A Comparative Social Media Study: Are applications with self-deleting features the new preference?

Gabe Hobeika, Audasia Ho, Vibha Iyengar, Eileen Jiang, Yuankun Li
Carnegie Mellon University

ABSTRACT

Applications designed for social media that use "self-deleting" features allow users to post content that automatically gets deleted after a certain amount of time, as opposed to more traditional applications that keep content online by default. We are interested in studying how applications that have "self-deleting" features affect users' decisions to post certain content, compared to more common applications. We narrowed down our study to Snapchat, a popular social media application with a default "self-deleting" feature for all its content, and Facebook, another widely used application that permanently keeps content online. Our study analyzes the different ways people use these applications by having them participate in a two-part study. This study looks at their decisions to specific compromising scenarios and tests their ability to control their privacy settings. Our results suggest that the majority of participants feel more secure about content posted to applications with "self-deleting" features, leading them to trust them more and share more compromising content.

1. INTRODUCTION

In the past decade, the use of technology to maintain an online presence has led to an increasing reliance on social media as a means to keep in touch with our friends and acquaintances. With this online presence comes concerns over what content we decide to share and what we decide to keep private. Many applications now offer a "self-deleting" feature that allows users to share content to their friends, but only for a brief period, after which the application will delete the content. This content normally takes the form of text messages, photos, or videos. Snapchat, a popular social media application, allows users to send photos and videos to specific friends for a predetermined amount of time, normally a matter of seconds. Snapchat also allows its users to add the content to their stories, which is a daily record of a user's day. By default, Snapchat will delete the content on a user's story after twenty-four hours. In contrast, Facebook, lets users post statuses, photos, and videos, and keeps the content unless the user explicitly deletes it.

The different lifespans of content on each platform can affect the type of content that users decide to share. For users that consistently use both Snapchat and Facebook, knowing that Snapchat will delete shared content can make users more bold about sharing content that they normally would not share on Facebook. They might be more willing to share compromising photos or messages to their friends on Snapchat than to permanently post that content to their Facebook Timeline because they believe that no record of the compromising content will be saved anywhere. Even though recipients on Snapchat can save a screenshot of shared content, Snapchat notifies the sender, which could lead to the sender sharing less compromising content to that recipient in the future. Thus, Snapchat fosters a culture of allowing friends to view snapshots into users' lives for brief periods of time, whereas Facebook creates a more traditional culture of allowing friends and acquaintances to view shared content at any point in time. The creation of this kind of culture on Snapchat can lead users to believe that their shared content is more private and more secure than it really is.

Our two research questions are targeted around understanding how users decide what kind of content to share on Snapchat or Facebook, as well as analyzing how much users really understand their privacy settings on both platforms. We would like to investigate whether the presence of a "self-deleting" feature in social media applications impacts the type and amount of content users share on these applications. We would also like to investigate whether users' perceptions of their privacy settings match the actual behavior of their privacy settings.

To help us answer these research questions, our hypotheses are focused on predicting how well users can control their privacy settings, as well as how they react differently to content posted on Snapchat and Facebook. We believe that users tend to share content more frequently on self-deleting social media than they do on traditional social media. We also hypothesize that users are not always aware of who can see their content and where they can modify these settings. In addition, users are not always aware of how and where they can restrict their privacy settings. Finally, we believe that users perceive that their privacy settings are more restrictive than they actually are.

Our paper starts off with some background on the current research and analysis on applications that use "self-deleting" features. We then describe our methodology for our two-part interview, in which we ask about how participants decide what kind of content to share on Snapchat and Facebook, as well as how well they can modify their privacy controls on both applications. We then discuss the results of our study and perform qualitative analysis on the responses gathered from participants. We end by discussing future work and how our study could be improved.

2. RELATED WORK

Self-deleting applications have become very popular in the last year, and Snapchat is one of the most popular ones [15]. There are multiple papers which exclusively discuss how self-deleting applications like Snapchat encourage users to post more compromising material than ones without this feature, such as Facebook. Jennifer Charteris mentions that young adults are the most influenced age group, who at times post intimate photos and engage in intimate behavior [2]. Thus, we decided to focus on college students aged 18 years and above (the most relevant age group) in our study. Enabling two-factor authentication, communicating only with confirmed friends, maintaining privacy settings, and taking note of screenshot notifications are some of the tips provided to Snapchat users [10], but there is the question of whether or not users know about it and use it.

2.1 Nature of ephemeral design

There has been much research on the nature of ephemeral design. In Bin et al., researchers interviewed Snapchat users to explore user behavior on Snapchat [18]. They found that users of Snapchat enjoy the platform because it prevents the accumulation of meaningless and potentially embarrassing content. Meanwhile in Onwuzurike et al., researchers analyzed applications that claim to be anonymous, ephemeral, or had end-to-end encryption [11]. They found that many of these applications were not as secure as they claimed they were, with data being able to be intercepted and decrypted. For Snapchat, researchers found that expired messages are not always deleted from their servers; in fact, some of these "expired messages" would be transmitted in packets set from the server to the client. This is notable because a key feature of Snapchat is the ephemeral nature of the content, which leads to privacy concerns if messages that were thought to be expired were existing and transmitted. Guolao et al. exposes the fact that the messages sent by Snapchat and other self-deleting services may not be truly hidden from other parties and are not really encrypted [6]. Researchers state that 25 percent of respondents to their survey have sent sensitive content via Snapchat. They also found that user behavior would have been different had they known the message destruction is not 100 percent guaranteed. Thus, in our study, we are interested in comparing users' Snapchat usage with Facebook usage to see if they behavior differently due to the ephemeral nature of the content.

2.2 Users' view of privacy and security

It is well documented that social media users do not limit themselves to one account, but tend to use different social media accounts for different purposes. Users may also have different views of how their privacy is preserved as opposed to how their data is actually used. In one case, Zimmeck used machine learning to look at privacy policies of 17,991 android applications [20]. He found that the applications show potential privacy inconsistencies, thus, some users may be misled in their beliefs about ephemeral social media. Through interviews, Zhao et al. researched how social media users managed different accounts and assessed what social media accounts to share content on [19]. They found that users consider "audience" and "content" when deciding which account they should post content to. Researchers found that users use different sites for different purposes. We also explored this same area to determine how users use social media applications differently. A few studies have emerged about the usage of Snapchat and the security of a user's content on Snapchat. Roesner et al. surveyed Snapchat users about how and why they use Snapchat [14]. They found that many Snapchat users do not use Snapchat to send sensitive content and that the use cases of Snapchat far outweigh the possible security and privacy concerns. However, they also found that a good portion of users would change their behavior on Snapchat after finding out about Snapchat's lack of security. As this study was a survey, there is the possibility of user's not wanting to disclose if they use Snapchat for sensitive content. Thus, users may not have been truthful in their responses on not being as concerned about the security of Snapchat. Furthermore, users tend to estimate that they are more security conscious than they actually are, leading to users stating that they would change their behavior. This study helped us see how Snapchat users view privacy and security on the application and helped us frame our questions to users about their privacy settings on Snapchat.

2.3 Users are not always wrong

Sometimes, it is also the mechanisms used in the system, which make the usability or facility difficult. Palande et al. found that the data used in self-deleting applications, which are stored in cloud platforms, face synchronization problems while being distributed, copied, and deleted [12]. Another study by Liu measured users' privacy preferences about Android permission systems, after which the author states that the default privacy mechanism is not very usable [9]. As part of this study, an effective permission recommendation system was built, which succeeded in changing most users' attitudes regarding their privacy. One must understand the usability concerns in an application and mend it as per requirement. Paul and Strufe built a new Facebook privacy setting interface, which proved to be more usable than the one currently existing [13]. These works motivated us to dig deeper into users' perspective about their privacy settings and their data retention on server.

2.4 Reassurances to users

Self-deleting applications claim to be more secure and private, but do these applications use more secure systems to implement the self-deleting feature? Vanish, self destructing digital data, utilizes a distributed hash table (DHT) to make sure that the key used to encrypt data is spread across hundreds or thousands of nodes in different geographic locations that, over time, become impossible to recover due to internal

DHT churn. At that point, the data is deleted since the key used to encrypt the data is impossible to re-obtain [5]. Cascade, a hybrid system for self-destructing data, is another such example that requires breaking into every single one of its key-storage components to violate privacy. Whereas a security system is often described as a system that is as secure as its weakest link, Cascade aims to be as secure as the union of its defenses [4]. Inclusion of systems like Vanish and Cascade help increase the security and trust that people have in applications with self-deleting content, which further reassures users that their privacy may be preserved on Snapchat as opposed to Facebook.

2.5 Privacy concerns vs. Impression management

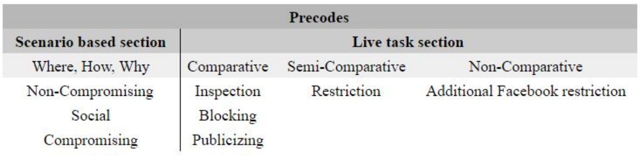
We found strategies which could help developers make privacy more user friendly and efficient based on users' characteristics. Broeck et al. attempted to understand the straightforward relationship between privacy concerns and impression management and found that the user engagement in these strategies involves several contextual factors such as age, sex, online skills, and network diversity. The statistics show that when more people join social networking sites and begin sharing personal information, the need to create customized privacy features becomes paramount [3]. Vitak conducted a study focusing on vulnerable internet users, like children and adolescents, and studied how privacy concern and the application of privacy settings on Facebook could be linked to Erikson's three stages of adulthood: emerging, young, and middle adulthood [17]. The results from this study indicated that although older age groups have higher privacy concerns, compared to emerging adults, who have a pragmatic approach to online self-disclosures, it was evident that younger adults had more knowledge of privacy protection settings and use these settings more frequently compared to the older adults. An article about Confide and TigerText, two self-destructing applications in the business domain, covers two main concerns, exposure of company data in case of a Snapchat breach and dealing with laws that require a company to retain their communications or documents [16]. Isajiw and Del Giudice also raised spoliation concerns when businesses use self-destructing applications like Cyber Dust and Snapchat [7]. Since self-destructing messages leave no documentary evidence about the conversation, the authors suggests that the law should treat self-destructing message communications like phone calls or face-to-face communications, not email communications, and define laws accordingly. This introduces a question of if privacy settings should be designed differently for personal and professional usage, and whether there should be external control over these settings in case of pending litigations.

2.6 Study methods used

We reviewed several papers to understand various usability study methods that have been employed. In "Why Johnny Can't Opt Out," an article that looks at the usability of several online privacy tools, researchers interviewed 45 participants in a 90 minute lab study, where they had participants go through several scenarios using online privacy tools [8]. In Bayer et al., researchers interviewed college students who used Snapchat [1]. They ran a two week data collection study to gather information on participants' mood and other social factors when they used Snapchat. Our study used a mix of both these approaches where we conducted scenario based interviews. We recruited active users of Snapchat and Facebook in order to draw results about their knowledge and habits on the applications.

3. METHODOLOGY

We conducted in-person semi-structured interviews, after receiving approval from the Carnegie Mellon University IRB in late April 2017. Participants were recruited via on-campus flyers advertising our voluntary study on Snapchat and Facebook. We first asked demographic questions allowing us to determine what social media applications the participants used, and how often they used both Snapchat and Facebook. Scenarios were then proposed to each participant to gauge how they would use their social media to broadcast those scenarios to their friends. Lastly, each participant was given a dummy Facebook and Snapchat account to use for think-aloud tasks centered around the privacy settings of the two applications. After the study, we used qualitative analysis techniques to aid our understanding of the data.



Precodes			
Scenario based section	**Live task section**		
Where, How, Why	Comparative	Semi-Comparative	Non-Comparative
Non-Compromising	Inspection	Restriction	Additional Facebook restriction
Social	Blocking		
Compromising	Publicizing		

Figure 1: The Study Pre-codes

3.1 Scenario-Based Interview

The first part of our study involved asking our participants different scenario questions to address our first research question. We thought of scenarios that were either non-compromising for a user, part of regular social interaction, or compromising scenarios. These resulted in six scenarios proposed to the participants of this study. Each scenario was based around one theme, with questions asked about if and how they would share information about that scenario to social media. Figure 2 illustrates the list of scenarios, their category, their corresponding labels, which are later used in Figure 4.

3.1.1 Scenario 1

This was focused on if a participant got a new job, and how they would share this information on social media. This was thought of as a non-compromising scenario that would allow us to gauge how the participant typically uses their social media. We hypothesizes that most participants would share this information to both Snapchat and Facebook, although they may possibly post different types of content to both.

3.1.2 *Scenario 2*

This revolved around a trip abroad, which allowed us to explore a spectrum of social media posts that a participant could make. This scenario was another example of a non-compromising scenario if participants felt that social media posts about vacation would not affect them in negative ways.

3.1.3 *Scenario 3*

This was based around the participant having a bad day at work. This scenario was slightly compromising, as the participants were asked about sharing sensitive material, like how they felt towards their work, on social media. This scenario allowed us to potentially gauge when users would use self-deleting features to preserve their privacy.

3.1.4 *Scenario 4*

This was a social-based scenario about interactions on a friend's birthday. This scenario had both compromising and non-compromising aspects in order to see how they impacted a participant's decisions on social media posts. Posting birthday posts on Facebook is generally acceptable behavior, however showcasing drinking at a club and a bar may be somewhat compromising to future employment.

3.1.5 *Scenario 5*

This was another social-based scenario about a day at the beach. It also included some acceptable behavior, such as hanging at the beach with one's friends, and some unacceptable behavior such as building an illegal bonfire on a beach. Similar to the birthday example, it allowed us to explore how the different types of social media are used over the course of the same event.

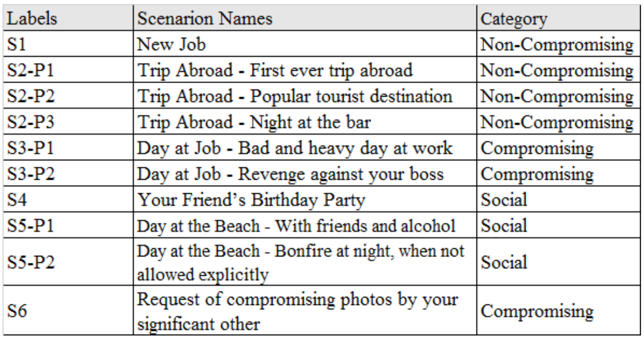
3.1.6 *Scenario 6*

This was a wholly compromising scenario based around sending compromising photos to a participant's significant other, and what platform they would use. This allowed us to understand explicitly what participants would do with compromising material, and if they would try to leverage self-deleting features when sharing compromising content.

3.2 Live Tasks

After going through the scenarios with participants we then began a series of live tasks that looked at our second research question. The live tasks explored the privacy settings of both Facebook and Snapchat to gauge whether participants could achieve their desired levels of privacy if they wanted to. We broke these live tasks down into categories to allow us to properly compare the two applications.

We first gave participants comparative tasks. These tasks had users going through the privacy settings of both Facebook and Snapchat, where the settings had comparable functions on both applications. Users would inspect their privacy settings and see if they understood what those settings meant. Then, the participants would check their blocking settings and would also block test users to see if they understood how blocking and unblocking mechanisms worked. Participants were also asked to open up their accounts to the public, to see if they understood how each application allows its users to broadcast to a wider audience.



Labels	Scenarion Names	Category
S1	New Job	Non-Compromising
S2-P1	Trip Abroad - First ever trip abroad	Non-Compromising
S2-P2	Trip Abroad - Popular tourist destination	Non-Compromising
S2-P3	Trip Abroad - Night at the bar	Non-Compromising
S3-P1	Day at Job - Bad and heavy day at work	Compromising
S3-P2	Day at Job - Revenge against your boss	Compromising
S4	Your Friend's Birthday Party	Social
S5-P1	Day at the Beach - With friends and alcohol	Social
S5-P2	Day at the Beach - Bonfire at night, when not allowed explicitly	Social
S6	Request of compromising photos by your significant other	Compromising

Figure 2: List of Scenarios and their categories

We then gave participants semi-comparative tasks, to see if users understood how to stop people from adding their Facebook and Snapchat accounts when they did not want them to. Snapchat does not have a mechanism to do this, but we still asked users to do this to observe if participants knew that this was not truly possible.

Finally we had non-comparative tasks centered around Facebook -specific functionality such as preventing people from writing on your wall, tagging you in photos, and enabling content review. These tasks gave us a bit more insight into how people understood their Facebook privacy settings.

3.3 Qualitative Analysis

After finishing our study, we qualitatively analyzed our gathered data. We focused this analysis on coding the responses to the scenarios and the responses to the live tasks. This allowed us to compare whether tasks were easy or difficult between participants and how participants thought through the scenarios that were proposed. We used the pre-split categories that we thought of when developing the scenarios to help us code the results. We used also used the categories and subcategories of our live tasks to help us code the results from participants. This analysis gave us a qualitative understanding of how users use their social media accounts and if they understand how to maintain their privacy on them.

4. RESULTS

4.1 Demographics

We recruited 8 participants for our study, ages 21-25. Figure 3 shows the gender distribution among the participants, 3 were female, and 5 were male. We found that all the participants used Facebook a few hours more than they used

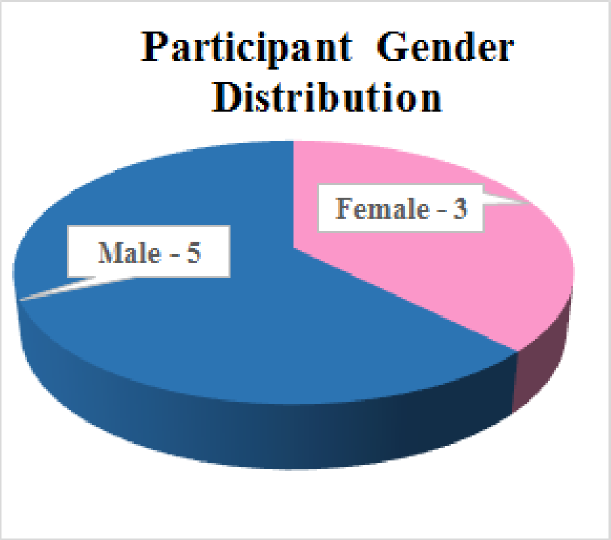


Figure 3: The Study Demographic

Snapchat on a daily basis. All participants were affiliated with Carnegie Mellon University.

4.2 Scenario-Based Interview

We had three different categories for our scenarios, non-compromising, social, and compromising. Each scenario also included sub-scenarios that would differ in the details of the scenario. In general, participants tended to make posts on their social media for non-compromising and social scenarios. Participants also did not want to share content on social media in compromising scenarios as shown in Figure 4a. Over all scenarios, an average of 4.5 participants would post on social media, 2.9 would not post on social media, and 0.6 might post on social media. Every participant had different reasons for either posting or not posting on social media. A participant stated that if a trip was interesting, they would take some pictures and post them to social media. Another participant explained that they would not post on Facebook during their trip, and would post an album of all of their "high quality photos," taken with their DSLR camera, at the end of the trip. This participant stated that they would post on Snapchat during the trip, but it would be "casual things, like if I was eating something."

We also found significant differences in participant behavior between non-compromising scenarios and compromising scenarios. In non-compromising scenarios and social scenarios, an average of 5.43 participants would post content on their social media. However, in compromising scenarios, only an average of 2.33 participants said they would post content on social media. In compromising scenarios, several participants conveyed their concerns about their reputations. One participant stated that, "I have people from work added on Facebook, they do not need to see me going out and partying."

Between Facebook and Snapchat, more participants preferred posting content on Snapchat. Within the 10 sub-scenarios we asked participants, we found that in 8 of the scenarios participants would be more likely to post on Snapchat. Only for the scenarios of getting a new job and first trip abroad would participants be more likely to post on Facebook, as shown in Figure 4c. Our results also show that participants would use different methods to share content based on the scenarios. For non-compromising and social scenarios, participants preferred to make a Facebook post and post content on their Snapchat story, which are more public than other ways of posting content on social media. However, for compromising scenarios, if participants would share the content, they would use direct messages to send it to a limited number of friends as illustrated in Figure 4b. One participant stated that they were more willing to send compromising content through Snapchat, because "I know that it will go away after a couple seconds, plus I will know if someone

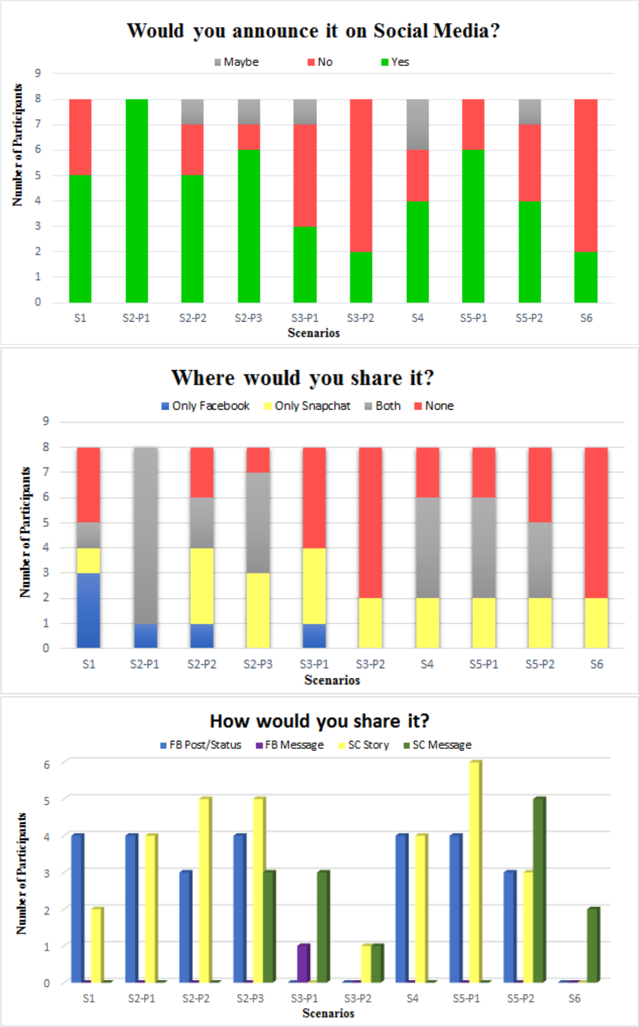


Figure 4: Distribution of participant choices in multiple scenarios for - a) Whether they will announce the information on Social Media, b) Which application would they prefer to do so, c) How would they share it

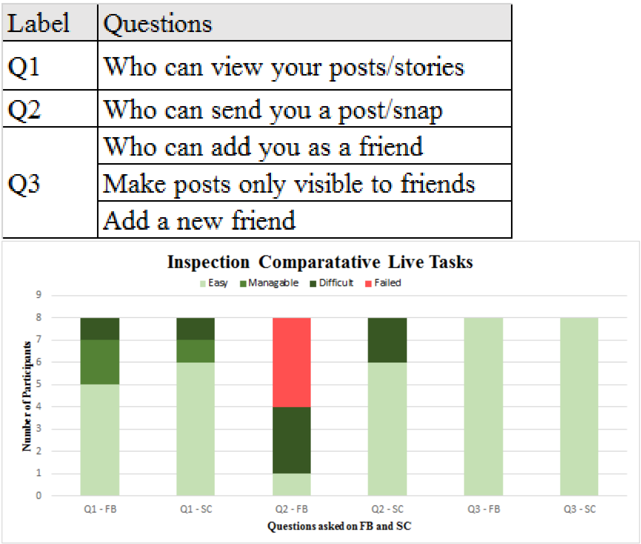
decides to screenshot it." We also found that privacy was not the only reason participants would choose Snapchat to send content. Some participants felt that Facebook is a summary of life, so more people are able to see their posts. Snapchat on the other hand is more private, and the friends they have on Snapchat tend to be close friends. One participant stated that the would post content more frequently on Snapchat, as "no one on Facebook cares to see my day to day, but I want to share what I'm doing with my friends on Snapchat." In compromising scenarios, although a majority of participants said they would not post anything on social media, among those who would post content, only one participant in one scenario was willings to post on Facebook. One participant who would post on Snapchat said he chose Snapchat because Snapchat would delete his posts in the future. In this case, we found that the self-deleting feature had influence on participants' attitudes towards social media.

Participants would also post different types of content on different social media. In general participants would share more formal things, such as higher quality photos, offer letters, and company logos on Facebook. For Snapchat, many participants said they would post casual and random photos to their Snapchat. For the job offer scenario, one participant stated that they would post on Facebook and Snapchat, and said, "I would probably make a life event for this, and then change my future job status; but on Snapchat I would post a picture of my letter along with a caption and send it to my friends."

4.3 Live Tasks

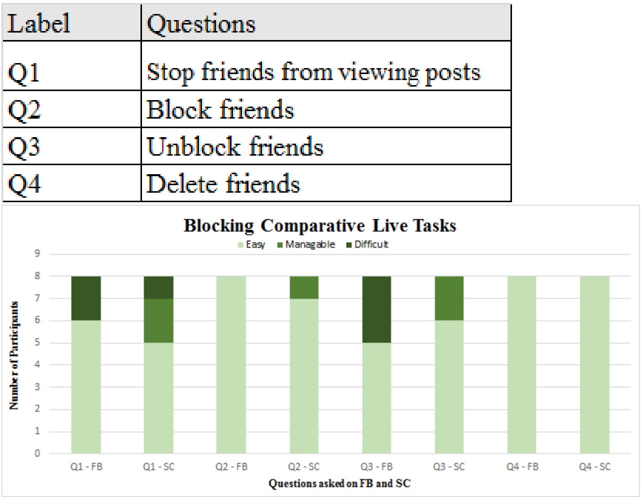
In general, our participants performed well on live tasks. The successful rate for all of our tasks is 97.5 percent. We also found that participants could finish most of their tasks easily, as they were able to navigate through the privacy settings relatively quickly, with little input from the interviewer.

For our comparative tasks, participants tended to perform better on Snapchat. 83 percent of the Facebook tasks were easily completed, whereas 88 percent of the Snapchat tasks were completed easily. However, participants' performance varied depending on the type of setting. Figures 5 and 6 shows the distribution of difficulty levels in each of the tasks given to them. Participants had better performance on Snapchat for inspecting the settings, whereas for both blocking and publicizing participants had similar performance on Facebook and Snapchat. This could be because of the differing complexities of privacy settings menus on the applications. It was interesting to note that for both applications participants did not always understand how blocking worked. When they were tasked with unblocking a user, many participants assumed that they would be able to find the user in their friends list, not understanding that blocking a user meant they were no longer your friend. One participant was able to easily block and unblock a user, and they explained that it was because they had blocked someone previously. In our semi-comparative tasks and non-comparative tasks, our live tasks covered functions that were not frequently used by most participants. Thus, participants tended to do worse on these tasks; only 66 percent of attempts were easily completed, with many attempts taking a long time to complete or never being completed.



Label	Questions
Q1	Who can view your posts/stories
Q2	Who can send you a post/snap
Q3	Who can add you as a friend Make posts only visible to friends Add a new friend

Figure 5: Distribution for inspection comparative live tasks



Label	Questions
Q1	Stop friends from viewing posts
Q2	Block friends
Q3	Unblock friends
Q4	Delete friends

Figure 6: Distribution for blocking comparative live tasks

We found that several settings on Facebook or Snapchat are difficult for many participants. In the comparative tasks, several participants had difficulties finding who can view their posts, and who can send them messages. However, once a participant stumbled upon the right menu, they were able to easily understand the privacy settings. On Facebook, half of the participants were unable to find who could send them messages, as there was no setting that explicitly addressed that case. Users had to extrapolate and understand that people that could add them on Facebook were the same people who could message them on Facebook. On Facebook, half of participants had difficulties making their walls postable to only themselves and 25 percent of participants had difficulties making their accounts not searchable by search engines. On Snapchat 75 percent of participants had difficulties making their accounts addable by only phone contacts, not realizing that this functionality is not included in the Snapchat privacy settings. Participants were not always aware of what was and was not possible, and would attempt to find settings thinking that they should exist. One observation that we made was that almost all Facebook tasks were completed through the same sequence of events, with participants going to the list of all settings and finding privacy settings. The centralized menu was useful for the participants who knew how to navigate to it, but for participants who had never used the settings pages, it was difficult to find. On the other hand, participants on Snapchat would attempt to find the privacy settings through many different means, and it was interesting that many users would stumble upon the privacy settings at some point, and would continue using that entry point to access the settings. Thus, not all users would access the Snapchat settings page through the traditional means of swiping down and clicking on the gear icon.

5. DISCUSSION

Due to time constraints for this project, we were unable to modify our study a significant number of times or recruit a significant number of participants. Treating this study as a pilot for a future research project, however, is very valuable due to the lessons that we learned throughout the study.

While analyzing and discussing our results, we realized we missed an essential set of demographics questions that we would have asked given the chance to refactor our study. We would have asked how many friends each participant had on each platform and some qualitative questions about their friends such as whether they were their parents, relatives, work colleagues, etc. These questions could have given us further insight into why people share the content that they do based on audience.

If we were pursuing this research further, it may also be advantageous to structure some of the survey questions to probe deeper into the preliminary results we gathered throughout this project. Specifically, we might want to tailor some questions to get further information on the apparent usage of Facebook as a record of life. We would also like to narrow down the scope of our Snapchat questions to see if we can show that people use Snapchat as a way to broadcast content to their close friends.

In addition to gathering more participants for more data, we would also want to diversify our participant pool. Specifically, the pool of Carnegie Mellon students and associates that we studied may be less willing to share compromising content than the general public. It may help us understand how other populations share or tend to use social media in regards to compromising situations outside of our university.

Even though there were some significant limitations in our project, we were still able to gather good preliminary data upon which future research can build. We feel that further comparative studies between Facebook and Snapchat may be useful in understanding what people actually "want" from their social media applications.

6. CONCLUSION

From our eight participants we are able to conclude some useful points based on our scenarios and live tasks. Two of our hypotheses being that users are not always aware of who can see their posts and where that can be changed and that users are not always aware of how and where they can restrict their privacy settings seem to be incorrect. Almost all of our live tasks were completed by subjects, and the large majority of the tasks were completed easily. This hints that Snapchat's and Facebook's privacy settings are easy to digest for young, daily users, but further research needs to be done to see if this conclusion applies to a more general population.

We were also able to draw some conclusions about the nature of how people perceive self-deleting social media when compared to normal media. Specifically, our compromising scenarios showed that our participants were not likely to share compromising information about work or risque pictures. They did, however, tend to mention comments such as they would use snapchat specifically because "it deletes." This shows that people perceive self-deleting to be effective, and could hypothetically be used to share compromising content. Once again, a more general population study may be useful in ascertaining whether this is a general feeling among the public or whether our results were biased by having career-conscious CMU students as our primary subjects.

We do not think that we adequately addressed our demographics questions in the first part of the study. Given the chance to refactor the study, we would include questions to ask about how many friends each participant had on the respective platforms. These questions would give us vital information that may shed light on why some of the participants felt that Snapchat was for their close friends and friend-to-friend interactions. We also needed to develop a study mechanism that allowed us to ask people about their privacy settings specifically. Our study showed that our participants could accurately decipher and set their privacy settings when asked. However, our study showed no information about whether the participants understood their own privacy settings or whether they cared to even know their own privacy settings. In a future study, we would also like to evaluate that hypothesis in more detail.

Overall, we learned valuable insights about users' Snapchat and Facebook habits through our study. We learned about a tendency to share friend-to-friend interactions on Snapchat, and a tendency for users to use Facebook as as "record of life." We also learned that users may not be as naive as it seems when it comes to understanding and setting their privacy settings. Our study can be bolstered by further work in this field with more general populations addressed.

We also learned valuable lessons about seeking IRB approval and working with human subjects. To effectively design a study such as ours, multiple rounds of pilot studies should be done with multiple iterations on the initial study design. Our time crunch with this being a semester-long project meant that we were only able to effectively pilot two initial forms of our study, causing us to miss some key insights on demographics questions. If we were to treat this project as a pilot of a broader study, that broader study would benefit from our findings in this study.

7. ACKNOWLEDGEMENTS

We thank Dr. Lorrie Cranor for her help in teaching us about usable privacy and security and providing the prompt with which this study was conceived. We would also like to thank Abby Marsh for her aid in the completion of this study, help in formatting our research questions and hypothesis, and review of our preliminary materials. A special thanks to our Teaching Assistant, Javed Ramjohn, for his continual support and feedback. Lastly, we would like to thank Microsoft Corp for the grant which allowed us to recruit and adequately compensate our participants. Without the above mentioned people and organizations, this study would not have been possible.

8. REFERENCES

[1] J. B. Bayer, N. B. Ellison, S. Y. Schoenebeck, and E. B. Falk. Sharing the small moments: ephemeral social interaction on snapchat. *Information, Communication & Society*, 19(7), 2016.

[2] J. Charteris, S. Gregory, and Y. Masters. Snapchat 'selfies': The case of disappearing data. *Rhetoric and Reality*, 2014.

[3] E. V. den Broeck, K. Poels, and M. Walrave. Older and wiser? facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. *Social Media + Society*, 1(2), 2015.

[4] R. Geambasu, T. Kohno, A. Krishnamurthy, A. Levy, H. Levy, P. Gardner, and V. Moscaritolo. New directions for self-destructing data systems. 2011.

[5] R. Geambasu, T. Kohno, A. A. Levy, and H. M. Levy. Vanish: Increasing data privacy with self-destructing data. *Proceedings of the 18th Conference on USENIX Security Symposium*, 2009.

[6] A. Goulao, N. O. Duarte, and N. Santos. Shareiff: A sticky policy middleware for self-destructing messages in android applications. *2016 IEEE 35th Symposium on Reliable Distributed Systems (SRDS)*, 2016.

[7] P. Isajiw and A. D. Giudice. Does use of self-destructing messages raise spoliation concerns? *www.NYLJ.com*, 2015.

[8] P. Leon, B. Ur, R. Shay, Y. Wang, R. Balebako, and L. Cranor. Why johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2012.

[9] Liu. To deny, or not to deny: A personalized privacy assistant for mobile app permissions. *Symposium on Usable Privacy and Security*, 2016.

[10] E. Moreau. 10 essential privacy tips for snapchat users. *www.lifewire.com*, Dec 2016.

[11] L. Onwuzurike and E. De Cristofaro. Experimental analysis of popular anonymous, ephemeral, and end-to-end encrypted apps. *Proceedings of WiSec '16*.

[12] A. Palande, C. Rao, P. Rodi, and V. Bhusari. Self-destructing data system using shamir secret sharing algorithm. *International Journal of Application or Innovation in Engineering & Management*, 2015.

[13] T. Paul, D. Puscher, and T. Strufe. Improving usability of privacy settings in facebook. *arXiv*, 2011.

[14] F. Roesner, B. T. Gill, and T. Kohno. Sex, lies, or kittens? investigating the use of snapchat's self-destructing messages. *Proceedings of FC '16*.

[15] R. Sinha. Top 7 self-destructing messaging apps for android and iphone. *www.beebom.com*, Sep 2016.

[16] J. M. Tanenbaum. self-destructing text messages for business professionals? there's an app for that. *Nixon Peabody*, 2014.

[17] J. Vitak. Balancing privacy concerns and impression management strategies on facebook. *Symposium on Usable Privacy and Security (SOUPS)*, 2015.

[18] B. Xu, P. Chang, C. L. Welker, N. N. Bazarova, and D. Cosley. Automatic archiving versus default deletion: What snapchat tells us about ephemerality in design. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, 2016.

[19] X. Zhao, C. Lampe, and N. B. Ellison. The social media ecology: User perceptions, strategies and challenges. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2016.

[20] S. Zimmeck. Automated analysis of privacy requirements for mobile apps. *NDSS '17*.

Appendix

Facebook and Snapchat Usability and Privacy Interview Script

Introduction

Hi, ________. My name is _________, and I will be going through this interview with you today. The format of this interview will be as follows: Part 1 will be some scenarios regarding Facebook and Snapchat usage that we would like you to consider. Part 2 will be a couple usability tasks on Facebook and Snapchat accounts. Do you have any questions?

With your permission, we would like to audio record this session, as well as video record your interactions with the phone screen. We would not be video recording your face, but only the hand movements on the screen. This recording will help us remember your answers to the interview questions, as well as allow us to see how you interact with the application's interface. You can withdraw from this interview at any time. Is this ok?

I'm going to ask you to sign a consent form for us that provides relevant details about the study. Please take as much time as you need to review the form, and let me know if you have questions. If you sign the consent form, note that we have your permission to record your voice and the screen, and that the recording will only be accessible to the people working on this project. All study data that we collect will be de-identified. Note also that your participation is entirely voluntary.

Please do not say anything that is both identifiable and private about yourself or others while recording is taking place. You can skip or choose not to answer any of the questions if you do not want to answer them.

Give participant pen and consent form to read and sign.

I'm now going to turn on the voice recording with your permission.
Wait for the participant to give a verbal "yes.", and then start voice recording.

Do you have any questions before we get started?

Demographic Questions

Before we get started on the interview questions, I have a couple of quick questions for you.

First, what is your age?
Are you a regular user of Facebook and Snapchat? How many hours per day would you estimate you spend on each?

Out of the two, which one do you tend to use more often?

Thank you. Now we will move on to the scenario part of this session.

Part 1: Scenarios

Now that we've established that you use Snapchat and Facebook, we'd like to understand your usage habits between the two platforms.
I'm going to take you through a couple different scenarios. Please answer each one as realistically as possible.

Go through the following scenarios with the participant, asking them questions about their choices and decisions. Depending on their responses; ask follow up questions.

SCENARIO 1: New Job

You've just received a new job! It's an awesome job in a field that you are interested in and you're very excited about it.

- Would you announce this information to social media?
- Would you announce it to Snapchat?
  - How would you announce it to Snapchat?
  - What would you post?
- Would you announce it to Facebook?
  - How would you announce it to Facebook?
  - What do you think the post would be like?
- If you would rather keep it to yourself, why do you chose to do that?

SCENARIO 2: Trip Abroad

You're going on your first ever trip abroad. You're visiting a bunch of cool countries that you've been dreaming of going to for years.

- Would you post about this trip on social media?
- Would you post pictures of your trip?
  - Would you use Snapchat or Facebook to post the pictures of your trip?
- What sort of things would you post to Facebook?
- What sort of pictures would you post to Snapchat?

You're now on a tour on your trip of some old ruins. It is a popular tourist destination and there are a good number of friends who have posted pictures from here.

- Do you post about the tour to Facebook?
- Do you post about the tour to Snapchat?

You're now out enjoying the nightlife of the country you're in. You're at a pretty popular bar, and you've met some people there. You guys decide to take selfies and pictures together. Alcohol is visible in the photos.

- Would you post pictures to Facebook?
- Would you post pictures to Snapchat?

If you wouldn't communicate that you're on a trip, what is the reason?

SCENARIO 3: Day at Job

You're having a bad day at your new job. There are a lot of small time consuming tasks that you must complete by the end of the day. Your boss is not helping and keeps assigning you more work. You feel unfairly treated as one of your coworkers seems to have no work to do.

- Would you talk about this on social media?
- Would you post about it on Facebook?
- Would you post about it on Snapchat?
- If not, why is that?

Your boss is wearing a ridiculous tie; and you've managed to take a picture of it. You're feeling a bit annoyed at him due to all the work he gave you.

- Would you post this picture to Facebook?
- Would you post this picture to Snapchat?

SCENARIO 4: Your Friend's Birthday Party

You're at your best friend's birthday party. You haven't seen them in a couple of months and are really excited to finally go out with them. You guys decide to start at a bar and then go hang out at a club.

- Would you post about this on social media?
- Would you post about this on Facebook?
  - If so, would you post pictures or write a status?
- Would you post about this on Snapchat?

SCENARIO 5: Day at the Beach

You've decided to go the beach with some friends. Someone has brought some alcohol and everyone is enjoying it.

- Would you post pictures on Facebook or Snapchat? Why?

It gets later in the night, and you guys decide to build a bonfire, even though the beach doesn't explicitly allow them.

- Would you take pictures?
- Would you post any of them on Facebook or Snapchat?

SCENARIO 6: Compromising Photos

Your significant other has asked for compromising photos from you. Hypothetically, say there is no risk of these photos being leaked or your partner maliciously spreading them. Thus, you are willing to take them.

- Would you send them these photos?
- Would it be through Facebook or Snapchat? Why?
- If you would still not send the photos, why is that?

Thank you, these are all the scenarios we have prepared for you. Now we will move on to part 2, the live tasks on Facebook and Snapchat. Do you have any questions before we continue?

Part 2: Usability Tasks

Now we will be asking you to go through some live tasks on Facebook and Snapchat. We have a test device and test accounts here so that you don't have to use your own account. You need to assume this account as your own account, based on which you perform the tasks. I'll be turning on the screen recorder now. Is this ok?

While going through these tasks, it would be great if you could think aloud as you do them, so that we can understand your thought processes between your decisions. Please feel free to ask me any questions as you go through the tasks. I will do my best to answer them as clearly as possible.

If the questions asked by the participant would impact the study motive, we would respond by saying "Sorry I can't help with this. Please try understanding/performing it to best of your level."
Also, if a participant takes too long for a task or is unable to figure out what is to be done, we would say, "You may try for another two minutes.", and after two minutes, "You may move on to the next task."

In lieu of a recording device, ask the interviewee to talk-aloud during these tasks. Prompt them with questions such as "So what screen are you looking at now" if necessary to collect information. The interviewee at no time should be using their personal accounts; accounts will be generated by the testing team.

Initial state: Accounts used for testing should be set as public as possible before testing. The interviewee will make them progressively more private, and then more public as they can. If the interviewee cannot accomplish a task within a 3-minute time frame, the interviewer is to assist in their completion

Note that references to the accounts in the following tasks hereto refer to the test-accounts provided.

If necessary, ask the participant to show you their screen to either help guide them, or to verify they have completed a task.

Comparative Tasks (Same effect on both applications):

Snapchat comparative tasks:

1. Please look at your existing settings and tell us who can view your stories currently
2. Please look at your existing settings and tell us who can add you as a contact on snapchat
3. Please look at your existing settings and tell us who can send you a Snapchat.
4. Please make your snapchat stories only visible by your friends
5. Please now add our [Test-Contact] to your snapchat contacts list.

Facebook comparative tasks:

1. Please look at your existing settings and tell us who can view your Facebook status updates (posts)
2. Please look at your existing settings and tell us who can add you as a friend on Facebook
3. Please look at your existing settings and tell us who can send you a Facebook message
4. Please try to make your Facebook posts only visible by your friends.
5. Please now add [test-friend] to your friends list.

Comparative Blocking tasks (using test-contact/test-friend)

Snapchat comparative blocking tasks

1. You don't want [test-contact] to see your most recent story; try to stop them from viewing it
2. [Test-contact's] account was hacked and they're sending you spam, try to block them.
3. [Test-contact's] account is back to normal, try to unblock them.
4. [Test-contact] has been posting questionable content and you no longer wish to be friends with them, please remove them from your contacts.

Facebook comparative blocking tasks

1. You don't want [test-friend] to see your most recent post on Facebook; try to stop them from viewing it
2. [test-friend's] account was hacked and they're sending you spam try to block them.
3. [test-friend's] account is back to normal, try to unblock them.
4. [test-friend] has been posting questionable content and you no longer wish to be friends with them, please remove them from your friends list.

Semi-comparative tasks (Not one to one, but similar functionality):

Facebook semi-comparative tasks:

1. Ensure that you are the only one who can post to your wall
2. Please ensure that only your friends of friends can add you as a friend on Facebook
3. Please ensure that your Facebook account is not searchable from search engines.

Snapchat semi-comparative tasks

1. Please ensure only the contacts on your phone can add you on Snapchat

Make Accounts Public (comparative/ cleanup)

Snapchat comparative task

1. Please make it so that anyone can see your Snapchat stories
2. Please make it so that anyone can add you as a Snapchat contact

Facebook comparative task

1. Please make it so that anyone can see your Facebook posts
2. Please make it so that anyone can add you on Facebook

Non-comparative tasks

Facebook non-comparative tasks

1. Please enable a way to make all posts on your timeline reviewable by you

2. Please disable the ability for someone to tag your photos
3. Please try to limit who can see what pages you like.

Remember after the interview to verify that the test accounts have been set to public once again!

This concludes part 2 of this research session. Thank you so much for going through these tasks.

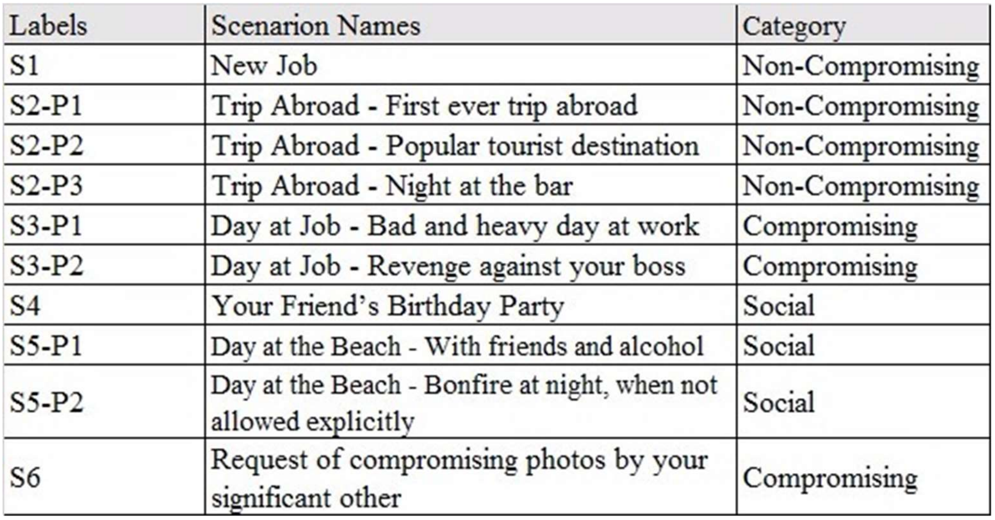
Conclusion

Now that we are done with this session, do you have any questions for me? If you have any questions regarding the study once you leave, please feel free to contact the Primary Investigator (PI) of this study. PI contact info: Phone: 412-268-7534 Email: lorrie@cs.cmu.edu

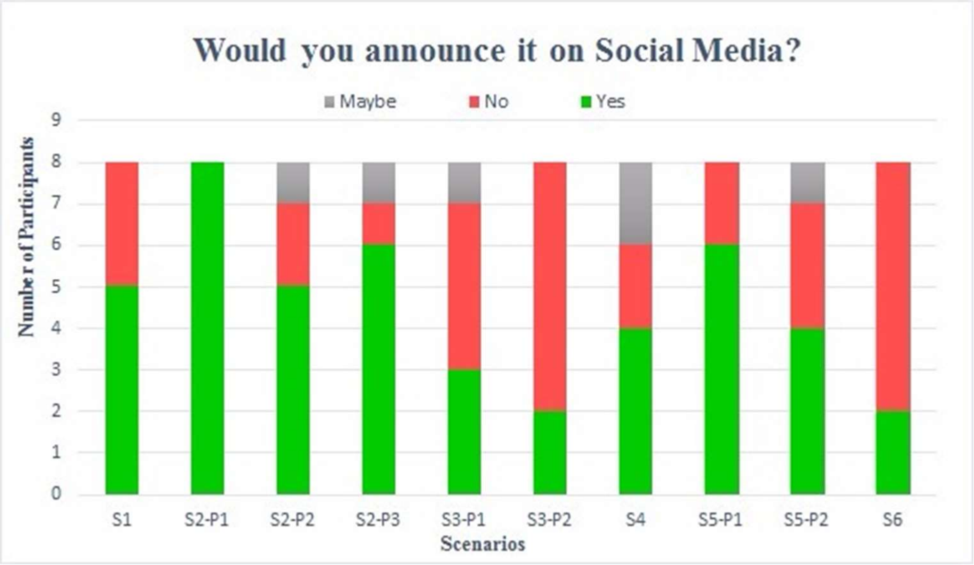
Thank you so much for your participation.

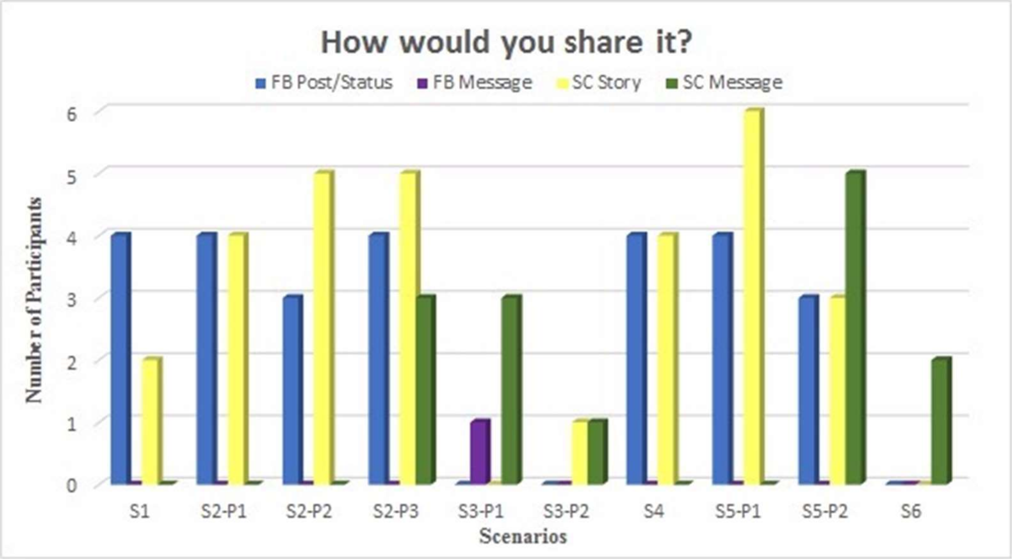
Stop recording and pay participant.

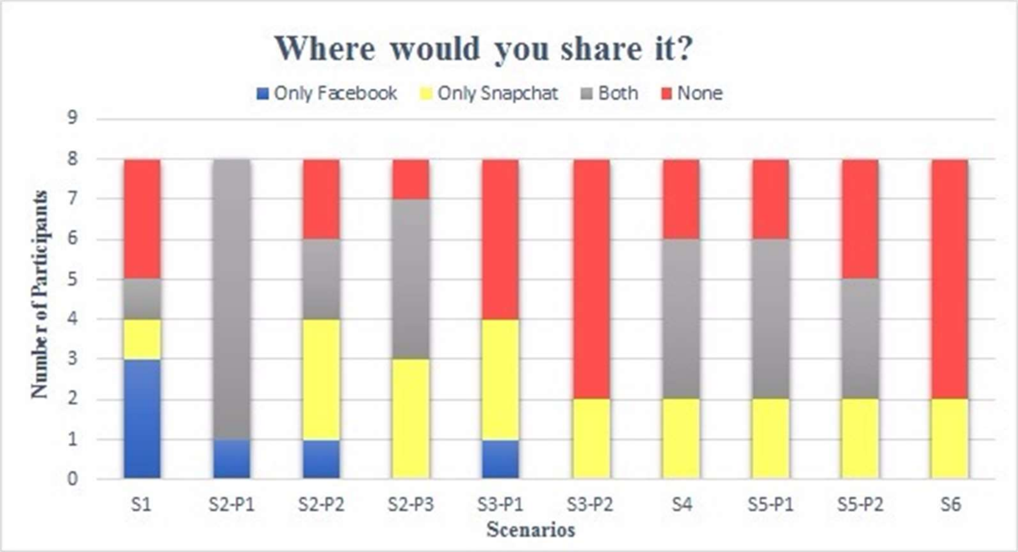
Graphs of the Study:

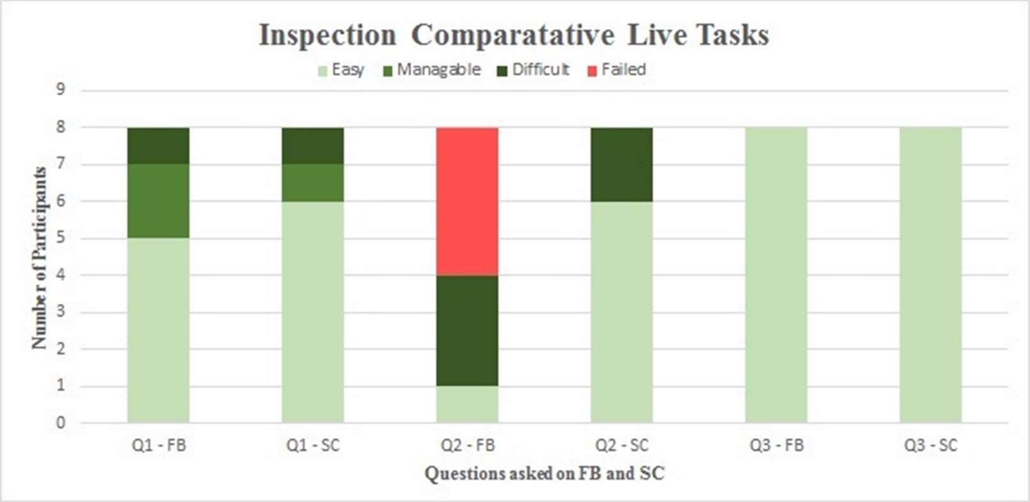


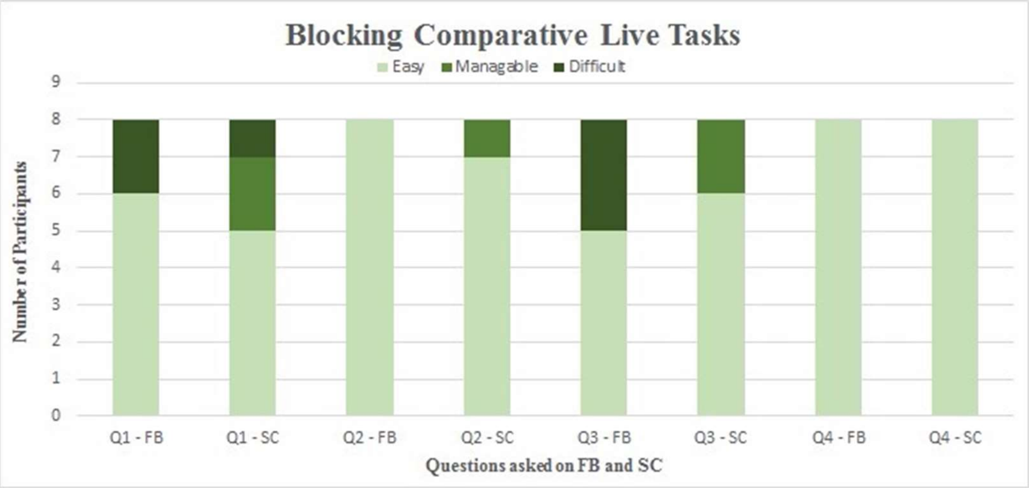
Labels	Scenarion Names	Category
S1	New Job	Non-Compromising
S2-P1	Trip Abroad - First ever trip abroad	Non-Compromising
S2-P2	Trip Abroad - Popular tourist destination	Non-Compromising
S2-P3	Trip Abroad - Night at the bar	Non-Compromising
S3-P1	Day at Job - Bad and heavy day at work	Compromising
S3-P2	Day at Job - Revenge against your boss	Compromising
S4	Your Friend's Birthday Party	Social
S5-P1	Day at the Beach - With friends and alcohol	Social
S5-P2	Day at the Beach - Bonfire at night, when not allowed explicitly	Social
S6	Request of compromising photos by your significant other	Compromising




How would you share it?
FB Post/Status
FB Message
SC Story
SC Message
Number of Participants
0
1
2
3
4
5
6
S1
S2-P1
S2-P2
S2-P3
S3-P1
S3-P2
S4
S5-P1
S5-P2
S6
Scenarios


Where would you share it?
Only Facebook
Only Snapchat
Both
None
Number of Participants
0
1
2
3
4
5
6
7
8
9
S1
S2-P1
S2-P2
S2-P3
S3-P1
S3-P2
S4
S5-P1
S5-P2
S6
Scenarios


Inspection Comparatative Live Tasks
Easy
Managable
Difficult
Failed
Number of Participants
0
1
2
3
4
5
6
7
8
9
Q1 - FB
Q1 - SC
Q2 - FB
Q2 - SC
Q3 - FB
Q3 - SC
Questions asked on FB and SC


Blocking Comparative Live Tasks
Easy
Managable
Difficult
Number of Participants
0
1
2
3
4
5
6
7
8
9
Q1 - FB
Q1 - SC
Q2 - FB
Q2 - SC
Q3 - FB
Q3 - SC
Q4 - FB
Q4 - SC
Questions asked on FB and SC

Date: Monday, April 19, 2017 12:47:00 PM
View: CMU-SF: Basic Information

Basic Information

1. * **Title of Study:**
Self-Deleting Social Media Habits

2. * **Brief description:**
The social media today is a major part in many people's lives, and with the adoption of the 'self-deleting' feature by multiple applications, one can find more people getting attracted towards it. Our project is based on such self-deleting social media applications. Our primary focus will be 'SnapChat', with a secondary focus on the other applications which claim to have self-destruction components. We want to understand the user's perspective of the privacy in these applications, and measure the extent to which these privacy settings are usable. We also hope to learn how users differentiate the applications with self-deleting feature from the ones without it.

3. * **Principal investigator:**
Lorrie Cranor

Title:
Professor

Department:
ISR: INSTITUTE FOR SOFTWARE RESEARCH

View: CMU-SF: Funding Sources (not integrated with Grants)

Funding Sources

1. * **Is this funded research?**
● **Yes** ○ No

If funded add the funding source:

	Funding Source (from list)	Funding Source (manual entry)	SPEX/SPARCS ID	Attachments	Is Internal / CMU Department
View	MICROSOFT CORPORATION				no

2. **Notes:**

View: CMU-SF: Study Team Members

Study Team Members

For the purpose of this submission, study team members to be listed are CO-Is and Study Faculty Advisors.

We recognize that other team members may be involved with the work with the PI being responsible for appropriate training.

1. **Identify each Co-Investigator and Faculty Advisor. These should be individuals involved in the design, conduct or reporting of the research. Who should be included as a Co-I is at the discretion of the PI (see OHRP Guidance on "who are investigators?").**

   Faculty Advisors must be listed for students serving as a PI.

   All team members who interact with participants or who have access to identifiable research data, whether listed here or not, must complete CITI training on Human Subjects Research.

Name	Roles	Involved in Consent	E-mail	Phone	Title	Department
Audasia Ho	CO-I	yes	audasiah@andrew.cmu.edu		Job Mgmt Student Job Profile	UNDERGRADUATE EMPLOYMENT
Gabriel Hobeika	CO-I	yes	gph@andrew.cmu.edu		UNDERGRAD-OTHER HRLY JOB	CENTRAL OPERATIONS
Vibha Iyengar	CO-I	yes				CENTRAL OPERATIONS
Yuan Jiang	CO-I	yes	yuanj@andrew.cmu.edu	+1 (412) 268-2000	Teaching Assistant for Computer Science	CSD EDUCATION-UNDERGRADUATE
Yuankun Li	CO-I	yes				CENTRAL OPERATIONS
Abigail Marsh	CO-I	yes	acmarsh@andrew.cmu.edu		Graduate Research Assistant	ISR: INSTITUTE FOR SOFTWARE RESEARCH

2.

3. **Identify any additional persons from external institutions who are also involved in the design, conduct, or reporting of the research, but who were not available in the preceding selector:**

First Name	Last Name	Email	Institution	SPARCS Account Requested

There are no items to display

4.

5. * **Please briefly describe the qualifications and responsibilities of <u>each</u> study team member in regards to the research. Include the PI and all persons listed above. Please list a few sentences for each study team member, describing responsibilities and relevant expertise. (*This question must be answered to satisfy a regulatory requirement.*)**

Examples:

Andrew Carnegie will serve as PI on this project and will oversee all aspects of the research, from design through data analysis and publication of the results. Dr. Carnegie is a professor in the college of engineering who has 20 years of experience conducting research. His research interests include...

Dr. Mellon will serve as a Co-I on this project. He is a physician from the Bayside Healthcare System who will oversee the research design, specific to the medical needs of the subject population. Dr. Mellon has been treating and researching this subject population for 30 years.

Scotty Carnegie is a PhD candidate whose work will be overseen by the PI. He will assist with the data collection and analysis.

Dr. Lorrie Cranor is the professor of the Usable Privacy and Security class, and the PI of this study. She will ensure the group adequately adheres to the protocols necessary when conducting the research, and like Abigail, will provide guidance during the course of the research.

Abigail Marsh is a Graduate Research Assistant at CMU, and will be overseeing the group in the data collection process. She will also be providing guidance along the way as they conduct their research. She would also be a part of the interview process as a supervisor.

Gabriel is a Master student from the ECE department, CMU.
Vibha is pursuing MS in Information Security from the INI department, CMU.
Yuankun is a Master student from the CS department, CMU.
Audasia and Ms. Jiang are pursuing BS. CS from CS department,CMU.

Gabriel, Vibha, Jiang, Yuankun, and Audasia, would collaboratively conduct the interviews, collect data sets, and analyze them. They would be using skills learned in the Usable Privacy and Security class that they are all enrolled in this semester.

View: CMU-SF: CITI Training

Study Team Training

CITI Training for Study Team Members:

Name	Training: Course	Group	Stage	Completion Date	Expiration Date	Uploaded Training Documentation
Yuan Jiang	IRB Members - Basic/Refresher	IRB Members - Basic/Refresher	Basic Course	6/6/2014	6/5/2017	
	Social & Behavioral Research - Basic/Refresher	Social & Behavioral Research - Basic/Refresher	Basic Course	1/18/2017	1/18/2020	
Audasia Ho	Social & Behavioral Research - Basic/Refresher	Social & Behavioral Research - Basic/Refresher	Basic Course	1/20/2017	1/20/2020	
Gabriel Hobeika	No training data to display					
Abigail Marsh	Social & Behavioral Research - Basic/Refresher	Social & Behavioral Research - Basic/Refresher	Refresher Course	9/8/2016	9/8/2019	
	Social & Behavioral Research - Basic/Refresher	Social & Behavioral Research - Basic/Refresher	Basic Course	8/27/2013	8/26/2016	
	Responsible Conduct of Research	Social and Behavioral Responsible Conduct of Research Course	Basic Course	8/27/2013		

Vibha Iyengar	Course	Group	Stage	Completion Date	Expiration Date
	Responsible Conduct of Research	Social and Behavioral Responsible Conduct of Research Course	Basic Course	8/20/2016	
	Responsible Conduct of Research	Responsible Conduct of Research for Engineers	RCR	8/20/2016	
	Information Privacy Security (IPS)	Information Security	Basic Course	8/20/2016	
	Social & Behavioral Research - Basic/Refresher	Social & Behavioral Research - Basic/Refresher	Basic Course	1/26/2017	1/26/2020

Yuankun Li	Course	Group	Stage	Completion Date	Expiration Date
	Responsible Conduct of Research	Social and Behavioral Responsible Conduct of Research Course	Basic Course	10/14/2016	
	Social & Behavioral Research - Basic/Refresher	Social & Behavioral Research - Basic/Refresher	Basic Course	10/14/2016	10/14/2019

CITI Training for Principal Investigator:

Course	Group	Stage	Completion Date	Expiration Date
Social & Behavioral Research - Basic/Refresher	Social & Behavioral Research - Basic/Refresher	Refresher Course	7/29/2015	7/28/2018

Training Documentation for Principal Investigator (only if PI is external to CMU):

View: CMU-SF: Review Type Requested

Review Type Requested

This choice will determine what type of review and approval your submission will receive as well as the type of questions which will follow this page. Requesting the correct type of review is important to avoid delays in the review. If you are unsure about which type of request is appropriate please contact the IRB Office at irb-review@andrew.cmu.edu.

1. * **What type of review are you requesting?**
   Non-Exempt (Expedited/Full Board)

View: CMU-SF: Study Scope

Study Scope

1. * **Does the study do any of the following:**
   - Specify the use of an approved drug or biologic?
   - Use an unapproved drug or biologic?
   - Use a food or dietary supplement to diagnose, cure, treat, or mitigate a disease or condition?

   ○ Yes ● **No**

2. * **Does the study evaluate the safety or effectiveness of a device?**

   ○ Yes ● **No**

3. * **Provide, in lay terms, a summary of your proposed study:**
   We plan to have a smaller in-lab between-subjects study. This will be an interview based study. We would ask the user to perform some tasks on the privacy settings panel of Snapchat tool, which would be followed by some questions. We would observe the users, to understand if the users could adequately apply the privacy preferences that they believe they wanted for their account. The interview questions would be majorly based on their experience in using the software, apart from the general ones about their privacy perspective. We intend to recruit younger university students, the reason being, we believe a younger population is representative of the user base of the self-deleting applications. This would give us an accurate picture of the problem space.

4. * **What is the purpose of the study (what is your research question) and how will the data collected be used?**
   As part of this study, our two main research questions are: “Do the users think self-deleting applications provide greater privacy than the ones without it?” and “Do the users succeed in achieving their desired privacy?”. We start our project with two hypotheses: 1. The users believed self-deleting social media applications preserve their privacy more than the traditional ones like Facebook, and hence they tend to share much more data to these applications, which otherwise they would have not shared. 2. People do

not completely understand the privacy setting interface of these applications, and thus fail to apply them as desired. They rely on the 'self-deleting' feature of the software.

5. * **For each activity/participant population, describe the research procedures:**
We will first be conducting an interview (see attached Interview Script in the Supporting Documents section of the submission), where we will propose different scenarios in which a user may use a social-media application. Then, we will give the user devices pre-loaded with SnapChat and Facebook with accounts pre-made for the study. We will assign some basic usability tasks pertaining to the applications and observe the users using them. We will have an audio-capture device running during the interview, and we will be using a screen capture application on the devices provided to the interviewee's in order to observe their actions on the application. On completion of the tasks, the participants would be asked if they have any question pertaining to the study, and that would be the end of the study.

6. * **For each activity/participant population, indicate the location(s). Specify whether the participant will be engaged in person, remotely via the internet, etc.:**
Participants will engage this study in person.The study will happen in the CIC Building at CMU, 4720 Forbes Avenue.

7. * **For each activity/participant population, describe the time required of the participant:**
The whole study should take no longer than 1 hour. Travel time is expected to be negligible as participants should be local members of the CMU community.

8. * **Who will be asked to participate?**
Students, age 18 and older, from CMU who are familiar with both SnapChat and Facebook will be asked to participate.

9. * **Will questionnaires or surveys be used?**
○ Yes ● **No**

View: CMU-SF: External Sites

Research Locations and Collaborating Institutions

Research Locations

1. * **a) Where will the research be conducted? If the research will be conducted via the internet, select the location of the primary researcher. Check all that apply:**

☑ **Pittsburgh campus**
□ **Qatar campus**
□ **Rwanda campus**
□ **Silicon Valley campus**
□ **Other**

c) If you are conducting research on one of the CMU campuses indicated above, please specify the exact location.
Conference rooms in CIC.

2. **a) If conducting research on a non-CMU property, have you received permission to conduct research at this location?**
N/A

3. * **a) In what country will the research be conducted (check all that apply)?**

☑ **United States**
□ **Qatar**
□ **Other**

Collaborations

4. * **a) Is this research intended to be done in cooperation with any institutions, individuals or organizations not affiliated with CMU?**
○ Yes ● **No**

View: CMU-SF: Study Deception

Deception

Deception is only possible in minimal risk studies. Investigators need to explain why the deception is necessary to achieve the study goals and how the degree of deception is kept to a minimum. The degree of deception means, for example, withholding part of the study's purpose as opposed to stating a false study purpose. Subjects should be debriefed as early as is feasible.

1. * **a) Will deception be used?**
No

View: CMU-SF: Participant Info (All)

Participant Information

1. * **What is the age range of participants in the proposed study?**
"Age 18 and older

2. * **How many participants are needed for the study?**
15

3. * **How was that number determined?**
We think 15 participants is a good amount because we can get adequate information from 15 participants, and it’s a within-group study, so we don’t need as many participants as a between-group study, and it’s a lab study (as opposed to an interview or survey), so the time requirements will be higher

4. * **Please list inclusion and exclusion criteria:**
Inclusion Criteria: Participants must be a CMU student, and familiar with both Facebook and Snapchat. Age criteria: "Age 18 and older

5. * **a) What do you estimate the ratio of males to females to be?**
We’d like to get a ratio of males to females that is representative of students at Carnegie Mellon University.

* **b) Will this be reflective of the local population?**
○ Yes ● **No**

c) If not, please explain:
It would reflect the population currently living around the CMU campus, since we would recruit the students from CMU, but this would not include local citizens.

View: CMU-SF: Participant Info (Non-Exempt)

Participant Information (Non-Exempt)

1. * **Will vulnerable subjects (Pregnant Women, Neonates, Prisoners, Children, and Cognitively Impaired Adults) be involved in the proposed study?**
○ Yes ● **No**

* **Pregnant women, human fetuses:**
Pregnant women will not be specifically included or excluded

Neonates:
○ Yes ● **No**

Prisoners:
○ Yes ● **No**

Children:
○ Yes ● **No**

Cognitively impaired adults:

○ Yes ● **No**

2. * **Will the participants be capable of understanding the nature of the study and the consent process?**

   ● **Yes** ○ No

3. * **Will you target a certain population?**

   ● **Yes** ○ No

   * **Please explain:**

   We would be recruiting the CMU students only.

4. * **a) Do you anticipate that your participants will represent a cross-section of the population in the region where the study is being conducted?**

   ○ Yes ● **No**

c) If no, please describe your study population and address why minority representation is not considered:

We would be recruiting the CMU students and hence, we expect to have a participants from various cross-sections. We do not have any other specific restrictions.

View: CMU-SF: Recruitment

Recruitment

1. * **Describe how participant recruitment will be performed:**

   We will use flyers with details about the study, compensation information, and contact information to recruit participants.

2. * **Indicate how and by whom potential participants are introduced to the study:**

   We have created an email account specifically for this study, so the study team will be able to reply to the participants who send an email.

3. **Check all boxes below that apply and attach documentation using Question 5:**

Flyers?	**Where will they be posted?**
☑	We will post flyers in common campus locations, such as the CUC, Gates, Wean, Baker/Porter, Hunt, and the common areas of on-campus dorms.
Radio, TV?	
□	

5.

E-Mail?

□

6.

Web-based?

□

7.

Participant Pool?

□

8.

Other?

□

9.

10. * **Will participants undergo screening prior to their participation?**

● **Yes** ○ No

If yes, please describe:
The study team will ensure that participants are CMU students, at least age 18 and that they use both SnapChat and Facebook (i.e., the study inclusion criteria).

11. **Please attach all recruiting and screening materials:**

	Document	Category	Date Modified	Document Hi
View	Project_Flyer_For_recruitment.pdf(0.03)	Recruitment Materials	3/18/2017	History

12.

View: CMU-SF: Consent Info (Non-Exempt)

Consent (Non-Exempt)

1. * **a) Do you plan to use consent forms?**

● **Yes** ○ No

Link to CMU Consent Form Templates

b) If yes, describe the process of how consent will be obtained, and by whom:
Our researchers will first introduce the purpose and procedure of our study to all of the participants, and answer participants' questions. Finally, participants will be asked to sign consent forms.

c) If yes, please attach your consent form(s) here:

	Document	Category	Date Modified	Document History
View	Project_ConsentForm.pdf(0.02)	Consent Form	3/18/2017	History

2. **Will the consent form be presented on paper?**

● **Yes** ○ No

3. **Will the consent form be presented online?**

○ Yes ● **No**

4. **Are you requesting to use a consent form that is different from the CMU model consent?**

○ Yes ● **No**

Waiver of Informed Consent
If requesting a waiver of informed consent, please complete the following:

5. * **a) Are you requesting a <u>waiver of informed consent</u>?**

○ Yes ● **No**

Waiver of Written Consent
If requesting a waiver of written consent, please complete the following:

6. * **a) Are you requesting a <u>waiver of written (signed) documentation</u> of informed consent?**

○ Yes ● **No**

Minor Participation
If participants are minors, please complete the following:

7. **Please describe how assent will be obtained:**

8. **Are minors at a developmentally appropriate age to assent? Please describe how this was determined:**

View: CMU-SF: Risk and Benefits (All)

Risk and Benefits (All)

1. * **Will participants receive a direct benefit from the study?**

○ Yes ● **No**

2. * **Discuss the expected indirect benefits to participants:**

Compensation of 10$ Amazon gift card.
Post the study, users may change their Facebook or Snapchat use, which could potentially be beneficial for them.

3. * **Discuss the potential risks to participants:**
Breach of confidentiality is a potential risk. Also, some of the questions asked during the study could make a participant feel uncomfortable. These risks are mentioned in the consent form.

4. * **Discuss how all potential risks will be managed and/or minimized:**
The study team will mitigate the risks by collecting minimal data from the participants, keeping all study data secure/de-identified, telling participants they do not have to answer any questions they don't want to answer.

View: CMU-SF: Risk and Benefits (Non-Exempt)

Risk and Benefits (Non-Exempt)

1. **Is deception used?**
No

Note: you answered this question on the Study Deception form. If you need to change your response, use the jump menu above to go to the Study Deception smart form.

2. * **Indicate the degree of any possible (e.g., physical or psychological) risk you believe the research will pose to human subjects*:**
N/A

3. * **Describe how the study fits in the selected risk level. If deception is used in the study (see question 1 above), please address how it fits in the selected risk level:**
The probability and magnitude of harm or discomfort anticipated in the proposed research are not greater, in and of themselves, than those ordinarily encountered in daily life of during the performance of routine physical or psychological examinations or tests.

*Risk Descriptions:

Minimal Risk: A risk is minimal where the probability and magnitude of harm or discomfort anticipated in the proposed research are not greater, in and of themselves, than those ordinarily encountered in daily life of during the performance of routine physical or psychological examinations or tests.

Greater than Minimal Risk: A risk is greater than minimal where the probability and magnitude of harm or discomfort anticipated in the proposed research are greater than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests.

View: CMU-SF: Compensation (All)

Compensation

1. * **a) Are participants to be compensated for the study?**
● **Yes** ○ No

b) If yes, what is the amount of compensation:
$10

c) If yes, what is the source of the compensation:
Amazon

d) If yes, what is the type of compensation (eg, gift card, cash):
Gift Card

2. * **Will participants receive any non-monetary compensation?**
○ Yes ● **No**

3. * **Are there any costs to participants?**
○ Yes ● **No**

View: CMU-SF: Compensation (Non-Exempt)

Compensation (Non-Exempt)

1. * **Will you compensate participants for injury resulting from participation?**
N/A

2. **a) Will participants who are students be offered class credit?**
No

View: CMU-SF: Data Security and Confidentiality

Data Security and Confidentiality

1. * **Will personal identifiers be obtained?**
● **Yes** ○ No

If yes, list the personal identifiers:
Names, emails, signatures on consents and audio.

2. * **Describe your procedure for coding your data (encoding):**
We will not record any of the subjects faces, or their names. Instead, each subject will be assigned a number for their time in the study, and we will associate their results with that number. Outside of payment, there should be no correlation between our subjects and their data.

3. * **Will audio recordings be made?**
● **Yes** ○ No

If yes, please describe:

We will record interview part of our study. The team will ensure that audio recording is conducted in a non-public, private area where non-consented individuals will not be audio recorded.

4. * **Will video recordings be made?**
   ● **Yes** ○ No

   If yes, please describe:
   We will record users' operations while they using social media, and only user's fingers and phone screen will be recorded.

5. * **Do you intend to obtain a certificate of confidentiality from NIH?**
   ○ Yes ● **No**

6. * **In addition to the individuals listed on the study personnel page, who will have access to research data (e.g. surveys, questionnaires, recordings, interview records, etc.)?**
   No other person will have the access.

7. * **Describe how you will protect participant confidentiality and secure research records (e.g. password protected, encrypted, etc.). Include location of where the data will be stored:**
   All of the data will be de-identified. Paper forms will be stored in a file cabinet in a locked office. Electronic records will be stored on a password-protected computer.

8. * **Describe your process for overseeing your study. Include a description regarding monitoring of data (to ensure that study goals are met and adherence to the IRB approved protocol is maintained). Examples: Review of lab notebooks, frequency of meetings to review data, who will be present at the meetings, how recruitment and retention will be monitored, etc.:**
   The study will be conducted by team members in a conference room in the presence of the study guide, Abby. The Principal Investigator will periodically oversee the process of this study. For performing qualitative analysis, post the data collection, the entire team would meet once a week.

9. * **Describe your process for ensuring that adverse events, unanticipated problems, and subject complaints are reported to the IRB Office in a timely manner:**
   The consent form provided at the start of the study includes the details of IRB, so that participants could report, if any complaints. Also, the team members would notify the PI in case of any such adverse events during the study.

10. **Confirm that all research data will be retained at CMU for a minimum of three (3) years past study completion:**
    ☑

View: CMU-SF: Supporting Documents

Supporting Documents

1. **Attach supporting files:**

	Document	Category	Date Modified	Document History
View	InterviewScript_WithMod.pdf(0.04)	Other	4/13/2017	History
View	Gabriel's CITI completion Report(0.01)	Other	3/6/2017	History

Suggested attachments:

- Other study-related documents not attached on previous forms

View: CMU-SF: Final Page

Final Page

1. * **Does study have potential conflict of interest?**
   ○ Yes ● **No**

You have reached the end of the IRB submission form. Read the next steps carefully:

Click **Finish** to exit the form.

Important! To send the submission for review, the principal investigator must click **Submit** on the workspace.