Pre-interview explanation-

In our study, we wish to check whether people will use our face cloaking system and most importantly, which parameters they prefer (parameters that control the privacy-usability metrics). We want to understand how people are willing to perturb their images for the sake of their privacy. For this purpose, we will conduct an interview and divide it into two parts:

1. The first part consists of general questions that assess the desire of people to protect themselves from the identification of their faces. Namely, the willingness to perturb their images to avoid this, and it also consists of several general questions about privacy.
2. The second part is directly related to our product. We prompt every respondent to provide his image, then we display some perturbed images of it. Next to each image, we show how well it protects privacy, namely, how different face recognition systems would be able to recognize this face on average. Firstly, we show the original image and perturbed images with low, medium, and high privacy levels (20%, 50%, 80% attack success) of our product outputs. If the respondent chose the original image, then, for research purposes, we display more images with fake privacy levels, and not necessarily authentic images we get from our product. For example, if we see that instead of a photo with a small perturbation, a person chooses the original one, we can intentionally increase the success rate of the attack. Or if we see that even with a high percentage of success and a slight change in the photo, a person still chooses the original one, we will introduce a new more minor perturbation that our current product cannot give out. Thus, we can infer the desired visuality changes and attack success rate we have to achieve by improving our algorithm, to make our product usable.

After receiving the answers to the interview, we will be able to answer the following research questions:

1. How willing are people, in general, to sacrifice image quality for security?
2. What is our target audience? (which people will mostly want to use our product)
3. What are the main problems with our particular product? (Is it runtime, too obvious noise, or something else?)

From the answers to these questions, we will be able to understand how much our product is needed in general, which audience should be targeted in future research, and what product problems should be paid attention to in the first place.

We will also gather demographic information from our interviewees, which we later use to statistically extract their preferences according to a chosen context (such as sex, age range, geographic location, social-economic situation, religion, etc.)

For young users (up to age 16), we know that their parents act as a significant role in their daily choices. Directing the application to parents to protect their children is also a part of our future goal since we think that children are the most vulnerable to the possible consequences of identification across all social networks, as children are more vulnerable in general.

Interview-

-Greetings. We are the face-cloaking team. Nice to meet you! First, we will ask you to answer a couple of questions so we can get to know you better.

1. What is your gender?
2. What is your age?
3. What is your monthly salary?
4. Do you live alone? If not, with whom?
5. Where do you live?
6. What is your religion? How would you consider yourself religious on a scale of 1-5?
7. How much time on average do you spend on social media every day?

-Now that we've gotten to know you a little, we're going to talk to you about internet security and privacy.

1. Do you think that your privacy has been significantly reduced due to social media?
2. Tell us, from 1 to 5, how concerned are you about your internet privacy?

[We toss a fair coin, if tails, do the next:]

> -Now, we want to tell you a little about what is happening in the world and how your privacy is at risk. Imagine a normal situation, you're on a vacation abroad with friends and you decide to post your photo at the sea on Instagram. It would seem that you posted this only for close friends, which means the photo is safe, right? Not really. Your photo got on the Internet, which means that the information that is stored in the image is now prone to exploitation. Large companies, such as Instagram and Facebook, have advanced technologies in the field of photo processing, including face recognition. This means that you and your friends got into their database by posting a photo. Seeing your and your friend's faces, the net understands from the photos it has in its database

who you are, what you did last weekend, who you are friends with, what you eat for dinner, what you are interested in, and so on. This list is endless, the essence is simple - the net knows everything about you. Isn't this a privacy issue?!

-Now we ask again.

1. Tell us, from 1 to 5, how concerned are you about your internet privacy?
2. Were you interested in what we talked about?
3. Have you learned something new?

-Now we are moving on to more practical things. Please provide an image with your face, the one you would like to post on the social network.

-We will offer you a choice of various perturbed versions of your photo and next to them, in percentage terms, the chance of successfully masking your face from face recognition systems. Each time we ask you to choose the photo that you would post on social media if you had the opportunity to choose only from what you see.

[Each time, we will give a choice of the original image and 3 perturbed images as explained in the pre-interview. After each user's choice, in case he chooses the original image, we will give other 3 perturbed options that are closer to the previous options, in terms of quality and accuracy of cloaking. Both perturbation and accuracy for the first time will be from our product, but further, we will also use fictitious indicators and perturbation, which by now we cannot achieve using only our product.]

-Thank you for participating! Do you have any unsaid words? What specific issues have been bothering you? It's time to say them!

-Goodbye and thanks again!

Post-interview analysis-

The first part of the interview is for statistics. With its help and answers to the second part, we will understand who is interested in our product in the first place, that is, we will find the target audience, to which our product will be mainly directed in the future.

In general, we will be able to use the following metrics:

- Dropouts- the percentage of people who completed the interview will show interest of people in our topic and in particular in our product. The more people of a certain category did not finish the interview to the end, the less their interest in the topic of security-privacy.
- The percentage of people who change their answer to a question about their internet privacy concerns will indicate the percentage of people who are not aware of these issues.
- The most frequently selected perturbations will point us to the most requested perturbations, namely what are the best parameters to use in our product in order to increase the usage of end users.
- By telling more people about the dangers to their privacy, we will understand how people understand these dangers. So, for example, if after our explanation their answer to the question about their concerns about Internet privacy does not change, we will understand that this person knew about these dangers. This will give us the parameters of the most requested perturbations, which we can use as options in our product. We will also understand how well our product works. For example, if people choose not a fictitious perturbation, but ours, then it is acceptable. By this, we can conclude what is the turning point in terms of security-privacy which will make our product usable.

Now we are able to answer our main research questions - we can tell how many users chose any perturbed image over the original (it will indicate how many of them are willing to sacrifice image quality for security). Following this, we can use the demographic data in order to segment the top target audience that will probably use our system and finally find out what parts of our tool should be improved.