to understand, the majority of users don't take the time to read them.

The purpose of this study was to see if increased awareness of privacy risks on social media influence one's concerns or attitudes when it comes to decisions regarding safety and overall privacy on social media. Topics covered and addressed include the rise of social media and usage, overall privacy on social media, self-disclosure motivations, etc., and how these overlap with one another. This study explored how college students at a private, faith-based, Midwestern school use social media and similarly, how concerns over privacy affect such use. How does network size affect individuals' posts? How do concerns of online privacy change with increased awareness of how data is collected and used? These are a couple of questions this study hopes to answer. A pre-test and post-test will be utilized in the study to measure if there is significant change in one's privacy concerns and attitudes towards social media after viewing a video on online safety and privacy risks.

In a world that is becoming increasingly technology based, protecting one's privacy will only grow more important. By studying this aspect of privacy in social media use, more can be learned about concerns regarding social media and behaviors.

LITERATURE REVIEW

Rise of Social Media & Usage

Social media platforms are applications that allow users to interact with each other on a digital level. Social media differs from traditional media channels in that users, or consumers, can also be producers of information. Over the course of the past two decades, Internet usage, specifically social media usage, has been on the rise (Hollenbaugh, 2019). According to Pew Research Center, in 2005, only 5% of U.S adults used social media. That percentage increased to 69% by the end of 2016 (Pew Research Center, 2017). Despite an overall increase in usage, certain groups of people are more likely to use social media platforms and practice certain online behaviors. One of these groups are younger individuals who are digital or social media natives. Digital natives are defined as "individuals whose childhoods were surrounded by advancing technologies, screens, pushing of buttons, and social networking sites" (Hollenbaugh, 2019). An annual survey conducted by Pew Research (2014) found that, "Social media natives are more likely to use multiple social media applications than older digital natives and digital immigrants. Members of older generations are both more aware and concerned of potential privacy problems, which then similarly leads them to use social media platforms at a lower rate" (Cain & Imre, 2021, p. 2706).

Privacy on Social Media

Online privacy, or privacy of information shared online is defined as, "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Cain & Imre, 2021, p. 2707). Because information-sharing is the basis of social media participation, the rise of social media use also

brings the rise of privacy concerns (Agosto & Abbas, 2017). Through focus groups and questionnaires, a study conducted using eighteen and nineteen year old public high school students found that older teenagers are less concerned with online safety and more concerned with online privacy (Agosto & Abbas, 2017). This finding relates to a separate study where participants were recruited to complete an online survey via an invitation posted on Amazon's Mechanical Turk's website. Participants were given statements regarding preferences on privacy and intensity of social media use and were asked to indicate their level of agreement on a numeric scale. Findings from this study "support that concerns over control, collection, and access to personal information are associated with decreased intensity of social media use" (Cain & Imre, 2021, p. 2706). In other words, the more concerned one is about the privacy of their information, the less intensely they will use social media platforms. Since Agosto & Abbas [2017] indicate that teenagers are more concerned with online privacy than online safety, findings from Cain & Imre [2021] should indicate that, because of these higher privacy concerns, these individuals would decrease the intensity of their usage. However, this is not the case, as external factors, such as peer influence, can pressure individuals to disclose personal information and participate on social media (Agosto & Abbas, 2017). A separate study examined the differences between cultures in terms of privacy and self-disclosures on Twitter. Using data from Twitter's Application Programming Interfaces, this study collected information from ~3.3 million valid Twitter accounts. This information included privacy protection settings, location settings, frequency of usage, age when the Twitter account was created, and network size (how many followers & how many following). Findings from this study support that users with higher levels of usage were more aware of information accessibility, and more likely to self-disclose if they had privacy protections enabled (Liang, Shen & Fu, 2017).

Factors That Influence Decision Making

In today's day and age, we are more surrounded by technology than we ever have been, and there are numerous factors that can sway our thinking and behaviors. The study of college students and their amounts of personal privacy protection behavior was an analysis of their privacy settings displayed in an online social network. “Private profiles may reflect a particularly strong discrepancy between online and other ‘public’ performances; a particularly strong sensitivity to *any* such discrepancy; or a general tendency towards role compartmentalization, even if the roles are compatible. Each of these possibilities, however, suggests a particular *cultural disposition*” (Kaufman at el, n.p). The goal and purpose of getting specific information was to find out the participant’s definition of privacy, and what the possible motivations for creating a private profile could be. The research found that if participants are surrounded by peers who have private accounts, they will also choose to have a private profile. The research was successful in its findings that other influences such as peer influence have a direct impact on the privacy decisions of college students. However, peer influence isn’t the only influence that affects one's attitudes towards online decision making.

Self Disclosure and Disclosure Motivations

Social media technologies have opened new possibilities for sharing personal information with online networks, and millions of people routinely self-disclose personal information on social network sites (SNSs).When you decide to create an online profile, there are various decisions as to the levels of self disclosed information that you want visible, or not visible to the public. There are also a variety of disclosure motivations, such as the people we surround ourselves with in life. How our peers think and view these challenges oftentimes shapes our own

views. Research was conducted to try to find answers for why people disclose the things they do, and why they decided to share things as well. The purpose of the study is to see if people post greater social validation goals in nondirected status updates compared to directed wall posts and private messages. The article examines starting point beliefs as well as different audiences people create on their social media sites. “This article introduces the functional model of self-disclosure on social network sites by integrating a functional theory of self-disclosure and research on audience representations as situational cues for activating interpersonal goals” (Choi, 2014). We all have reasons why we post, and this article examines that logic and way of thinking in order to try and dig deeper into the reasoning behind these decisions. Since everyone has their own definition of privacy, there is going to be a very wide range of opinions and beliefs, so it becomes extremely important to cast a wide net in hopes of uncovering answers to why people make the decisions that they do regarding online privacy and disclosing certain amounts of information. Kaufman’s research (2008) draws on the protection motivation theory to investigate privacy protective behavior online. They tested the hypothesis that higher levels of perceived severity of online privacy threat will lead to more protective behavior. The results supported the hypothesis that there is indeed a self-reported protective behavior. “Given the relationship between use and privacy concerns, leaving privacy concerns unaddressed might also lead to a reduction of use if these concerns continue to grow among users” (Cain, Imre, 2021).

Challenges for Online Privacy

With many social media and online shopping sites utilizing cookies, users are now more fearful of their own private data being used by corporations to make more profit (Pierson, J. and Heyman, R. 2011). With the utilization of these web data collectors, users struggle to find a way

to keep their privacy safe from others. This concern draws from a lack of awareness, when a tech company collects data through cookies, the user is usually unaware that their data is being collected (Lavin M. 2016). Users have also found the collection of private data to be intrusive, they find themselves being constantly recommended different sites and products (Pierson, J. and Heyman, R. 2011). This starts to hinder the flow of self-communication through social media if most discussions and posts are centered around promoting products (Pierson, J. and Heyman, R. 2011).

Another challenge for privacy is the fast paced time that we live in, the digital age is ever changing and rapidly changing, and is as tempting as ever, so as much as we can do to limit temptation and not conform to what peers and those around us are doing, the better that will be. As previously mentioned in the Lewis study, peers and parents are at the top of the list for influences, but there are also challenges presented by these groups. We are most likely to conform to our surroundings when it comes to privacy as a whole, and when it comes to individualized decisions and privacy preferences.

HYPOTHESES

When considering people's social media habits, privacy is often taken a backseat in favor of social interactions with other users. In the study of motivations for online privacy protection behavior (Boerman, S, C. 2021), it was shown that users' confidence in online privacy is mixed. The focus of this study will be to observe if there is a change in attitudes regarding privacy after watching a short video about how users data is collected from social media and online activity as well as potential risks.

H1: There will be a change in attitudes or concerns about privacy online after watching a short video about how their information is collected and used.

Research suggests that many social media users are unaware of privacy protections and how these platforms collect and use personal information. Terms of service agreements are often lengthy and complicated to read, so many users agree to the terms of usage without fully understanding the contracts. Increased knowledge and awareness of how users' information is being used will lead to a change in concern or attitudes about privacy.

H2: Individuals with larger social media networks will protect their profiles and disclose less private information.

As social media continues to grow more easily accessible to users across the globe, concern over self disclosure in posts has become a prevalent issue. In a global study of privacy protection and self-disclosure (Liang, Shen & Fu, 2017), data suggests that cultural variations of privacy settings and self-disclosure differed by society. Individuals from more collectivist cultures tend to disclose more, however, those from more individualistic cultures or those with smaller network sizes tend to disclose less. A larger network usually implies a less familiar audience and thus is associated with higher privacy risks. So, individuals with larger networks will disclose less private information and likely have a private account.

METHODS

Participants

The units of analysis for our research study are students attending a small, private faith-based (Lutheran) university in the midwest. Besides the requirement of attendance, there were no other demographic factors like age, race, ethnicity, gender, etc., that were required for participation. There were no incentives used to motivate participants. Our research focuses on social media use and its surrounding privacy concerns. In order to garner as many responses as possible, the researchers used SurveyMonkey to create our survey and a link to send via email to

all undergraduate students at the university. Of the 1,286 emails that were sent out, 50 responses were received. However, only 39 participants completed the entirety of the survey, giving the researchers a response rate of <1%.

Procedure

Our experimental design is a cross-sectional study which focuses on analyzing data from a population at a specific point in time. Using a pre-test and a post-test, the study is field-independent and self-administered, as it was conducted via SurveyMonkey, an electronic survey platform. Prior to completion of the survey, participants read the consent form which detailed the purpose of the study and amount of time it would take to complete. In between the pre-test and post-test, a video on how user data is collected and used on social media, as well as potential privacy risks was shown. In terms of type of sampling, we used the convenience method as we relied on volunteers from the university, our population, to participate. The survey remained open for one week for participants to respond before it was closed.

The survey is a pre-experiment with one-large group pre-test & post-test design. The survey was created by the researchers, with the pre-test/post-test questions, or statements for participants to indicate a level of agreement to, being close-ended. This way, we could obtain measurable and quantitative data. Additionally, the questionnaires are easier for participants to understand and complete. For this research study, we used a Likert scale in which respondents could indicate a level of agreement to a particular statement. The survey questions focused on what platforms participants used and for how much time daily, network size, privacy protections and concerns over privacy on social media (See Appendix: Figure 1). For the first hypothesis (two-tailed), in order to observe if there was a change in attitudes or concerns over privacy on social media, a single-sample t-test was used for each set of corresponding questions on the pre-

test and post-test. For our second hypothesis, a chi-square test was used to determine whether there was a significant relationship between network size and frequency of posting.

RESULTS

A total of 50 surveys were completed by undergraduate students at a private, faith based university in the Midwest. However, 11 of the 50 surveys were incomplete, so only 39 responses are available for analysis. There were 15 questions in total on the survey, with 10 questions on the pre-test and 5 questions on the post-test. The first five questions of the survey were about the participants' online activity and social media presence. Participants were asked to indicate what social media platform(s) they used daily and for how long, their privacy settings, network size and how frequently they post. The next five questions asked respondents to indicate their attitudes regarding privacy of their information and the levels of concern they had. A short video was then shown, with the post-test questions being the same as the last five questions of the pre-test.

H1: There will be a change in attitudes or concerns about privacy online after watching a short video about how their information is collected and used.

For our first hypothesis, in order to observe if there was a statistically significant change in attitudes or concerns about privacy online after watching a video, a single sample t-test was used for each corresponding set of questions on the pre-test and post-test. The first question on both the pre-test and post-test asked “How aware are you about how your information is being collected and stored on social media platforms?”. The result is significant [$p < .00001$]. The researchers can conclude there was a change in awareness following participants being shown the video on privacy risks on social media.

The second question asked "How much concern do you have about your privacy on these social media platforms?". The value of p is .000031, with the result significant at $p < .05$. The researchers conclude that there was a change in concern from watching the video on social media privacy risks.

The third question asked participants to indicate their level of agreement to the statement, "I am concerned that social media sites are collecting personal information about me". The result is significant [$p = .000877$], meaning there was a change in concern over social media sites collecting user data.

The fourth question asked participants to indicate their level of agreement to the statement, "I am concerned that social media sites do not devote enough time and effort to preventing unauthorized access to my personal information". The value of p is .000271. The result is significant at $p < .05$, so there was a change in participants' concern over how much their information was protected.

The fifth and final corresponding question of the pre-test and post-test asked participants to indicate their level of agreement to the statement, "I am concerned that social media site databases that contain my personal information are not protected from unauthorized access". The result is significant [$p = .000257$]. There was a change in level of concern over the protection of users data from unauthorized parties.

With these results from five different t-tests from each corresponding question from the pre-test and post-test, the researchers fail to reject the null and accept the first hypothesis, that there is a significant change in attitudes or concern over privacy on social media after watching an informational video on how information is collected and potential risks.

H2: Individuals with larger social media networks will protect their profiles and disclose less private information.

The second hypothesis, that individuals with larger social media networks will protect their profiles and disclose less private information, was tested by using a chi-square test. We compared question four which asked for a level of agreement to the statement, "I would consider my social media network (all of the people I am friends with/mutually follow on social media/have on Snapchat/etc.) to be large" and question five, "How often do you share personal information about yourself on social media? (Tweeting, posting pictures, using tracking features on social media platforms such as SnapMaps, announcing achievements, etc.)". We compared those who indicated "strongly agree" or "agree" to having a large network, to their answers on how often they post, which we expected to not be frequently. However, the value of p is .448545, meaning the result is not significant with $p < .05$. Of the 26 participants who indicated "agree" or "strongly agree" to having a large network, only 34% of them indicated that they posted "rarely" or "very rarely". The researchers cannot assume that there is a relationship between network size and frequency of posting.

We also compared those who indicated "strongly agree" or "agree" to having a large network to question three which asked if participants' social media profiles were private, public, or a mix of both. The p value is .461131. The result is not significant at $p < .05$. There is no significant relationship between frequency of posting and privacy settings of social media accounts. With these results, we accept the null and reject the hypothesis that individuals with larger social media networks will protect their profiles and disclose less private information.

DISCUSSION

For this research, we referred to Sandra Petronio's Communication Privacy Management theory to illustrate our hypotheses. This involves the idea that people have a right to control the amount of private information that they choose to disclose. If someone were to reveal private information to someone, they would retroactively become co-owners of the information. If no mutually agreeable privacy rules are met, the trust between the two parties will be broken.

Sandra Petronio's privacy management theory is broken down into three key systems. The first being privacy ownership, which deals with privacy boundaries. The privacy boundaries have sensitive, private information that only the user can and should have access to. The user knows they have it and it exists, but others don't know about it. Privacy control is the second part of the system and it involves the decision to share private information with another person. When you make the decision to self disclose, you also endure all of the risks that go along with that decision. Risks could involve identity theft and a loss of control of private information. Petronio considers this to be the driving force and the engine of the model, because the user has the complete control to use their decision making skills. What would a certain individual decide to disclose vs not disclose, and what are the possible consequences and ramifications of that decision? Privacy turbulence is the third system of privacy management and comes into play when there is a problem with the original plan. If something happens within your privacy setting that is unexpected, it is during this time that we see the five principles at play. People believe that they have a right to control their private information. Our research supports this privacy turbulence data. The main aspect respondents want control of is their private, disclosed information. Problems can arise when those aspects of our freedoms are threatened. Once there is an understanding of the individual, then the decisions and personal privacy protection behaviors

can be studied. Some other factors that may determine why a person makes the decisions that they do are culture, gender, motivation, context, and risk-benefit ratio. Since many of the participants come from the same background and culture, that factors into one's personal privacy management online, and why many of our correspondents demonstrated a similar way of thinking and responding to these challenges.

In our research, we presented a short video about how information and data is being collected and used. We specifically looked at questions 1-5 of the pre-test and post-test, both sets of questions correspond with each other. Each question had the significant result of $p < .05$. Question one's value of p is .00001, question two's value of p is .000031, question three's p is .000877, question four's value of p is .000271, and question five's value of p is .000257. These values have allowed us to determine that our hypothesis in regards to personal data privacy usage is valid. However, in an article study conducted by Sunil Hazari and Cheryl Brown, the researchers sought to test the knowledge of respondents' attitudes towards privacy awareness. After analyzing the data from the respondents, the researchers were unable to find a significant change in attitude towards information privacy concerns. Counter to Hazari and Brown's research, our results indicate that respondents do take greater awareness of social media privacy after they became educated on social media practices. We achieved our desired outcome of increasing awareness due to our survey providing proper guidance to the participants through our questionnaire and video demonstration.

In question six of the post-test, 72% of our respondents indicated an awareness of data privacy on social media platforms. This level of awareness indicates that individuals are becoming increasingly more aware of their information being stored and leveraged on social media. These statistics are aligned with Ludwig Slusky and Parviz Partow-Navid's research

article on “Information security practices and awareness” (2012). This research indicated that although people are aware of data privacy the major problem is due to a lack of applying this knowledge in real world situations such as phishing scams and ransomware tactics. Our research indicates that after being made aware of social media privacy, the respondents indicated a heightened level of awareness.

As the number of social media platforms increase and expand the overall usage of these technologies continues to grow. Through our survey, we determined that of the 39 respondents, 100% of the respondents indicated that they leverage social media regularly in their life. According to the article titled “Trends in U.S. Adolescents’ media use” social media usage in high school seniors has increased dramatically from 50% in 2008 to upwards of 82% in 2016 this percentage has surely increased through the year of 2022.

In question nine of the survey we focused on preventing unauthorized access to personal information. Surprisingly, respondents indicated overwhelmingly that they are very concerned about the level of protection for their personal information. Although the usage of social media platforms is increasing, the lack of protection of private data does not seem to be a deterrent to its usage. The Privacy Jungle (Bonneau & Preibusch, 2010) indicates that social media providers are making major efforts to implement privacy enhancing technologies in their platforms. Although major efforts are being made, social media platform owners are not advertising these technological advances or monetizing the security enhancements that they are making.

In our survey, participants were asked if they are concerned that social media site databases that contain their personal information are not protected from unauthorized access. 62% of the respondents agreed that they are concerned, demonstrating a changed belief and sometimes a changed behavior regarding social media usage. This survey data corresponds to

Petronio's claim that people aren't willing to disclose their personal information when they aren't in control of the information.

Limitations

There are a few limitations to this study to consider. Although there weren't any other requirements for participation aside from attendance at the university, the sample size will be fairly homogenous. Many of the students have similar religious backgrounds and are of the same age demographic (18-22 years). With a sample that is both small in number (39 participants), and narrow in demographics, the results from this study will not be able to be generalized to a larger population, despite any statistical significance found from the results of the experiment. A larger sample size with a broader range of participant demographics is required in order to make supported conclusions.

Additionally, we are relying on participants to self-report their behavior and attitudes regarding social media use and privacy concerns. Due to this self-reporting aspect of the study, the results may be somewhat less reliable than observed social media use. Nonetheless, the self-reporting will give insights on the participants' attitudes and behaviors. Another limitation is that we will only be surveying for immediate changes in concerns over privacy on social media; We aren't measuring if the participants change their behaviors on social media following completion of our study, to see if the video had any influence over their actions.

Suggestions for Future Research

The results and formatting of this survey shows that more extensive research can be done. Studies conducted in the future should be formatted in a way that will allow for a larger sample size. With only 39 participants, the results cannot be applied to a general population. One

disadvantage we experienced was the formatting of the Privacy and Social Media video before the post-test. 11 of our participants completed the pre-test but didn't complete the post-test after watching the video. Having a clearer path for participants to follow to ensure they complete the entire survey would prove beneficial for gathering more responses to analyze. Similarly with the formatting of the test, administering the post-test at a later date could be beneficial in observing if the video had any lasting effects on participants' attitudes regarding privacy and actions on social media.

CONCLUSION

As the world continues to change, the role of technology and social media continues to expand. Technology and social media impact the daily lives of the vast majority of people in our society. As the role of social media expands, the critical need for enhanced security and privacy protection have grown. The need for data and privacy protection has never been greater. Although we currently have immense security and privacy challenges, individuals often are not protecting themselves or their data online.

Our group has performed a robust study on internet privacy and individuals personal habits towards securing their data and actions online. During our study, we administered a detailed electronic survey that enabled us to gather key information on the habits and actions that individuals take while interacting with social media. Our approach for administering the survey gave clear data that people are generally aware of privacy concerns, but they take stronger actions after understanding the security risks of self-disclosure and personal sharing online. Upon entail questioning, respondents were somewhat passive in their privacy responses. After watching a short video that raised awareness of social media security flaws, survey respondents expressed a deeper concern for their privacy online. Although the results of our survey supported

our initial theory that there will be a change in concern upon being aware of privacy details, a larger sample size could further solidify our theory. Our secondary theory of greater social media security awareness for individuals with larger social footprints was inconclusive as our questionnaire did not probe deep enough in order to fully support this theory. Technology and social media are playing increased roles in our society, it is critical for individuals to raise awareness and protect themselves online.

REFERENCES

1) Agosto, D. E., & Abbas, J. (2017). "Don't be dumb—that's the rule I try to live by": A closer look at older teens' online privacy and safety attitudes. *New Media & Society*, *19*(3), 347–365. https://doi.org/10.1177/1461444815606121

2) Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: insights from panel data. *Communication Research*, *48*(7), 953–977. https://journals.sagepub.com/doi/full/10.1177/0093650218800915

3) Bonneau, J., & Preibusch, S. (2010, July 21). *The privacy jungle:on the market for data protection in Social Networks*. SpringerLink. https://link.springer.com/chapter/10.1007/978-1-4419-6967-5_8

4) Cain, J. A., & Imre, I. (2021). Everybody wants some: Collection and control of personal information, privacy concerns, and social media use. *New Media & Society*, *24*(12), 2705–2724. https://doi.org/10.1177/14614448211000327

5) Hazari, S., & Brown, C. (2013). An empirical investigation of privacy awareness and concerns on social networking sites. *Journal of Information Privacy and Security*, *9*(4), 31–51. https://doi.org/10.1080/15536548.2013.10845689

6) Hollenbaugh, E. E. (2019). Privacy management among social media natives: An exploratory study of Facebook and Snapchat. *Social Media + Society*, *5*(3). https://doi.org/10.1177/2056305119855144

7) Krämer, N. C., & Schäwel, J. (2019, August 12). Mastering the challenge of balancing self-disclosure and privacy in Social Media. *Current Opinion in Psychology*. https://www.sciencedirect.com/science/article/pii/S2352250X19301265

8) Lavin, M. (2006). Cookies: What do consumers know and what can they learn?. *Journal of Targeting, Measurement and Analysis for Mark*eting, *14*, 279–288.

9) Lewis, K., Kaufman, J., & Christakis, N. (2008). Taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication, 14*(1), 79-100. https://academic.oup.com/jcmc/article/14/1/79/4582967#104147704

10) Liang, H., Shen, F., & Fu, K. (2017). Privacy protection and self-disclosure across societies: A study of global Twitter users. *New Media & Society, 19*(9), 1476–1497. https://doi.org/10.1177/1461444816642210

11) Pierson, J., & Heyman, R. (2011, September 27). *Social media and cookies: Challenges for online privacy*. https://www.emerald.com/insight/content/doi/10.1108/14636691111174243/full/html

12) Ruleman, A.B. (2012), Social media at the university: a demographic comparison. *New Library World*, *113*(7), 316-332. https://doi.org/10.1108/03074801211244940

APPENDIX

Figure 1:

Pre-Test Questions:

1. What social media platforms do you use on a daily basis?
2. How many hours per day do you use social media? List the time for all those that apply to you.
3. Are your social media platforms public or private? If there is a mix, indicate which ones are set to private and which ones are public.
4. I would consider my social media network (all of the people I am friends with/mutually follow on social media/have on Snapchat/etc.) to be large.
5. How often do you share personal information about yourself on social media? (Tweeting, posting pictures, using tracking features on social media platforms such as SnapMaps, announcing achievements, etc.)
6. How aware are you about how your information is being collected and stored on social media platforms?
7. How much concern do you have about your privacy on these social media platforms?
8. I am concerned that social media sites are collecting personal information about me.
9. I am concerned that social media sites do not devote enough time and effort to preventing unauthorized access to my personal information.
10. I am concerned that social media site databases that contain my personal information are not protected from unauthorized access.
11. Before moving on to the post-test, please watch this video for more information regarding social media privacy. *Video shown here*

Post-Test Questions:

12. How aware are you about how your information is being collected and stored on social media platforms?
13. How much concern do you have about your privacy on these social media platforms?
14. I am concerned that social media sites are collecting personal information about me.
15. I am concerned that social media sites do not devote enough time and effort to preventing unauthorized access to my personal information.
16. I am concerned that social media site databases that contain my personal information are not protected from unauthorized access.