Usability of End-to-end Encryption (E2EE) Chat Services

Ryan Cryar
Oregon State University
cryarr@oregonstate.edu

Yi Xuan Chia
Oregon State University
chiay@oregonstate.edu

ABSTRACT

When it comes to chatting with friends or family, it is quite common to talk about sensitive things that one would not want other people knowing about. This is what end to end encryption chat services hope to solve (will be refereed to as E2EE), making a safer way to chat with others without your privacy being compromised. There are many chat services out there, but it is difficult to find the right one that meets the needs of the average user. Some of the primary concerns with finding the right E2EE application is awareness, whether users are even aware these services are available, and whether the application can be used and understood without a security background. This is what the study hopes to uncover, by comparing three common E2EE apps, (WhatsApp, Riot.im, PGP), as well as surveying on what makes people want to use a chat service. This study is conducted in the hopes of understanding what makes an E2EE application usable, and how to make them more exposed to users looking to be more secure in their messaging.

1 INTRODUCTION

End-to-end encryption chat services are applications that use different cryptography to help keep users messages and private info safe from adversaries. Those adversaries might be other people trying to gain information to exploit them, or it could be the government attempting to gain information on them. Using normal services for messaging such as SMS, email, or Facebook Messenger, makes it much more likely for your messages to be compromised by any adversary. This breach of privacy is mitigated by using E2EE applications. The goal of this project is to analyze the usability of these E2EE applications and understand how to make them better for people not in security. This is an important factor of the adoptability of these services, so identifying the problems of these applications can make it easier to understand what design principles must be taken into account when designing an E2EE app.

This paper is structured as follows: In Section 2, the design of our study is stated. Next, in Section 3, the approaches that were taken to answer the research questions are discussed, followed by Section 4 where the results are described and visualized. In Section 5, some of the discovered threats of validity are stated. Finally, the implications the results for future study and research are mentioned, and a conclusion is made in Section 7.

2 DESIGN OF STUDY

To study the usability of end-to-end encryption in chat services, we basically came out with two research questions.

First of all, privacy and security are most likely binded to trust in most of the time, even if it is not obvious. Even more, trust plays an important role in this digital era. It takes part when people are willing to share sensitive personal information with numerous information recipients such as Internet service providers (ISPs), banks, search engines, shopping website, and etc. Other than that, trust is also involved when people shares information with companies in return for their services, which mostly happens a lot in social media and chat services [2]. Particularly, privacy and security in chat services has become one of the highlights as soon as people are aware of surveillance activities. Consequently, E2EE chat applications aim to give their users a peace of mind while communicating or sharing private data. However, the level of trust that the users have towards their communicating applications is still remained unknown. Therefore, it is worth to find out to what extent these users are willing to trust the reliability (or security) of their chosen everyday use application.

On the other hand, privacy paradox often happens among those who have varying degrees in privacy and security concerns. These people can be privacy fundamentalist, but at the same time they might not being part of the E2EE application community, while some might be vice versa. Since concerns and actions do not always come as a combination, it rises a question of whether privacy and security concerns that the users have had led them to the adoption of their current E2EE

chat services, or perhaps will eventually make users to adopt one. Furthermore, concerns can be part of the reasons, along with other possible usability and social factors that are pulling users into this community. Whichever reasons that lead the users to this adoption can make significant impacts in the usability perspective.

To gather information, we designed a series of questions asking the users about their privacy concerns and opinions about their everyday use applications, both verbal and paper form. These questions enabled us to collect qualitative and quantitative data that overall produced a final conclusion to our research questions.

3 SOLUTION APPROACH

When conducting this study, it was originally thought best to go with interviews and then follow it up with a survey to get our data validated. But after some reviewing, the best method was to begin with a survey and to validate it through interviews.

3.1 Surveys

One method we used was to conduct a survey on Amazon MTurk. We expected to gather 20 participants and pay each participant $0.50 to compensate their time and contribution. Based on our survey design, the estimated duration for each participant to take the survey was roughly five minutes. While publishing the survey on MTurk, the only qualification of workers that we set was HIT approval rate of 95% or greater.

In the survey, we asked the participants on questions about their online privacy concerns in a five point Likert scale format from "Very unconcerned" to "Very concerned", followed by questions about the chatting application that they are using. The participants answered the questions, *"What chatting application(s) do you use?"*, and *"Who do you communicate with those application(s)?"*. We also asked the participants about the simplicity of use and privacy regarding their applications in a five point Likert scale from "Terrible" to "Excellent". The "I'm not sure." option was also available. For users who were not using any messaging application, some specific questions regarding their messaging applications were skipped.

The second part of the survey was about two scenarios. The first scenario was about the privacy concerns that the users have if they use their application to send a photo to different recipients. Similarly, the second scenario was about sharing tax forms. Both scenarios had the same recipients: family, friends, classmates, neighbors, colleagues, teachers/instructors, and any other possible recipients. We wanted to see if there is a relationship between a recipient and the way to communicate when privacy and security is taking into account. Both scenarios also had questions on a five point Likert scale from "very concerned" to "Very unconcerned".

Next, the third part of the survey was covered by questions from Internet Users' Information Privacy Concerns (IUIPC) to measure their concerns about information privacy based on different categories. The categories, based on IUIPC, are control, awareness, collection, and unauthorized secondary use [1]. The participants answered three to four questions in each category structured in a seven point Likert scale from "Strongly agree" to "Strongly disagree".

Finally, we collected the demographic data of each participants for age and gender.

3.2 Interviews

The next method we did was to conduct interviews with a walkthrough of the three E2EE chat services with four users. The users were limited to four due to time contraints with the interviews. Originally, interviews were expected to take around 20 minutes, but ended up being close to an hour per user. This was in part due to users taking their time to explore the applications when assigned their tasks.

These interviews began by asking a few demographic questions and was also a quick survey of their privacy concerns. Then we also recorded what chat services they had used and what they mainly liked about those applications. This was conducted in the hopes of understanding what the users were coming from. Should all of the users be coming from iMessege, it might skew the likes and dislikes of each chat service to something different than should the users have a mixed background. The walkthrough then began with each user starting up the application, looking around it, doing a key agreement, and sending an encrypted message. With the exception of PGP, which the users had to copy and paste the encrypted text and decrypt as another user as email was not an available medium at the time of conducting the walkthroughs. The likes, dislikes, and improvements were then recorded after each and every walkthrough. Upon finishing the walkthroughs, the user was asked a series of questions reflecting on their experiences with the applications. They were asked which were their favorite, and their least favorite, and why they liked/disliked them.

Throughout the walkthrough, the user was be asked to comment on their thoughts as they go through the applications. This was to prevent the users forgetting any of the parts they were going to comment on once they finished the task. One key factor when writing the interview script, was to make sure that user fatigue was minimized. As the interview went on the more the data could be less valuable due to the user being fatigued and wanting to get through it.

Finally the interview concluded with being asked whether they might explore more of E2EE applications out there.

4 RESULTS

4.1 Surveys

The data that we collected from the surveys are mostly quantitative, being that most questions have multiple choices, or were structured in five or seven Likert scale format.

Eventually, we gathered 20 participants on Amazon Mechanical Turk, but 2 were later rejected due to invalid entries to some corresponding questions. The total cost of distributing the surveys was $13.30. We ended up analyzing 18 surveys and came out with the results described in this section.

4.1.1 Demographics

12 out of 18 of our participants aged from 26 to 33, followed by 3 participants who aged from 18 to 25 years old, 2 participant who aged from 34 to 41, and finally 1 participants of 50 to 57 years old. Among these participants, we had 13 males and 5 females. The data for this part are imbalance for both aspects because participants were not carefully chosen to contribute.

4.1.2 General Questions

We measured the privacy concerns that the participants have on a five point Likert scale. Overall, 72.22% of our participants are considered concerned about their privacy in general, but only 66.67% of them concerned about both online privacy and security.

Among the 18 participants, only 16 of them were currently using some kind of messaging application, which includes WhatsApp, Facebook Messanger, iMessage, Riot, PGP, and Viber. When we asked them about the reasons of choosing their specified applications, 56.25% (9 out of 16) of them said that the applications are easy to use, while 43.75% (7 out of 16) said that they chose to use those applications because someone they know, mostly friends and family, are also using it. Since each application does not work on cross-channels, they had to adopt the same one in order to communicate. Hence, privacy and security concerns may not necessarily taking into account when users are choosing their messaging application. The distribution of users for each messaging application was not even at all as we gathered 83.33% of WhatsApp users, 66.67% of Facebook Messenger users, 11.11% of Riot users, and 5.5% of PGP user, and each participant may belong to one or more of those percentages as they own multiple chat service accounts of different companies. Moreover, more than 80% of the participants rated WhatsApp and Facebook Messenger of having good or even excellent in terms of their simplicity of use and privacy, and more than 50% of the participants would expect the applications that they are using to have good or excellent privacy and security.

To measure the level of concerns about information privacy that the participants had, we measured the entries of participants on the IUIPC questions. Figure 1 shows the number of entries for each Likert scale element on different categories. Because each category is associated with different number of questions, the results are therefore measured using percentages. Based on the line graph, the control and unauthorized secondary use set peak for participants who somewhat agree about them, while the collection set peaks for most participants who agree about the data collection statements. It is slightly higher for participants who neither agree or disagree about the awareness set compared to the group who agree and somewhat agree. Overall, our participants have higher level of concerns as we see highs at the "agree" side and lows at the "disagree" side. However, if we break these results down for each individual, they definitely do not support our conclusion because our participants have different responses in previous part of the survey, meaning that the responses of a particular participant from previous part of the survey and his IUIPC responses did not match up. This occurred in multiple participants. In this case, the IUIPC results are invalid for our study.

	Scenario 1	Scenario 2
Very concerned	15.74%	18.52%
Mildly concerned	23.15%	32.41%
Neutral	33.33%	24.07%
Mildly unconcerned	16.67%	16.67%
Very unconcerned	11.11%	8.33%

Table 1: Each response in scenario 1 & scenario 2

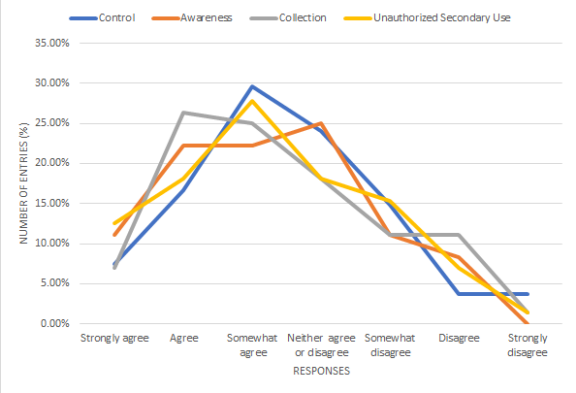

Figure 1: Results for IUIPC Questions

4.1.3 Scenarios

Figure 2 and 3 visualized the entries that we got from the participants about their level of concerns while using their application to send some specific information to some specific recipients. Scenario 1, which had the participants to assume that they want to send a photo to different recipients with their

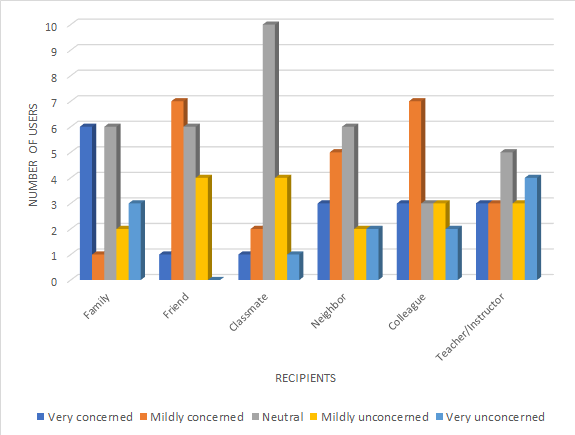

Figure 2: Results for Scenario 1 - Send photo to different recipients

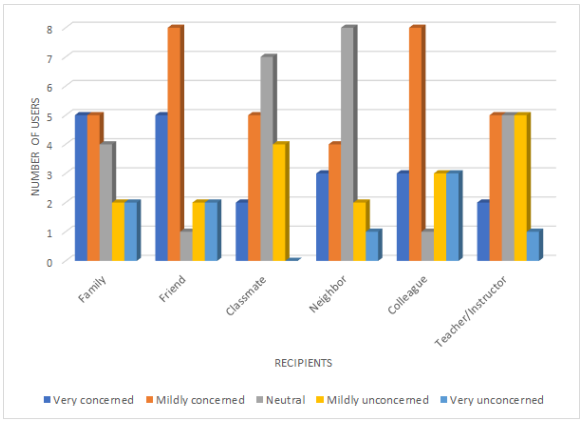

Figure 3: Results for Scenario 2 - Sharing tax forms with different recipients

messaging application, had high percentage of 33.33% of "Neutral", followed by 23.15% for "Mildly concerned". Compared to scenario 1, scenario 2, which had the participants to assume that they want to share tax forms with different recipients with their messaging application, had higher responses for "Mildly concerned" of 32.41% but lower for "Neutral" of 24.07%, showing that people are more concerned about privacy when sharing confidential data. It is also worth mentioning that in Table 1 the responses for "Very concerned" and "Very unconcerned" in both scenarios are opposing to each other depending on the information that the participants want to share, regardless of which recipients that they chose to share. Looking to each individual recipient, family, friends, and colleagues are the top three that took the highs for "Very concerned" and "Mildly concerned". These results are anticipated as those recipients are considered the target group of communication in most of the time; participants may not talk to their neighbors or teachers very frequently via chat services.

4.2 Interviews

The interview data is broken up into two parts: qualitative and quantitative. Our quantitative data is measured through the preliminary study questions (privacy concern scale, apps used, etc.), and final application preferences. The qualitative data is the walkthrough, including comments, likes/dislikes, and improvements.

4.3 Pre-interview

There were four users that were interviewed and participated in the walkthrough. Three out of the four participants were female, all of which belonged to the 18-24 age group. One male was interviewed, who belonged to the 25-30 age group. It was an even split of 50% concerned about their privacy, 50% neutral. 50% were also concerned about their privacy within their chat applications that they were using. Half of the participants had heard previously of end to end encryption, but noted with their answer that they could not explain what it was.

The most common chat service among all of them was iMessage, which 100% of the users used. The second most common was Facebook messenger which three of the four used, and third was WhatsApp, which only two of the four used. When asked what made them use their chat services, there were scattered responses including: the UI, ease of use, and the most common: to talk to friends and family that use that service. Facebook messenger was mostly used to talk to friends, while WhatsApp was used to talk to out of country friends/family.

4.4 App Walkthroughs

4.4.1 WhatsApp

WhatsApp was mostly liked for its ease of use. Since two of the four participants had already used it before, this was the fastest task that was completed amongst all of the walkthroughs. The task consisted of the user getting a feel for the application and looking around all the settings commenting on what they thought, and then sending an encrypted message to our test phone. WhatsApp, when selecting a chat with someone, automatically enables encryption, so the user does not have to do anything in order for the chat to be secure.

However, because of this, it was the most liked out of all of the applications. Even though every user had thought it was ugly and some even preferred riots UI but WhatsApps ease of use.

One of the dislikes that was very strongly emphasized was the dislike of "Statuses". WhatsApp has a status feature where the user can post a status about what they're up to that day or anything else they wish other people to know. The participant

expressed extreme distaste for this feature, which added to their dislike of the apps design.

4.4.2 Riot.im

Riot yielded the most volatile of the responses among all of the tested applications. The app was most liked for its security, and its UI structure. One participant reported feeling "aesthetic", in reaction to the layout of the UI. The other participants commented on the UI as well, the general consensus was that the UI was much cleaner than that of WhatsApp.

The apps security was also a nice selling point to the users. Having to go in and manually start the encryption process and do a key agreement showed that the application took security extremely seriously. This was very comforting to the participants and many showed satisfaction when they completed the key agreement and were in a secure chat room, knowing that it is secure because of something they did.

However, the security was also its downfall. Because of the applications design, directions were extremely sparse. Even during key agreement, there were no directions explaining what was going on. Riot's key agreement feature is having a "Verify" button and having a sequence of emojis pop up on each users device. The users must verify these are the matching emojis before proceeding, upon which the device will be verified and they are in a secure chat room. The emoji design seemed to be put into place so that it would make it easier to go forth and do the verification. But because of the lack of directions, this confused the participants. One participant was recorded saying that they did not understand why the emojis appeared and what verifying them has to do with security.

To even get to the verify button, a user would have to click on the room page, click on the other users name and select their devices. But the issue that many of the participants faced was even finding this. It was not clearly labeled, and some did not think to click on the room page as it did not seem clickable. One participant said that if the application was just clearly labeled it would have more likable.

A feature of riot is detecting shaking of the phone while using the application. The user is then presented with a message: "You seem to be shaking the phone in frustration, would you like to submit a bug?". This feature popped up when one of the participants did just that. This terrified the participant, and they promptly said they "did not like that". Their distaste of this feature could have been that it was annoying or weird it was tracking that, but the participant did not go further than that.

Riot was the most disliked, tied with PGP. With two of the four participants saying they disliked it. Riot was only liked by one participant, although they had wished for more directions, which they said "would have made it easier to use and would have liked it more". Another reason that participants felt they disliked it, was that it made them feel dumb. One participant was telling us that when going through the key agreement, because there were no directions and they did not understand it they felt dumb while using the application.

This is obviously a key issue when using this application, as if it makes you feel dumb when using it then there is a high chance of not using it in the future.

4.4.3 PGP

PGP also yielded interesting results, as it was expected that it was going to be the most difficult, but participants figured it out quite quickly. Participants liked it because it was simple and seemed secure. Because it required a lot of the encryption be done by manually clicking on what to encrypt, participants said that they felt "fancy" or "like a hacker". This was interesting because since all of the participants have no security background, they are seeing this as perceived security. That when something looks "fancy" or it relies on manually doing the dirty work, it is somehow more secure. While, yes PGP is very secure, even especially since using a 4096 bit key and RSA, it could have been using a terrible algorithm and it would have seemed very secure purely off of looks.

One participant really liked PGP. They said that it felt very simple and it helped them understand more about what encryption is really doing. In fact two of the four participants started to figure out what end to end encryption is when using PGP. The other participants were still confused as to what they were doing, but could understand the process of encrypting. The component that a lot of participants did not understand was the concept of keys. But after performing some of the encryption that PGP requires, it became a little more clear about what keys had to do with encryption. When asked to try to conceptualize using keys, a common analogy the participants all used was the file cabinet concept. Where files are secure and nobody can access them unless they have the key. This showed they had basic understanding of encryption.

PGP was also the most disliked tied with Riot. This was largely due to its lack of clear direction. When presented with the UI, there's no clear path to try to send a message to someone. One participant had said that they were confused because the messaging component wasn't tied in with actual PGP, it had to be over email. They suggested one way to make it easier was to have a PGP mail client as well, to help integrate it all into one system, and not have to spend time trying to get everything set up in different locations.

Directions were also a huge issues, as participants went along, there could have been points where they selected something wrong and could have exposed their message without them knowing. Some directions on a proper way to do all of the encryption and sending would be a huge help for first time users, especially since exposing their privacy could be a mistake that happens on first use.

5 THREAT TO VALIDITY

There are two methods, surveys and interviews. Because of the different structure, there were two sections of different threats to validity.

5.1 Surveys

One external threat to validity was the age of users. From the data that we collected, most of the participants were 26 to 33 years old, which considered the generation that have high influences from modern technology. Any issue that relates to technology or privacy may be magnified and level up their concerns. For this reason, they were hardly to eliminate their fixed mindset and experience while taking the survey. Eventually, the results of the survey are not generalized for all population.

The second external threat to validity existed was Hawthorne effect. Although the surveys were not monitored at the moment when participants were taking them, the behaviour of participants might still change and give ideal answers that we anticipated. Overall, if this happened to all the participants, then our results are considered invalid to represent even an individual.

5.2 Interviews

One outstanding external threat, was that all of them were iPhone users. This means that they all use iMessage as their key chat service. Now this could effect the data as all of them could be expecting something like iMessage for them to really feel comfortable and like the application. However, it did seem like the participants kept an open mind with each application, especially when using PGP which is a completely different interface. This is slightly shown in the data with the preference for WhatsApp overall, but that also could be purely because WhatsApp is easier to use. This would be something to further study.

Another external threat that was observed is that some of the participants felt they couldn't give valid advice. Two of the female participants said that they felt they had no experience with these applications and did not have a lot of confidence with computers, so their input was less valid than should they have been a CS major. They also were afraid to give answers sometimes because "they did not want to sound dumb". Reassurances were given, and they were absolutely helpful in aiding in input for this study. But because of these factors, not all information might have been collected on how they felt, as participants could have been hiding what they thought to avoid saying something they felt was "dumb".

6 DISCUSSIONS

An interesting result that came up in the surveys and interviews, was how the participants primarily used applications when their friends used them. It is entirely possible that should enough of their social group use a certain application, they would use that application in order to just talk with them no matter what its usability status is. That will be something that should be further studied.

Another interesting result that would be good to look at is the need for clear directions in the applications. Different applications will need different types of directions, some might be best to do a walk through set of directions at the start. PGP might especially benefit from this just to get users started with using it.

The interview methodology changed quite a bit from the midterm report due to there not being enough hard usability data. We decided to add the walkthroughs in order to get the usability data and understand what real people are thinking/doing when using these applications. The interview we previously thought up is still present in the current script, but as a pre-interview to the walkthrough to get an understanding of what the users privacy ideals are.

There are a few things that would be redone. For the interviews, having a dedicated test environment would be great to make sure that everything is consistent with each participant. This would help keep results organized and easy to conduct the interviews. It could even shorten the time required for the interviews should they be efficient. It would also be ideal to have a larger number of participants, but time did not permit it. As for the surveys, Amazon Mechanical Turk is not an effective platform for conducting such a small research. Even more, participants are more likely to target the rewards instead of spending adequate amount of time to take the survey seriously. However, the effort for collecting reasonable data will be much greater, despite time consuming. In any case, this should also taken into account.

7 CONCLUSION

With end to end encryption chat services being a key component in keeping yourself private with your messaging, it is important to keep these services usable even for those with no security experience. These applications can be helped tremendously through adding features to make them easier to use, which will effect which application is used more in day to day life. One of the primary reasons for adaptability is social groups. Whichever applications friends/family use, are going to be applications that their social groups also use. When it comes to usability, directions are key. The directions can help ease the user in to more complicated UI setups and even allow them to learn more about the cryptography that goes on behind the scenes, but users should at least know why they are doing a certain thing within the application. This overall

can help adoptability, but also allow users who adopt the application through their friends and family an easier way to use the application.

References

[1] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355, 2004.

[2] Neil Richards and Woodrow Hartzog. Taking trust seriously in privacy law. *Stanfort Technology Law Review*, 19, 2016.

APPENDIX

Appendix material is formatted differently than what appeared in the actual survey seen by participants.

A Survey Questions

1. How concern are you regarding your:
   (Answered on a five point Likert scale from "Very Unconcerned" to "Very Concerned")
   (a) Privacy in general
   (b) Online privacy
   (c) Online security
   (d) Security in chat services (e.g. WhatsApp, iMessage, etc.)
2. Do you use any messaging applications?
   - Yes
   - No
3. What makes you want to use those applications?
   (e.g. easy to use, interface looks nice, because my friends are using, etc.)
4. What chatting application(s) do you use? (Pick whichever apply)
   ☐ WhatsApp
   ☐ PGP
   ☐ Riot
   ☐ iMessage
   ☐ Facebook Messenger
   ☐ Viber
   ☐ Others (Please specify) _____
5. Who do you communicate with using your chatting application(s)? (Pick whichever apply)
   ☐ Family
   ☐ Friends
   ☐ Classmates
   ☐ Neighbors
   ☐ Colleagues
   ☐ Teachers/Instructors
   ☐ Others (Please specify) _____
6. How do you feel about the simplicity of use of your chatting application(s)?
   (Answered on a five point Likert scale from "Terrible" to "Excellent")
   (a) WhatsApp
   (b) PGP
   (c) Riot
   (d) iMessage
   (e) Facebook Messenger
   (f) Viber
   (g) Others
7. How do you feel about the privacy and security of your chatting application(s)?
   (Answered on a five point Likert scale from "Terrible" to "Excellent". "I'm not sure." option available)
   (a) WhatsApp
   (b) PGP
   (c) Riot
   (d) iMessage
   (e) Facebook Messenger
   (f) Viber
   (g) Others
8. What level of security and privacy do you expect the chatting application(s) provide while communicating with:
   (Ans: Terrible, Poor, Average, Good, Excellent)
   (a) Family
   (b) Friends
   (c) Classmates
   (d) Neighbors
   (e) Colleagues
   (f) Teachers/Instructors
   (g) Others

9. How concern are you about giving permissions to your chatting application(s) to access to your data in your devices?
(e.g. contact list, photo gallery, files, etc.)
(Answered on a five point Likert scale from "Very Concerned" to "Very Unconcerned")

10. **Scenario 1: Assuming that you want to send a photo of yourself with the person below using one of your chatting applications that you picked.**

    For a specific recipient, how concern are you for using the application to complete this task?
    (Answered on a five point Likert scale from "Very Concerned" to "Very Unconcerned")

    (a) Family
    (b) Friends
    (c) Classmates
    (d) Neighbors
    (e) Colleagues
    (f) Teachers/Instructors
    (g) Others

11. **Scenario 2: Assuming that you want to share your tax forms with the person below using one of your chatting applications that you picked.**

    For a specific recipient, how concern are you for using the application to complete this task?
    (Answered on a five point Likert scale from "Very Concerned" to "Very Unconcerned")

    (a) Family
    (b) Friends
    (c) Classmates
    (d) Neighbors
    (e) Colleagues
    (f) Teachers/Instructors
    (g) Others

12. IUIPC Questionnaire [1]
    Purpose: To reflect Internet users' concerns about information privacy.
    (Participants answered the following questions on a seven point Likert scale from "Strongly Agree" to "Strongly Disagree")

    (a) Online privacy is really a matter of my right to exercise control and autonomy over decisions about how my information is collected, used and shared.
    (b) Control of my personal information lies at the heart of privacy.
    (c) I believe online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.
    (d) Companies seeking information online should disclose the way data are collected, processed, and used.
    (e) It is very important to me that I am aware and knowledgeable about how my personal information will be used.
    (f) It usually bothers me when online companies ask me for personal information.
    (g) When online companies ask me for personal information, I sometimes think twice before providing it.
    (h) It bothers me to give personal information to so many online companies.
    (i) I'm concerned that online companies are collecting too much personal information about me.
    (j) Online companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.
    (k) When people give personal information to an online company for some reason, the online company should never use the information for any other reason.
    (l) Online companies should never sell the personal information in their computer databases to other companies.
    (m) Online companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.
    (n) If I receive a financial incentive to share my location, the business operating that location is entitled to receive some personal information about me.

13. What is your age?

    ◦ 18 - 25
    ◦ 26 - 33
    ◦ 34 - 41
    ◦ 42 - 49
    ◦ 50 - 57
    ◦ 58 - 65
    ◦ 65 and above

14. What is your gender?

    ◦ Male
    ◦ Female
    ◦ Prefer not to respond
    ◦ Prefer to self-describe _____

B Interview Script

Demographics

1. Record Age, Gender
2. How would you rate yourself on a scale of 1 being very unconcerned to 5 being very concerned, on your concern regarding:
   (a) Privacy in General
   (b) Online Privacy
   (c) Online Security
   (d) Security in chat services

Pre-study Questions

1. What messaging applications do you use?
2. How would you rate your trust in this applications security?
3. Have you heard of end to end encryption? (If not can explain what it is)
4. What makes you want to use a chat service?
5. Would you be open to learning more about end to end encryption chat services?

Walkthrough

In this section, we will have two phones with WhatsApp and riot installed, and a laptop with PGP installed. The initial accounts will be provided for the applications so they do not have to go through making an account as it is fairly similar across all applications and we are not measuring that part of usability. The user will be then tasked with trying to do a key exchange with the other person (i.e. one of us who has the other phone) and attempt to send a message to the other person successfully. The user will then be tasked with looking around the application to get a feel for it.

Getting a feel for it will include looking at settings, how to send media, and other features of the applications. Throughout the process of the study one of us will be taking notes documenting what they say on what screen. After they have completed a certain screen they will be asked if they have any comments or concerns about that page. Finally once the user finishes the application they have started with they will be asked how the application felt and if they have suggestions on what could improve it and what they felt was lacking. They will then move onto the next application.

Once finishing all of the applications they will be presented with these final questions:

1. Which application did you feel you liked the best?
2. Why did you like this application? Be specific. (UI, feel of security, messaging features)
3. What was the application you disliked the most?
4. Why did you dislike this application? Be specific. (UI, feel of security, messaging features)
5. What is your view on these chat services? Do you feel you might explore end to end encryption chat servces?