Effect of Mood, Location, Trust, and Presence of Others on Video-Based Social Authentication

Cheng Guo
Clemson University

Brianne Campbell
Clemson University

Apu Kapadia
Indiana University

Michael K. Reiter
Duke University

Kelly Caine
Clemson University

Abstract

Current fallback authentication mechanisms are unreliable (e.g., security questions are easy to guess) and need improvement. Social authentication shows promise as a novel form of fallback authentication. In this paper, we report the results of a four-week study that explored people's perceived willingness to use video chat as a form of social authentication. We investigated whether people's mood, location, and trust, and the presence of others affected perceived willingness to use video chat to authenticate. We found that participants who were alone, reported a more positive mood, and had more trust in others reported more willingness to use video chat as an authentication method. Participants also reported more willingness to help others to authenticate via video chat than to initiate a video chat authentication session themselves. Our results provide initial insights into human-computer interaction issues that could stem from using video chat as a fallback authentication method within a small social network of people (e.g., family members and close friends) who know each other well and trust each other.

1 Introduction

Web services and mobile apps mostly rely on users' self-provided passwords for authentication. However, passwords are easy to forget: nearly three-quarters of people report that they often or sometimes forget a password [69]. A survey study conducted by SAP Inc. found that over the course of 12 months, 84% of users forget a password at least once [35]. At the same time, passwords are relatively easy to steal. Theft of credentials happens regularly via users being phished or users sharing the same passwords across many platforms, one of which is compromised [7]. In both cases, users may be forced to use a form of secondary or fallback authentication mechanism to regain access to their accounts.

The most common secondary or fallback authentication mechanisms are security questions and out-of-band communications, which are unreliable and/or hard to use. For security questions, previous research has shown that answers are easy to forget and maybe guessable by users' acquaintances [73, 77, 94]. Forgetting passwords, user names, and answers to security questions are the most common reasons for authentication failures [61]. Fallback authentication via SMS or email is preferable to security questions in terms of usability and security [13]. However, mobile phones are frequently lost or stolen [15, 21, 80], and when this occurs, the legitimate owner may not receive the SMS or email. For these reasons, the National Institute of Standards and Technology (NIST) has suggested avoiding SMS or email as out-of-band authenticators [38].

To address the risks associated with SMS and email as out-of-band authenticators, Libonati and colleagues [60] developed a system where a phone would remain usable only while in its owner's possession, as confirmed by the owner's social network members when interacting with the owner. For example, video chatting with the owner would present an opportunity to *notarize* that the owner was still in possession of the phone, in which case the owner's phone would continue to function as normal. If a sufficiently long time passed without such a successful notarization, then the phone's functionality would be degraded, and critical capabilities (e.g., approving a fallback authentication push notification or checking email) rendered unavailable until such authentication was obtained. Alternatively, a notarization could be required to perform a critical transaction with the device.

Attempting to involve another person to act as a notary to confirm the owner's possession of their phone naturally raises many questions relating to feasibility and motivation. Libonati and colleagues [60] attempted to answer some of these questions via a lab study. In their study, participants were randomly assigned to act as either a supplicant—a person requesting authentication, or a notary—a person who supported authentication. While physically separated in the lab, the notary interacted with the supplicant via video chat, decided whether the supplicant was present in a set of images, and, if so, identified the supplicant. They found that, in the lab, notarization by strangers is effective and argued that this might be useful in combating device theft. However, their study did

not address whether video-based social authentication would be usable by people outside the lab and over a longer period of time. If it is, what factors may affect people's ability and willingness to use this form of fallback authentication?

To explore users' perceived willingness to use video-based social authentication, we performed a four-week-long ESM (experience sampling method) study. The ESM study simulated important aspects of the authentication process. We sent simulated video authentication requests to participants' mobile phones and measured how participants reacted to these simulated requests. We also measured factors like mood, location, trust, and presence of others to see how these factors affect people's perceived willingness to use video authentication. In this study, we focused on the following two research questions.

- **RQ1**: *What is the effect of mood, location, trust, and presence of others on people's perceived willingness to use video-based social authentication?*
- **RQ2**: *What are the reasons people agree or decline to participate in simulated video-based social authentication at the moment?*

To summarize, our work has three major contributions:

- Our results demonstrate people's perceived willingness to use video chat as a secondary or fallback social authentication method, especially within a small social network of people who know each other.
- We find that mood, location, trust, and presence of others are contextual factors that are associated with the perceived willingness to use such an authentication.
- Our paper offers initial insights into human-computer interaction issues stemming from simulated use of such authentication and presents implications that may be useful for designing and implementing video-based social authentication systems.

2 Related Work

2.1 Fallback Authentication

2.1.1 Security questions

Security questions are widely used as a secondary or fallback authentication mechanism when primary passwords are lost, forgotten, or users need to recover their accounts for other reasons. Using security questions as an authentication method is well studied. For example, research has found that while answers to security questions are easy to recall, about one-third of the answers can be guessed by those who are close to the users [94], and nearly forty percent can be guessed by parents, partners, close friends, etc. [73]. Bank security questions had a set of usability and security issues, including inapplicability, ambiguity, lack of memorability, guessability, attackability, and automatic attackability [75]. Twenty percent of the answers to the security questions used by top webmail providers cannot be recalled by users [77], but many can be guessed by attackers [77]. More recently, a study conducted by Google in 2015 about security questions revealed that it is nearly impossible to design security questions that are both secure *and* memorable [13]. Based on these results, some best-practice suggestions favor more reliable alternatives for fallback authentication [13].

2.1.2 Out-of-band communications

One popular alternative to security questions is the use of out-of-band communication such as SMS or email. Using SMS or email as fallback authentication is considered more secure, reliable, and preferable to security questions by big tech companies such as Google [13]. Beyond that preference, SMS is also preferred over email because people often use the same password for their primary account and recovery email, and some email providers recycle inactive email addresses [13]. However, using SMS for fallback authentication is also risky due to the security and privacy vulnerabilities of mobile phones and SMS. SMS authentication messages often include the name of the application for which the message was intended, which may risk compromising users' accounts [89]. For these reasons, the National Institutes of Standards and Technology deprecated SMS as an out-of-band verification method, though they have recently softened this guidance [38].

Furthermore, mobile phones are frequently lost or stolen. For example, in the U.S., 31% of mobile phone owners have had their mobile phone lost or stolen, and 12% of them have had another person access their phone in a way that they felt their privacy was invaded [15]. Current solutions such as Google's 'Find your phone' [37] and Apple's 'Find my iPhone' service [4] inadequately protect the data on devices since they can be disabled or hacked by others [62, 78, 90]. Moreover, the protection offered by these services is reactive, meaning the data on the device remains vulnerable until users realize their devices are stolen or lost and then take actions to lock them.

2.2 Social Authentication

Social authentication, which is defined as "the direct or indirect utilization of social knowledge or trust relationships in human-computer authentication systems deployed in online or offline contexts" [2], has been shown to be a promising fallback authentication mechanism. For example, Schechter and colleagues designed, built, and tested a social authentication system for Windows Live ID and found that about 90% of participants who made the effort to call trustees successfully authenticated [77]. This form of social authentication can be improved by adding multi-level social networks to automate

the process [93]. Another social authentication protocol used mobile phones to issue and use tokens to authenticate [83]. Facebook launched its trustee-based social authentication system called Trusted Friends to recover locked accounts in 2011 and redesigned it to Trusted Contacts in 2013 [28]. The redesigned Facebook social authentication system added a layer to ask users to verify information and interactions about their social contacts to enhance security [50]. However, Facebook's Trusted Contacts was found to have a number of security risks [51]. Also based on Facebook, Yardi and colleagues designed and built a photo-based web authentication framework [91]. In this social authentication system, users verify others with tagged user photos in a group. Besides photos, social authentication can also use videos to verify users' identity. Sherman and colleagues found that most (68%) of the participants chose video verification over photo ID cards and voter ID cards in terms of the accuracy in verifying individuals for voting [81]. Moreover, they found that most of the participants (74%) said they are willing or very willing to participate in video verification [81].

Another form of social authentication that could be used for fallback authentication is device notarization (DNo), which has inspired the study here. DNo was suggested as a way to allow users to proactively maintain and improve the security of their mobile devices [60]. DNo employs human-mediated, crowdsourced biometric authentication as a potential solution to the problem of remote authentication. In this system, a person from the crowd (the notary) confirms that the current device user (the supplicant) is, in fact, the device owner via a short video chat. Similarly, Shropshire and Menard proposed an approach using videos and trusted contacts as a form of fallback authentication [82]. In their approach, the supplicant uploads a video to the server. Then the notary confirms the identity of the supplicant by viewing the video from a text message. Video-based authentication may be suitable for protecting data of users deemed highly vulnerable or for high-value transactions, such as moving money between bank accounts. For example, using live video for authentication has recently been explored by the banking industry for high-value transactions [12]. In addition to other forms of video authentication, uploading a short video during enrollment [42] is currently being explored. While notarization is not expected to be used for frequent actions such as unlocking a phone because it would be too cumbersome, it could be effective for rare transactions such as password recovery [60]. Libonati and colleagues [60] also discussed potential privacy risks for both supplicant and notary and outlined the steps taken in their design to minimize those risks.

To date, DNo and most other social authentication systems have only been tested in lab settings. In the field, many external factors may affect the efficiency and the reliability of a social authentication system. For video-based social authentication, factors such as mood [72], location [74], trust [14], and presence of others [16] may affect users' perceived willingness to use it in the field. Therefore, in this work, we explore these issues in research questions RQ1 and RQ2.

3 Method

Our study had three steps. First, participants completed a pre-survey. Next, we used the experience sampling method [58] to collect data over four weeks from 30 participants. Finally, participants completed a post-survey. We organize our methods in the following five sub-sections: recruitment and participants, pre-survey, experience sampling, post-survey, and ethical considerations.

3.1 Recruitment and Participants

We advertised our study as "a study that uses video chat as an alternative form of authentication, instead of using passwords or security questions, for example." We recruited participants in two phases. First, we recruited participants via social media, flyers, and word of mouth. Then, since we wanted to recruit participants who already knew each other, we used snowball sampling, where existing participants suggest possible future participants from among their acquaintances [36]. Participants who expressed interest in joining our study were asked to provide the email address of one to ten individuals from their social network who might also be interested in our study. Subsequently, we invited all these individuals to participate via email that included a pre-survey. Participants were required to participate in the study together with at least one person they knew prior to the study. As a result, 36 people accepted our initial invitation and were qualified to participate in the study. Among these 36 participants, two participants had technical issues with their mobile phones, and four participants dropped out of the study after the pre-survey. Thus, 30 participants who owned at least one smartphone completed the study, and their data were used in later analysis. See Section 4.1 below for additional information about our participants. Each participant was awarded a $40 gift card after the completion of the study.

3.2 Pre-survey

The pre-survey (see Appendix A) had questions covering demographic items (including gender, age, race, income, and education) as well as mobile app usage and the perceived sensitivity of data captured by those apps. Participants were asked to list at least five and up to ten of their most frequently used mobile apps. Two questions adapted from those used by Gibbs, Ellison, and Lai [34] were added to allow us to categorize the applications in terms of data sensitivity from low to medium to high. The pre-survey also asked whether participants currently use PINs to lock their phones, whether they have ever used video chat before, and how many hours per week they spend on video chatting. Participants were asked

to list at least one and up to ten individuals from their social network who may also be interested in participating in the study with them. This list was not limited to close relations (e.g., family, friends) but could also include weak ones (e.g., strangers). We also requested that each participant upload a photo of themselves, which we used later in the ESM questionnaire. Finally, participants responded to a trust question about each individual they listed. Trust was assessed via an adapted version of a validated interpersonal trust scale [53]. Trust was categorized as low, medium, or high using this scale.

3.3 Experience Sampling

3.3.1 The experience sampling method

We used the experience sampling method (ESM) [58] in our study. Using ESM, participants are prompted to provide systematic self-reports (e.g., answers to questionnaires) about events as they occur throughout daily life [24]. One major advantage of ESM is it does not require participants to recall anything, which minimizes the effects of reliance on memory and reconstruction. Instead, it asks about participants' current activities and feelings [24]. ESM data may, therefore, be more reliable than data that must be recalled, because it is less susceptible to subject recall errors than other self-report feedback elicitation methods [26]. It is particularly well-suited and widely used for ubiquitous computing [24] and mobile device studies [10].

3.3.2 Group

We used the social network information participants provided in the pre-survey to form social networks for the purpose of the study. We placed six participants together in a group, which resulted in five groups total. Each group had some participants who knew each other and some participants who did not know each other prior to the study (i.e., strangers). We first paired the participants who already knew each other. Then we randomly placed these pairs in five groups to make sure there were both strangers and known people for every participant. As a result, two groups had three participants who knew each other, and the other three participants were strangers. The other three groups had two participants who knew each other, and the other four participants were strangers. We created groups consisting of both strangers and people who knew one another, so we could measure if trust in the person will affect people's willingness to use a video-based social authentication system. The same adapted version of the validated interpersonal trust scale [53] was used again to measure participants' trust in each group member. Trust was categorized as low, medium, or high using the same scale.

3.3.3 Procedure

Before the formal study, we used text explanations and a mock-up to simulate the authentication process and to help participants differentiate video-based social authentication from general video chat. Participants were instructed that they should think of the system as a way to recover accounts, rather than for primary authentication or general video chat. Participants were also instructed to provide the perceived willingness to use such authentication.

Participants agreed to receive SMS text messages from the researchers for the duration of the study and to respond via their mobile phone's web browser. Participants received two or three prompts per day over the four-week period between the hours of 9 AM and 9 PM. This resulted in 72 SMS prompts per participant over the four-week period.

Each SMS prompt signaled participants to fill out a response form about their perceived willingness to do a video authentication at that moment. There are two types of prompts: initiate and help. For an initiate prompt, participants were informed that they needed to initiate a video chat to gain access to one of the apps on their phone. The app and its sensitivity were selected based on participants' responses in the pre-survey. If a participant was willing to initiate a video chat for authentication, then the participant was asked to select one person from the six-person group (with six avatars presented, collected from the pre-survey) to send a video-based authentication request. For a help prompt, participants were informed that they were being asked to help one person (with an avatar presented, collected from the pre-survey) from the six-person group to gain access to an app via a video chat. The image of the avatar was used to simulate a video-based social authentication call, just as people would see each other in a video chat.

Participants received one initiate SMS and one help SMS per day. In addition, four times a week, they received an additional initiate or help SMS. Thus, each participant received nine initiate SMS and nine help SMS messages per week. To address the possibility of the time of day being an important factor of the willingness to initiate or help [63, 71], we wrote a program to randomly determine a time of day during the morning (9:00 AM – 11:59 AM), afternoon (1:30 PM – 4:29 PM), or evening (6:00 PM – 8:59 PM). Thus, each participant received six SMS messages in the morning, afternoon, and evening, respectively. We randomized the time points with rules since, in a real-world scenario, a video-based social authentication request could also happen at any time. Upon receiving an SMS, each participant was prompted to click a link in the SMS to take the ESM questionnaire. In the questionnaire, participants were given the option to decline or accept a video-based authentication (initiate or help). We then asked the reasons for the accept or decline decision. In the questionnaire, we also asked about participants' mood, location, and the presence of other people. Note that we did not ask partici-

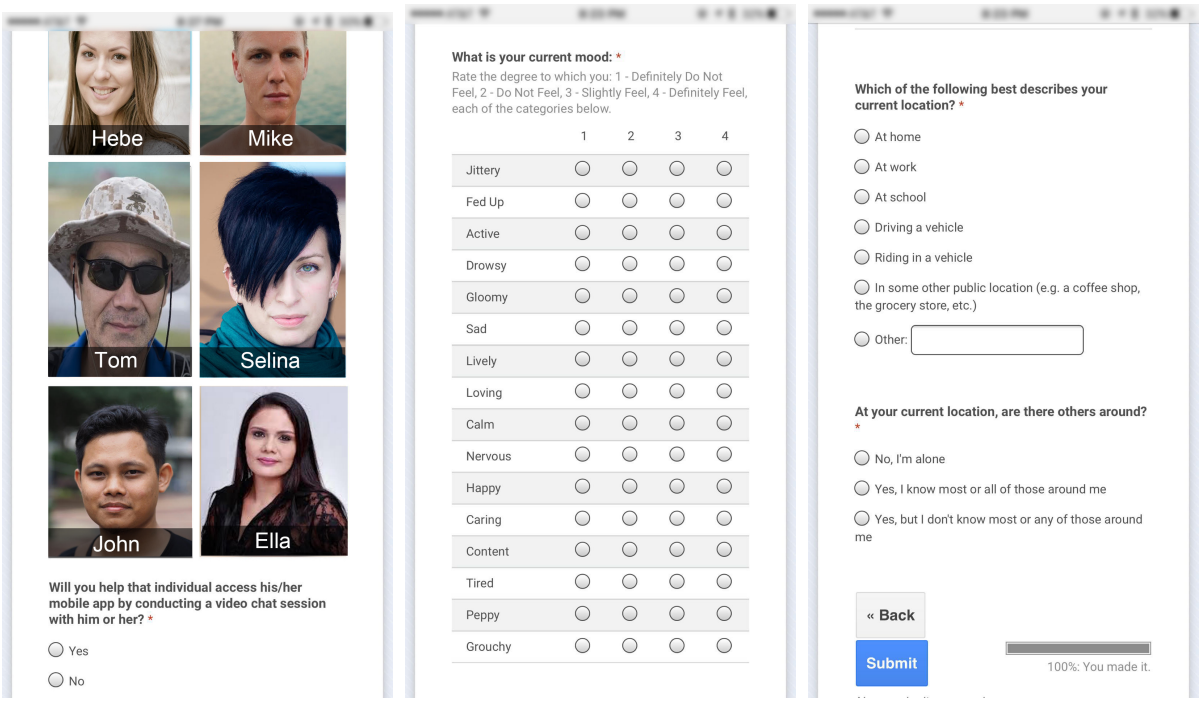

Figure 1: Example Interface of ESM Questionnaire

pants to do any real video chatting or authentication. Instead, we simulated the real video-based authentication scenario and asked for participants' perceived willingness to initiate or help with authentication via a video chat. As participants may not see the ESM questionnaires until later, participants were instructed, "If you do not see a text until later, respond to the survey based on what you were doing and how you were feeling at the time the text came to your phone, NOT when you saw it."

Overall, during the four-week period, 72 (2 types of request (initiate or help) $\times$ 9 per week $\times$ 4 weeks) SMS messages were scheduled to be sent to each participant. This resulted in 2,160 SMS messages in total. Due to human errors or technical issues, 1,992 SMS messages were successfully sent and received by participants. The human errors or technical issues stemmed from two issues: 1) manual typing issues from research assistants and 2) SMS delivery issues on participants' phones. An example interface of the ESM prompt can be found in Figure 1. The entire ESM questionnaire can be found in Appendix C.

3.3.4 Reasons to agree

The following options were provided for participants to choose from: Length of time we've known each other; What I know about them; I know I would recognize them effectively; They are responsive when I ask them to help me; We have lots of friends in common; We don't have many friends in common; I would want additional contact with them; I think they are attractive. We also provided an "other" option for participants to manually enter a response in a text box if needed. Note that some of the options provided were adapted from the pilot study (see Section 3.5).

3.3.5 Reasons to decline

The following options were provided for participants to choose from: I'm busy; I don't want to; I'm not in a location that could use video chat; I'm having network issues (e.g., no wi-fi, over data usage); I'm having technical issues (e.g., phone is broken, camera won't work); I don't trust anyone in my network. We also provided an "other" option for participants to manually enter a response in a text box, if needed.

3.3.6 Mood

Mood was assessed via the Brief Mood Introspection Scale (BMIS) [65]. BMIS allows us to compute a standard composite pleasantness score. The BMIS pleasant-unpleasant composite includes 16 items, and each item is measured by a four-point Likert scale [64]. We used this assessment to see if mood played a factor in people's willingness to accept or decline a video-based social authentication.

3.3.7 Location

Location was assessed via a question in the ESM questionnaire, which gathered where participants were when they were responding. The following options were provided to participants: at home, at work, at school, driving a vehicle, riding in a vehicle, and some other public location (e.g., a coffee shop, a grocery store). We also provided an "other" option for participants to manually enter a response in a text box, if needed. Because the SMS prompts were random, we had no idea where participants would be when they received the prompts. We asked participants to respond to the prompt as soon as they safely could, not while driving.

3.3.8 Presence of other people

Presence of other people was assessed via a question in the ESM questionnaire regarding whether the participants were around other people when they were responding. The following options were provided to participants: "No, I'm alone", "Yes, I know most or all of those around me", and "Yes, but I don't know most or any of those around me".

3.4 Post-survey

The post-survey (see Appendix B) had nine questions. First, we asked what type of mobile phone each participant used in the study. Then, we asked about participants' comfort (adapted from [52]) with video chat in general and their comfort with the idea of seeking identification from another person through video chat. Then, we asked participants which person from their group they prefer to have authenticate their identity and why they prefer that person. Finally, we asked three questions about their opinions on asking or giving help for video-based authentication. We closed the post-survey by asking participants for any additional comments about the study.

3.5 Pilot Study

We conducted a pilot study with ten participants for five days. During that period, we were able to test the procedure and fix technical issues related to sending and receiving SMS messages. Some of the response options we provided in the formal study were also adopted from the pilot study (e.g., "We don't have many friends in common" and "I think they're attractive" for agreeing to help.)

3.6 Ethical Considerations

The entire research protocol was IRB approved. Each participant read and signed the consent form before the study. All the participants volunteered to participate in the study and understood that they could withdraw from the study at any point without consequence. We told participants about the potential risks and benefits of taking part in this study and documented these on the consent form. The potential risks we noted were minimal and did not exceed the activities of everyday life, such as using a mobile phone to video chat. One potential risk we noted was that filling out survey questions about mood may cause participants to think about negative emotional states. To avoid disturbing participants' sleep, we decided to limit ESM prompts to 9 AM through 9 PM. We emphasized that all user data collected was to be kept strictly confidential. Only members of the research team had access to it, and the data was only used in this work.

	Participants	
Gender		
Female	17	57%
Male	13	43%
Age		
18-29	22	73%
30-39	5	17%
40-49	1	3%
50+	2	7%
Race		
White	24	80%
Asian & Pacific Islander	5	17%
Other	1	3%

Table 1: Demographics of participants

	N = 246	Mean Sensitivity (SD)
Finance	9	3.8 (1.2)
Shopping	9	3.4 (1.4)
Productivity	23	3.2 (1.3)
Social Networking	102	3.0 (1.1)
Utilities	15	2.3 (1.3)
Health&Fitness	3	2.7 (1.3)
Music	11	2.4 (1.1)
News	20	2.3 (1.2)
Navigation	11	1.9 (0.6)
Sports	9	1.8 (0.8)
Education	4	1.8 (1.0)
Game	18	1.8 (1.0)
Weather	8	1.8 (1.2)
Entertainment	4	1.3 (0.5)

Table 2: Popular apps reported by participants, ordered by sensitivity

4 Findings

We first provide an overview of our 30 participants in Section 4.1. We then report the mobile app usage self-reported by our participants in Section 4.2, which shows that our participants use similar mobile apps with many other mobile

Week	Initiate			Help			Total
	Sent	Received	Response rate	Sent	Received	Response rate	Response rate
1	261	194	74.3%	254	200	78.7%	76.5%
2	257	124	48.2%	261	180	70.0%	58.7%
3	219	134	61.2%	221	149	67.4%	64.3%
4	256	122	47.7%	263	133	50.6%	49.1%
Overall	993	574	57.8%	999	662	66.3%	62.0%

Table 3: Response rate to the ESM prompts by week, split by request type

	Initiate	Help
No	344 (59.9%)	337 (50.9%)
Yes	230 (40.1%)	325 (49.1%)

Table 4: Responses to the video chat request for authentication, split by request type (Excluding non-responses)

	Initiate	Help
No	344 (34.6%)	337 (33.7%)
Yes	230 (23.2%)	325 (32.6%)
Non-response	419 (42.2%)	337 (33.7%)

Table 5: Responses to the video chat request for authentication, split by request type (Including non-responses)

phone users. Also in Section 4.2, we report the sensitivity of these mobile apps rated by our participants. In Section 4.3, we present the response rate and the average response time of the ESM questionnaires. Since not all the ESM questionnaires got responded to, in the following Section 4.4, we interpret the rate of agreeing or denying the video chat for authentication in two approaches: excluding and including the non-responses.

In Section 4.5 and Section 4.6, we present the results of the predictors that influence the perceived willingness to use video chat as an authentication method. We found that trust of others, the presence of others, location, and mood had notable effects on the perceived willingness to use such an authentication mechanism (see Table 6 and Table 7 for details). We analyzed the results using repeated-measures logistic regressions with Generalized Linear Mixed-effects Models, which fits the experience sampling methods we used. To understand the effects of different values of each parameter, we conducted Tukey's post-hoc tests to adjust p values to account for family-wise errors [86]. Given the sample size and the effect size (odds ratio) we reported in the paper, we calculated the post-hoc power (all above 0.8), which means we had enough participants. The following predictors were used in the repeated-measures logistic regressions (for categorical predictors, we selected the most normative category as the baseline):

- the sensitivity of apps (for initiate); ordinal (low; medium; high)
- trust in person (for help); ordinal (low; medium; high)
- location; categorical (at home; at work; at school; driving a vehicle; riding in a vehicle; some other public location (e.g., a coffee shop, a grocery store)
- mood; continuous (from 1 to 4)
- presence of others; categorical (no other people around; I know most or all of those around me; I don't know most or any of those around me)
- timing; categorical (morning; afternoon; evening)

We then present the reasons for agreeing to help or declining to video chat in Section 4.7 and Section 4.8, respectively. Finally, we present the post-survey results in Section 4.9.

4.1 Participants' Demographics

Participants' demographic information was collected in the pre-survey (see Section 3.2 and Appendix A). All of our participants were recruited from the United States, distributed across ten different states. Among the 30 participants, there were more females than males (57% vs. 43%). Participants fell primarily into the age range of 18-29 years old (see Table 1 for details). Eighty percent of the participants were white, with the next most common race being Asian & Pacific Islander (17%). The participants self-reported a range of incomes: 23% reported incomes under $30,000, and 33% reported incomes over $75,000. The participants were also highly educated, with the vast majority (97%) having attended at least some college. The majority (63%) of the participants reported that they used a PIN to unlock their phones. About 83% of our participants self-reported having used video chat at least once before the study. Of those 25 participants who had used video chat before, most (84%) of them reported using video chat for less than two hours per week. Twenty-four percent of our participants self-reported not using video chat at all during a typical week.

4.2 Apps and Sensitivity

Participants self-reported 261 unique apps installed on their mobile phones (collected in the pre-survey, see Section 3.2 and Appendix A). We grouped these apps into 18 categories based on Apple's app category [48] (see Table 2). The most

Model *initiate* ~ (1|pid)	*Chi.sq*	*df*	*p*	*B(SE)*	2.5% *CI*	*Odds Ratio*	97.5% *CI*
+sensitivity	0.60	1	.440	0.11 (0.13)	0.86	1.12	1.45
+mood	26.10	1	**< .001**	1.75 (0.28)	1.33	2.04	3.22
+location *(baseline: at home)*	21.01	6	**.002**				
at work			**.001**	-1.21 (0.38)	0.14	0.30	0.63
at school			.294	-0.45 (0.43)	0.27	0.64	1.49
driving a vehicle			**< .001**	-2.42 (0.70)	0.02	0.09	0.31
riding a vehicle			.513	-0.40 (0.62)	0.19	0.67	2.30
someone else's house			.743	0.24 (0.72)	0.31	1.27	5.74
other public			.173	-0.61 (0.44)	0.22	0.55	1.31
+others around *(baseline: none)*	9.77	2	**.008**				
people I know			.158	-0.38 (0.27)	0.40	0.68	1.17
strangers			**.002**	-1.38 (0.44)	0.10	0.25	0.59
+timing *(baseline: evening)*	1.47	2	.480				
morning			.996	0.01 (0.27)	0.59	1.00	1.71
afternoon			.306	-0.29 (0.28)	0.43	0.75	1.31

Table 6: Effect of the sensitivity of apps, location, mood, presence of others, and timing on perceived willingness to initiate a video chat for authentication. Initiate is coded as 1. Do not initiate is coded as 0.

frequently occurring app categories were social networking (messaging, dating, photo sharing, etc.), productivity (email client, note-taking, task management, etc.), and news (television, video, RSS readers, etc.). This is consistent with the statistics on mobile app use [43], indicating that our participants were similar to many other mobile phone users. We also asked participants to rate the sensitivity of each app they reported (see Section 3.2). Finance apps (personal financial management, mobile banking, etc.), apps for shopping (Amazon, eBay, Starbucks, etc.), and productivity apps were rated as the top three most sensitive (see Table 2).

4.3 Response Rate and Time

Table 3 shows the responsiveness to the ESM prompts by week over the course of the four-week study. In week one, participants responded to 76.5% of all ESM prompts. In week two, the response rate dropped to 58.7%. In week three, the response rate stayed relatively consistent with week two, adding about five percentage points to a 64.3% response rate. During the last week, the ESM response rate dropped to 49.1%. This leveling off of participant responsiveness is consistent with other ESM studies [32]. This is common for ESM investigations [87] and highlights the importance of conducting the study over time. Across the entire study, participants responded to 62.0% of all the ESM prompts.

In general, participants were more likely to respond to help with a video chat request than to initiate a request ($\chi^2(1) = 15.09$, $p < .001$). The average response time for each prompt was 63.4 ($\pm$ 3.1) minutes. The agreed responses had significantly shorter response time than denials responses (45.2 mins *vs.* 78.2 mins, U = 231,610, $p < .001$). Across participants, the response rates were similar. For initiate prompts, they were between 52.6% and 70.2%. For help prompts, they were between 68.9% and 73.1%.

4.4 Effect of Type of Request

As we reported in Section 4.3, not all the ESM prompts received a response (which is common in ESM studies [32]). Thus, we examined the effect of type of request in two ways. The first was more conservative than the second: 1) considering all non-responses as denials; 2) ignoring non-responses and only examining the ESM prompts that received a response. In both cases, participants were more willing to agree to requests for help (49.1% of the time and 32.5% of the time, respectively) than to agree that they would initiate (40.1% of the time and 23.2% of the time, respectively) a video chat for authentication ($\chi^2(1) = 10.12$, $p = .001$, see Table 4; $\chi^2(1) = 13.27$, $p < .001$, see Table 5). Although the numbers vary between participants, all of the participants in our study agreed to initiate and help with a video chat for authentication at least once.

4.5 Predictors of Initiating a Video Chat

As shown in Table 6, location, mood, and presence of others had significant effects on the willingness to initiate a video chat for authentication, while the sensitivity of the app and timing had no significant effects. A Tukey's post-hoc test showed that while at work, participants were less likely to initiate a video chat for authentication than at home ($p = 0.020$, *odds ratio (OR)* = 0.30, *95% Confidence Interval (CI)*: [0.14, 0.62]). Similarly, while driving a vehicle, participants were less likely to initiate a video chat for authentication than at home ($p = .008$, *OR* = 0.08, *CI*: [0.02, 0.35]). The

Model *help* ∼ (1|pid)	*Chi.sq*	*df*	*p*	*B(SE)*	2.5% *CI*	*Odds Ratio*	97.5% *CI*
+trust	36.26	1	**< .001**	0.76 (0.13)	1.67	2.14	2.77
+mood	40.48	1	**< .001**	1.17 (0.23)	2.07	3.22	5.17
+location *(baseline: at home)*	32.28	6	**< .001**				
at work			**.001**	-1.29 (0.34)	0.14	0.28	0.54
at school			.148	-0.58 (0.40)	0.27	0.64	1.49
driving a vehicle			**< .001**	-3.11 (0.68)	0.01	0.04	0.15
riding a vehicle			.650	-0.25 (0.56)	0.26	0.78	2.35
someone else's house			.764	-0.17 (0.57)	0.27	0.84	2.65
other public			.146	-0.58 (0.40)	0.26	0.56	1.22
+others around *(baseline: none)*	16.65	2	**< .001**				
people I know			**< .001**	-1.00 (0.26)	0.22	0.37	0.61
strangers			**.002**	-1.30 (0.42)	0.12	0.27	0.62
+timing *(baseline: evening)*	3.62	2	.164				
morning			.100	0.41 (0.25)	0.93	1.51	2.46
afternoon			.110	0.40 (0.25)	0.91	1.50	2.46

Table 7: Effect of the trust in person, location, mood, presence of others, and timing on perceived willingness to help with a video chat for authentication. Help is coded as 1. Do not help is coded as 0.

more positive and pleasant their mood was, the more likely they were willing to initiate a video chat for authentication (p = .001, OR = 5.23, CI = [2.77, 9.86]). Participants were also less likely to initiate a video chat when they were with strangers than when they were alone (p = .005, OR = 0.25, CI: [0.11, 0.60]). When participants agreed to initiate a video chat for authentication, they tended to choose someone they knew prior to the study rather than someone they didn't know before the study (87.1% of the time vs. 12.9% of the time).

4.6 Predictors of Willingness to Help

As shown in Table 7, trust, location, mood, and presence of others had significant effects on the perceived willingness to help with a video chat for authentication, while timing had no significant effect. A Tukey's post-hoc test showed that the higher the in-person trust was, the more likely participants were to agree to help others with a video chat for authentication (p < .001, OR = 2.16, CI: [1.68, 2.77]). Note that since in-person trust and whether the participants knew each other prior to the study were almost perfectly correlated (r = .93, p < .001), we used only trust (leaving out whether participants knew each other prior to the study) as a predictor in the regression model. This was required to avoid multicollinearity [29], which is when independent variables in a regression model are highly correlated. We can see the trend in the descriptive data about how whether people knew each other prior to the study was related to their willingness to help: when the help request was sent from someone the participants knew prior to the study, participants were willing to help 63.3% of the time. On the other hand, when the help request was sent from someone the participants didn't know prior to the study, the participants were willing to help only 42.1% of the time.

While at work, participants were less likely to help with a video chat for authentication than at home (p = .002, OR = 0.27, CI: [0.14, 0.52]). Similarly, while driving a vehicle, participants were less likely to help with a video chat for authentication than at home (p < .001, OR = 0.05, CI: [0.01, 0.17]). Actually, when participants were driving a vehicle, they were significantly less likely to help with a video chat for authentication than any other location. The more positive and pleasant their mood was, the more likely they were willing to help a video chat for authentication (p < .001, OR = 6.87, CI: [3.80, 12.45]). Participants were also less likely to help with a video chat when they were with people that they knew than when they were alone (p < .001, OR = 0.37, CI: [0.23, 0.62]). Similarly, when participants were with strangers, they were less likely to help with a video chat than when they were alone (p < .001, OR = 0.27, CI: [0.12, 0.61]).

4.7 Reasons for Agreeing to Help

Participants were allowed to give one or more reasons why they agreed to help per ESM prompt response. From the 325 times participants agreed to help via video chat, participants provided 907 reasons, many of which overlapped. Across these 907 responses, seven stood out, accounting for more than 10% of reasons each (in other words, seven reasons accounted for 70% of the responses). The most frequently cited reason for agreeing to help was "the length of time the participant knew the other person," followed by their "confidence in their ability to recognize that person effectively" and "they are responsive when I ask them to help me" (see Table 8).

	Responses
Length of time we've known each other	145 (16%)
I know I would recognize them effectively	140 (16%)
They are responsive when I ask them to help me	133 (15%)
What I know about them	125 (14%)
We have lots of friends in common	97 (11%)
I think they are attractive	95 (11%)
I would want additional contact with them	94 (11%)
We don't have many friends in common	46 (5%)
Other	16 (2%)
- Appearance of other person as happy or friendly	4 (< 1%)
- To be helpful	3 (< 1%)
- Close relationship	3 (< 1%)
- Bored	2 (< 1%)
- Not busy	2 (< 1%)
- Believe the other person will help them	2 (< 1%)

Table 8: Reasons for agreeing to help with a video chat, sorted by frequency

	Initiate	Help
I'm busy	203 (59%)	219 (65%)
I don't want to	70 (20%)	32 (9%)
I'm not in a location to video chat	47 (14%)	40 (12%)
Other	8 (2%)	18 (5%)
Sleeping	8 (2%)	9 (3%)
I'm having network issues	3 (1%)	7 (2%)
I don't trust him/her	5 (1%)	3 (1%)
I don't know him/her	0 (0%)	6 (2%)
Sick	0 (0%)	3 (1%)

Table 9: Reasons for declining video chat, sorted by frequency

4.8 Reasons for Declining

When participants opted to decline to an ESM prompt to authenticate via video chat, we also asked reasons for declining. The most common reason they provided was that they were "busy" (59% for initiate and 65% for help; see Table 9). The percentage of "busy" was consistent across the four-week period (52.3%, 69.3%, 65.6%, 58.7%, respectively). The other common reasons included "I don't want to" and "I'm not in a location to use video chat". Participants also gave more "other" explanations (5% vs. 2%) when they were prompted to help versus initiate.

4.9 Post-Survey Results

In general, participants self-reported that they were comfortable with interacting through video chats (M = 2.2, SD = 1.1). Only 10% of the participants reported that they disagreed or strongly disagreed that they were comfortable interacting through video chats in general. When we asked about seeking authentication from another person through video chat, they were still relatively comfortable (M = 2.8, SD = 1). About 23.3% of the participants reported that they disagreed or strongly disagreed that they were comfortable seeking authentication through video chats. The majority of participants also had fun helping others (M = 2.5, SD = 1.1), would have liked seeing the other person on video chats when helping them (M = 2.6, SD = 1.2), and liked the opportunity to help other people (M = 2.3, SD = 1.2).

5 Discussion and Implications

We explored people's perceived willingness to use video chat as an alternative social authentication method. Furthermore, we explored the contextual factors that may affect people's perceived willingness to use such authentication. Our results suggest that people are, in general, willing to use video chat as a social authentication method. Specifically, we find that trust in other people, location, mood, and the presence of others are factors that could potentially affect people's perceived willingness to use social authentication. We included participants' quotes in the discussion, which are illustrative sources. The primary data was from the ESM questionnaires. The quotes just helped us to further interpret the data we saw from the logistic regression models.

5.1 Use Video-Based Social Authentication in a Small Group of People Who Know Each Other Well

Video-based social authentication differs from general video chat, in which the motivation for participation is usually the desire for closeness [56]. For video-based social authentication, for people who initiate the authentication, the motivation is usually the singular desire to get authenticated when primary authentication fails. For example, "*I think a verification through video chat is very secure if I cannot get access to the app and my family or friends can help me out.*" (P4). For people who help the authentication, the most commonly cited reasons for agreeing to help are "Length of time we've known each other" and "I know I would recognize them effectively." Examples included, "*Only because it's Alice*" (P19)[1] and "*Cause I like to help people and think I would recognize her*" (P11). Our study shows that the motivation of people participating in video-based social authentication is very different from participating in general video chats.

When participants declined to video chat to authenticate, the reason they most often gave was that they were busy. It was not lacking of ability (e.g., only 1 – 2% of the time was the reason a technical issue) or because of trust or familiarity issues (1 – 2% of the time) that participants declined (see Table 9), but rather because they were unable to since they were already engaged in other activities. It is also worth noting that under the circumstances of the study, participants were queried at random times, but under actual conditions, they

[1]The real name was replaced with "Alice."

would be initiating themselves, not via a prompt. Thus, it is likely that participants would be more willing to initiate since they would be likely available to do so.

Furthermore, when a person was asked to help and they declined, they gave substantive reasons for not helping instead of just saying that they did not want to (20% for initiate, see Table 9). This indicates that to not seem unhelpful or selfish, individuals want to clarify that it is not just that they "*do not want to*" help, but instead, they are sick, sleeping, or just do not know the person well enough to have a video chat for authentication.

These findings are in contrast to prior work on friendsourcing questions on Twitter, for example, which found that some participants found "friendsourcing anything at all was too onerous" [76]. While we can only speculate on the reasons for the differences in findings, there are some possible reasons behind these differences. For example, in our study, we did not offer any financial incentives for participants to either initiate or help. Sometimes financial incentives are a disincentive to participation [76]. Another possible reason is that in our study, participants only had to reach out to one member of their social network groups rather than their entire network of Twitter followers.

Our results show that social authentication, such as the video-based authentication we propose here, may benefit from existing social ties (relationships between people to share information, feelings, knowledge, and experience [30]). Participants who already know each other benefit not only from the ability to recognize each other, they are also willing to help each other. This finding is consistent with the near-perfect correlation between in-person trust and whether participants knew each other prior to the study (see Section 4.6). It is also consistent with the results generated from the logistic regression model (see Table 7), suggesting that trust is an efficient predictor of people's perceived willingness to help with a video-based authentication. People tend to help people they know and trust. For example, more than half of social network users self-reported that they had asked questions on social networks to get help [70]. Even when there are social costs to helping friends, people are still willing to help [76].

When participants agreed to initiate a video-based authentication, they were also more likely to choose someone they already knew (see Section 4.5). Participants reported confidence in their ability to recognize the person requesting help, which suggests the individual may experience a sense of accomplishment and self-confidence because of their abilities to succeed at the task of authentication. This is consistent with previous studies that people are more easily able to recognize familiar faces than unfamiliar faces [17, 20].

Our results also suggest that individuals may benefit from using video chat as an additional opportunity for social interaction since another motivating factor was that it gave the participant a sense of personal accomplishment stemming from assisting others. We interpret this based on the fact that some of the participants wanted to "*be helpful*". Boredom is also a factor, as it was mentioned multiple times by participants. For example: "*I'm bored, so why not?*" (P15) or "*I'm not busy right now.*" (P3). This comment, while not specifically mentioning boredom, is related since the participant did not have anything else going on that might prevent her from engaging in a video chat. Since they could have still chosen to ignore the prompt but did not, it suggests that people would welcome the opportunity to interact socially via this form of authentication. This is similar to other online social activities such as social questions and answers [33, 70, 79], where people ask for help, and others help when available.

These findings indicate that using video chat as fallback authentication, especially within a small group of people who know and trust each other (e.g., family and close friends), is potentially feasible.

5.2 Use Location and Mood Detection for Video-Based Social Authentication Systems

Our results show that when individuals were at home and when they were alone, they agreed to initiate and help more often. This differentiates video-based social authentication from general video chat at home, where, for example, video chat with family or friends often involves multiparty interactions [56]. In other single party video chats, for example, people who use video chats at a long distance often use other techniques such as an instant message to check if the partner is in a location that is good for video chats first [3, 54, 72]. But as we discussed earlier, in our study, participants received random prompts. Our study reveals that location is one of the key factors for video-based social authentication. For example, *"while I think it is a very secure way to verify who someone is, sometimes I did not have the flexibility or availability to verify anyone in my network right when they needed me. I was often in meetings, driving in my car, or coaching hockey for my children and did not see the texts until much later."* (P25).

In real-world situations, people may be able to connect with each other in advance to enhance the response rate and response time of the video-based social authentication. Previous research has used location as a contextual factor to adapt the form of authentication [5, 44, 59]. Our paper extends these works to further suggest that video-based social authentication may be most appealing as an option when people are at home and alone. Future video-based social authentication could use location detection to help people choose whom to ask for help in getting authenticated.

As we expected, a pleasant mood was associated with participants being willing to authenticate via video chat. What is not clear is the directionality of this relationship. Is it that participants who were in a more pleasant mood already were willing to use video chat to authenticate? Or is it that when participants reported that they would agree to help with a

friend to authenticate via a video chat put them in a more pleasant mood? Research on social networking-based chat services indicates that messages between members of a social network group can increase feelings of well-being and connectedness [19].

Furthermore, research on altruism and helping behaviors suggest that when people help others, it may improve their own mood [8, 39]. If participants realized this, they have been more, instead of less likely to respond when they were in a pleasant mood. However, if participants were worried about how their negative effects may affect others, they might have been less willing to authenticate via video chat. One participant's response sheds some light: "*I'm grumpy in the morning, and I don't think I would be very enjoyable to video chat with right now.*" (P9). This comment suggests that existing mood affects the willingness to use video chat for authentication, and also demonstrates a recognition that the other person would be negatively affected by their unpleasant mood as well. Future video-based social authentication systems could consider integrating wearable devices that detect mood (e.g., [25, 92]) if designers wanted to use mood as a decision criterion for choosing notaries.

5.3 Potential Pitfalls and Solutions for Video-Based Social Authentication Systems

5.3.1 Interaction and attractiveness

Our results reveal that people in video-based social authentication maybe not only be motivated by helping one another but may also be motivated by the interaction with others as a beneficial form of social contact. This is similar to one of the motivations of friendsourcing, which is connecting to social networks [11]. In addition, participants also sometimes reported that when they were willing to help, the reasons were because: they wanted additional contact with the other person (11%), they thought the other person was attractive (11%), or the appearance of other people as happy or friendly (4%). For example, "*He has a nice smile!*" (P26). One participant even combined these reasons boldly, saying, "*Honestly, I'm only willing to help them because they're hot, that's why I want more contact with them.*" (P10). This participant wanted more contact with the other participants because they perceived them as attractive. They thought of the simulated authentication opportunity as a way to achieve more contact.

Our finding that some people reported they were motivated, at least in part, by how attractive the chat initiator was, is not surprising or unique. People who are physically attractive benefit from many advantages. For example, attractive people are paid more, get higher fringe benefits [27], are more highly trusted [22, 40], are able to charge higher prices for Airbnb listings [49], are more likely to be elected to public office [55], and perform better in high school and university [23, 31]. One reason for these benefits is that people tend to respond to attractive individuals with approaches and affiliative tendencies [88]. Some researchers even argue that a reason physically attractive people live longer than less attractive people is because of accrued benefits over a lifetime [46].

Our finding that a reason people cited for their willingness to help was when the initiator was attractive is consistent with the body of research on the positive relationship between physical attractiveness and receiving help [9]. Across many situations, people are more willing to help people they perceive as attractive. However, while physically attractive people are more likely to receive help across the board, this aspect of human bias should ideally not be amplified by technology.

We acknowledge that, without thoughtful consideration, video-based social authentication, like all technology that includes images of users, has the potential to extend or exacerbate existing biases against less attractive people. In this case, it is possible that less attractive people may have a harder time getting someone to help authenticate them than more attractive people. However, it is important to note that attractiveness was not one of the top five reasons people gave for agreeing to help someone with a video chat. The majority of reasons people gave were knowing someone a long time, being able to effectively recognize them, how responsive they are, and the number of friends they have in common. So, while people cannot change many aspects of their physical attractiveness, they do have control of many other reasons people would authenticate them. For example, users could choose authenticators they've known for a long time and/or reciprocate when they are asked for help.

Furthermore, this finding reinforces our perspective that video-based social authentication may only be suitable as a fallback authentication method and may not be appropriate as the primary authentication method. It would seem to be most appropriate for use within a small group of people who know and trust each other well (e.g., family members and close friends). Interaction Appearance Theory suggests that perceptions of physical attractiveness can be altered by social interaction [1]. Positive social interaction leads to higher perceptions of physical attractiveness among people who interact with each other regularly [1]. In a situation where people used video-based social authentication over a long time period, it is possible that users could even build such regular social interactions that their mutual perceived physical attractiveness could increase [1].

5.3.2 SMS usability and reliability

We chose to use SMS to deliver ESM questionnaires due to its ubiquitous availability and universal support by mobile devices and cellular providers, as our participants used different devices and services. However, SMS may not always be usable and reliable. Prior research has shown that the SMS delivery failure ratio can be as high as 5.1% during normal operating conditions [67]. Indeed, in our study, some of the

ESM questionnaires were not delivered (see Section 3.3.3). Moreover, the mechanism will not be secure against a compromised phone. Although the situation did not happen during our study, and we did not use SMS for authentication, we argue that future video-based social authentication should avoid using SMS due to its usability and reliability issues.

6 Limitations

This study has a number of limitations. One limitation is that our sample is composed primarily of people living on the east coast of the U.S. and therefore may not be representative of other areas of the United States or the rest of the world. Furthermore, like other published studies [6, 47], our sample is mostly white, highly educated, young, and high socio-economic status. On the other hand, participants' phone use, the apps they had on their phone, and passcode use were similar to many mobile phone users in the U.S. [15, 43]. We recruited participates in two phases. First, we recruited participants using social media, flyers, and word of mouth. Then, we used snowball sampling to recruit members of those participants' social networks. Social networks tend to be demographically homogeneous [66]. We prioritized social network connections because one of our goals is about whether members of the social network would be more willing to help each other rather than strangers (we found they were). Therefore, these results may serve as a foundation for understanding what motivates people when social networks are used as part of the authentication process. We encourage replication of this work with a broader population.

Second, during the study, there were a few technical issues and human errors. For example, as we mentioned in Section 3, two participants were not able to receive any ESM messages, and some responses were sent incorrectly by participants (entered the wrong people's name they were helping) thus, we cannot match with participants' responses. We simply eliminated these participants and responses from the analysis. Given the overall response rate and the small number of these mistakes, we do not expect that the discarded responses impacted the overall results of the study.

Third, as in many similar studies [57, 68, 84], participants did not respond to every prompt we sent them. Participants in this study exhibited around a 47 – 64% response rate for the last two weeks of this study. We do not know whether non-responses indicate a lack of willingness to engage in authentication via video-chat, although to be conservative, as we discussed in Section 4, this is what we have assumed throughout this paper.

Fourth, there are potential security issues in the use of video chat as an authentication method such as video spoofing or "deep fakes" [85]. Future work could explore potential intervention mechanisms to help identify or prevent video spoofing. Future work could also explore privacy-enhancing technologies to prevent other potential privacy issues of using this system, such as harassment or stalking [41], since it is possible that people could misuse this system to stalk or harass others, as is unfortunately common in many other systems that connect people.

Fifth, as in all studies that rely on users' self-reported data, our results are limited by reporting errors [18] and respondent adherence [45] because of our reliance on assumptions about the compliance of our participants.

Sixth, although we did explore some of the factors such as emotion (mood), we did not explore all sociocultural variables in the study. Sociocultural and political-economic variables and the influence of power dynamics are factors that may influence the behavior of the sampled participants [89], but coverage of all these variables was beyond the scope of this paper. Future work should consider how these variables will influence the adoption and utilization of video-based social authentication by the public.

Finally, we did not require participants to complete an actual authentication process (i.e., we did not install software on their phones that prevented them from using any of their apps). Instead, we used ESM to simulate an authentication process by video chat. Since we prompted participants at random times throughout the day and surveyed them at that moment, we were able to gather large amounts of *in situ* data about how a person might be motivated to engage in, or not engage in, friendsourced authentication based on their various feelings, location, and level of trust. We anticipated that the benefits of surveying participants on their own unmodified phones would outweigh the drawbacks of a modified authentication process, at least initially. Furthermore, we were interested in gathering a large amount of data about emotion, time of day, etc. In a real authentication scenario, we anticipate that social authentication would be a rare event, perhaps saved for a password reset or other unusual event rather than multiple times per day, week, or even month event. Waiting for these events to occur would have meant we were not able to interrogate a large number of events to determine the effects of feelings, location, etc.

Notably, some participants reported that they thought they were indeed helping the people in their network by authenticating them. For example, one participant mentioned: "*I thought every time I texted for help, that person had chosen me when they selected someone to help them access their app. I thought it was weird since I don't actually know them, but I helped anyway.*" (P8). While another reported: "*I just wanted to be helpful.*" (P13). This indicates that at least some participants thought their responses were behavioral rather than attitudinal. Future work should examine whether the results we report here replicate during real authentication situations.

7 Conclusion

Finding new ways to make authentication more secure and reliable is crucial. Our research suggests social authentication

using video chat might benefit end-users while also leveraging a form of human-to-human identification that could be more reliable than alternatives. Our paper provides insights into contextual factors that may affect the use of video chat as a fallback authentication method in a small social network (e.g., family members and close friends). Among these contextual factors, the trust of others, mood, location, and the presence of others stand out as they are associated with the willingness to use video chat as a fallback authentication method. Besides these opportunities, all authentication methods, including video-based social authentication, have challenges. For example, the response rate could heavily rely on its users' social ties and the contextual factors we found. While having these challenges, all the participants in the study agreed to initiate and help a video-based social authentication prompt at least once. When excluding non-responses, participants agreed to initiate or help for more than 40% of the time. The majority of the participants also showed the comfort of using video-based social authentication. With having these opportunities and challenges in mind, we believe video-based social authentication is a meaningful direction and needs further exploration. Our paper offers useful insights for the design of future, video-based social authentication systems.

Acknowledgments

We thank Dr. Katharina Krombholz and the anonymous reviewers for their helpful feedback on this work. We also thank Peter Barnett, Trevor Ormson, and Subina Saini for their help setting up the study. Finally, we thank Dr. Bart Knijnenburg and Dr. Emily Sidnam-Mauch for their comments on this work. This material is based upon work supported in part by the National Science Foundation awards CNS-1228364 and CNS-1228471.

References

[1] Kelly Fudge Albada, Mark L Knapp, and Katheryn E Theune. Interaction appearance theory: Changing perceptions of physical attractiveness through social interaction. *Communication Theory*, 12(1):8–40, 2002.

[2] Noura Alomar, Mansour Alsaleh, and Abdulrahman Alarifi. Social authentication applications, attacks, defense strategies and future research directions: a systematic review. *IEEE Communications Surveys & Tutorials*, 19(2):1080–1111, 2017.

[3] Morgan G Ames, Janet Go, Joseph'Jofish' Kaye, and Mirjana Spasojevic. Making love in the network closet: the benefits and work of family videochat. In *Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work*, pages 145–154. ACM, 2010.

[4] Apple. Keep track of what's important, 2017. Retrieved February 5, 2021 from https://support.apple.com/explore/find-my.

[5] Patricia Arias-Cabarcos and Christian Krupitzer. On the design of distributed adaptive authentication systems. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, 2017.

[6] Jeffrey J Arnett. The neglected 95%: why american psychology needs to become less american. *American Psychologist*, 63(7):602, 2008.

[7] Dirk Balfanz, Richard Chow, Ori Eisen, Markus Jakobsson, Steve Kirsch, Scott Matsumoto, Jesus Molina, and Paul van Oorschot. The future of authentication. *IEEE Security & Privacy*, 10(1):22–27, 2012.

[8] Alixandra Barasch, Emma E Levine, Jonathan Z Berman, and Deborah A Small. Selfish or selfless? on the signal value of emotion in altruistic behavior. *Journal of Personality and Social Psychology*, 107(3):393, 2014.

[9] Peter L Benson, Stuart A Karabenick, and Richard M Lerner. Pretty pleases: The effects of physical attractiveness, race, and sex on receiving help. *Journal of Experimental Social Psychology*, 12(5):409–415, 1976.

[10] Niels Van Berkel, Denzil Ferreira, and Vassilis Kostakos. The experience sampling method on mobile devices. *ACM Computing Surveys (CSUR)*, 50(6):93, 2017.

[11] Michael S Bernstein, Desney Tan, Greg Smith, Mary Czerwinski, and Eric Horvitz. Personalization via friendsourcing. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 17(2):6, 2010.

[12] Pratik Bhakta. Rbi mulls live video authentication for customer verification, 2018. Retrieved February 5, 2021 from https://economictimes.indiatimes.com/industry/banking/finance/banking/articleshow/67018496.cms.

[13] Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google. In *Proceedings of the 24th International Conference on World Wide Web*, pages 141–150, 2015.

[14] Nathan Bos, Darren Gergle, Judith S Olson, and Gary M Olson. Being there versus seeing there: Trust via video. In *CHI'01 Extended Abstracts on Human Factors in Computing Systems*, pages 291–292. ACM, 2001.

[15] Jan Lauren Boyles, Aaron Smith, and Mary Madden. Privacy and data management on mobile devices. *Pew Internet & American Life Project*, 4, 2012.

[16] Jed R Brubaker, Gina Venolia, and John C Tang. Focusing on shared experiences: moving beyond the camera in video communication. In *Proceedings of the Designing Interactive Systems Conference*, pages 96–105. ACM, 2012.

[17] Vicki Bruce, Zoë Henderson, Craig Newman, and A Mike Burton. Matching identities of familiar and unfamiliar faces caught on cctv images. *Journal of Experimental Psychology: Applied*, 7(3):207, 2001.

[18] Alan Bryman. *Social research methods*. Oxford university press, 2016.

[19] Moira Burke, Cameron Marlow, and Thomas Lento. Social network activity and social well-being. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1909–1912. ACM, 2010.

[20] A Mike Burton, Stephen Wilson, Michelle Cowan, and Vicki Bruce. Face recognition in poor-quality video: Evidence from security surveillance. *Psychological Science*, 10(3):243–248, 1999.

[21] Rory Cellan-Jones. Government calls for action on mobile phone crime, 2010. Retrieved February 5, 2021 from http://news.bbc.co.uk/2/hi/technology/8509299.stm.

[22] Nawar N Chaker, Doug Walker, Edward L Nowlin, and Nwamaka A Anaza. When and how does sales manager physical attractiveness impact credibility: A test of two competing hypotheses. *Journal of Business Research*, 105:98–108, 2019.

[23] Giam Pietro Cipriani and Angelo Zago. Productivity or discrimination? beauty and the exams. *Oxford Bulletin of Economics and Statistics*, 73(3):428–447, 2011.

[24] Sunny Consolvo and Miriam Walker. Using the experience sampling method to evaluate ubicomp applications. *IEEE Pervasive Computing*, 2(2):24–31, 2003.

[25] Jonathan Daniel Cowan. Wearable monitoring and training system for focus and/or mood, March 19 2015. US Patent App. 14/323,770.

[26] Mihaly Csikszentmihalyi and Reed Larson. Validity and reliability of the experience-sampling method. In *Flow and the Foundations of Positive Psychology*, pages 35–54. Springer, 2014.

[27] Maryam Dilmaghani. Beauty perks: Physical appearance, earnings, and fringe benefits. *Economics & Human Biology*, page 100889, 2020.

[28] Facebook. How can i choose friends to help me log in if i ever get locked out of my account?, 2019. Retrieved February 5, 2021 from https://www.facebook.com/help/119897751441086.

[29] Donald E Farrar and Robert R Glauber. Multicollinearity in regression analysis: the problem revisited. *The Review of Economic and Statistics*, pages 92–107, 1967.

[30] Scott L Feld. The focused organization of social ties. *American Journal of Sociology*, 86(5):1015–1035, 1981.

[31] Michael T French, Philip K Robins, Jenny F Homer, and Lauren M Tapsell. Effects of physical attractiveness, personality, and grooming on academic performance in high school. *Labour Economics*, 16(4):373–382, 2009.

[32] Matthew Fuller-Tyszkiewicz, Helen Skouteris, Ben Richardson, Jed Blore, Millicent Holmes, and Jacqueline Mills. Does the burden of the experience sampling method undermine data quality in state body image research? *Body image*, 10(4):607–613, 2013.

[33] Rich Gazan. Social q&a. *Journal of the Association for Information Science and Technology*, 62(12):2301–2312, 2011.

[34] Jennifer L Gibbs, Nicole B Ellison, and Chih-Hui Lai. First comes love, then comes google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research*, 38(1):70–100, 2011.

[35] Inc Gigya. Survey guide: Businesses should begin preparing for the death of the password, 2016. Retrieved February 5, 2021 from https://www.gigya.com/resource/whitepaper/death-of-the-password/.

[36] Leo A Goodman. Snowball sampling. *The annals of mathematical statistics*, pages 148–170, 1961.

[37] Google. Find your phone, 2010. Retrieved February 5, 2021 from https://myaccount.google.com/find-your-phone.

[38] Paul A Grassi, Michael E Garcia, and James L Fenton. Digital identity guidelines. *NIST special publication*, 800:63–3, 2017.

[39] Kurt Gray, Adrian F Ward, and Michael I Norton. Paying it forward: generalized reciprocity and the limits of generosity. *Journal of Experimental Psychology: General*, 143(1):247, 2014.

[40] Anne Groggel, Shirin Nilizadeh, Yong-Yeol Ahn, Apu Kapadia, and Fabio Rojas. Race and the beauty premium: Mechanical turk workers' evaluations of twitter accounts. *Information, Communication & Society*, 22(5):709–716, 2019.

[41] Ralph Gross and Alessandro Acquisti. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, pages 71–80. ACM, 2005.

[42] Erste Group. Erste bank introduces video-based identification of new customers, 2017. Retrieved February 5, 2021 from https://www.erstegroup.com/en/news-media/press-releases/2017/01/23.

[43] Avery Hartmans. These are the 10 most used smartphone apps, 2017. Retrieved February 5, 2021 from https://www.businessinsider.com/most-used-smartphone-apps-2017-8.

[44] Eiji Hayashi, Sauvik Das, Shahriyar Amini, Jason Hong, and Ian Oakley. Casa: context-aware scalable authentication. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, pages 1–10, 2013.

[45] Joel M Hektner, Jennifer A Schmidt, and Mihaly Csikszentmihalyi. *Experience sampling method: Measuring the quality of everyday life*. Sage, 2007.

[46] Joshua JA Henderson and Jeremy M Anglin. Facial attractiveness predicts longevity. *Evolution and human behavior*, 24(5):351–356, 2003.

[47] Joseph Henrich, Steven J. Heine, and Ara Norenzayan. The weirdest people in the world? *Behavioral and Brain Sciences*, 33(2-3):61–83, 2010.

[48] Apple Inc. Choosing a category, 2020. Retrieved February 5, 2021 from https://developer.apple.com/app-store/categories/.

[49] Bastian Jaeger, Willem WA Sleegers, Anthony M Evans, Mariëlle Stel, and Ilja van Beest. The effects of facial attractiveness and trustworthiness in online peer-to-peer markets. *Journal of Economic Psychology*, 75:102125, 2019.

[50] Sakshi Jain, Juan Lang, Neil Zhenqiang Gong, Dawn Song, Sreya Basuroy, and Prateek Mittal. New directions in social authentication. In *Proceedings of the Workshop on Usable Security*. Citeseer, 2015.

[51] Ashar Javed, David Bletgen, Florian Kohlar, Markus Dürmuth, and Jörg Schwenk. Secure fallback authentication and the trusted friend attack. In *2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pages 22–28. IEEE, 2014.

[52] Gina M Jay and Sherry L Willis. Influence of direct computer experience on older adults' attitudes toward computers. *Journal of Gerontology*, 47(4):P250–P257, 1992.

[53] Cynthia Johnson-George and Walter C Swap. Measurement of specific interpersonal trust: Construction and validation of a scale to assess trust in a specific other. *Journal of Personality and Social Psychology*, 43(6):1306, 1982.

[54] Tejinder K Judge and Carman Neustaedter. Sharing conversation and sharing life: video conferencing in the home. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 655–658. ACM, 2010.

[55] Amy King and Andrew Leigh. Beautiful politicians. *Kyklos*, 62(4):579–593, 2009.

[56] David S Kirk, Abigail Sellen, and Xiang Cao. Home video communication: mediating'closeness'. In *Proceedings of the 2010 ACM conference on Computer Supported Cooperative Work*, pages 135–144, 2010.

[57] Robert W Kubey. Television use in everyday life: Coping with unstructured time. *Journal of Communication*, 36(3):108–123, 1986.

[58] Reed Larson and Mihaly Csikszentmihalyi. The experience sampling method. *New Directions for Methodology of Social & Behavioral Science*, 1983.

[59] Gabriele Lenzini, Mortaza S Bargh, and Bob Hulsebosch. Trust-enhanced security in location-based adaptive authentication. *Electronic Notes in Theoretical Computer Science*, 197(2):105–119, 2008.

[60] Alana Libonati, Kelly Caine, Apu Kapadia, and Michael K Reiter. Defending against device theft with human notarization. In *10th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pages 8–17. IEEE, 2014.

[61] Ponemon Institute LLC. Moving beyond passwords: Consumer attitudes on online authentication, 2013. Retrieved February 5, 2021 from https://www.ponemon.org/local/upload/file/NokNokWP_FINAL_3.pdf.

[62] Steve Lohr and Katie Benner. With wikileaks claims of c.i.a. hacking, how vulnerable is your smartphone?, 2017. Retrieved February 5, 2021 from https://www.nytimes.com/2017/03/07/technology/cia-hacking-documents-wikileaks-iphones-tvs.html?

[63] Afra J Mashhadi and Licia Capra. Quality control for real-time ubiquitous crowdsourcing. In *Proceedings of the 2nd International Workshop on Ubiquitous Crowdsouring*, pages 5–8. ACM, 2011.

[64] John D Mayer and Rachael Cavallaro. Brief mood introspection scale (bmis): Technical and scoring manual. 2019.

[65] John D Mayer and Yvonne N Gaschke. The experience and meta-experience of mood. *Journal of Personality and Social Psychology*, 55(1):102, 1988.

[66] Miller McPherson, Lynn Smith-Lovin, and James M Cook. Birds of a feather: Homophily in social networks. *Annual review of sociology*, 27(1):415–444, 2001.

[67] Xiaoqiao Meng, Petros Zerfos, Vidyut Samanta, Starsky HY Wong, and Songwu Lu. Analysis of the reliability of a nationwide short message service. In *IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications*, pages 1811–1819. IEEE, 2007.

[68] Alexander Meschtscherjakov, Astrid Weiss, and Thomas Scherndl. Utilizing emoticons on mobile devices within esm studies to measure emotions in the field. *Proc. MME in conjunction with MobileHCI*, 9, 2009.

[69] Abbas Moallem. Did you forget your password? In *International Conference of Design, User Experience, and Usability*, pages 29–39. Springer, 2011.

[70] Meredith Ringel Morris, Jaime Teevan, and Katrina Panovich. What do people ask their social networks, and why?: a survey study of status message q&a behavior. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1739–1748. ACM, 2010.

[71] Yaser Mowafi, Dhiah Abou-Tair, Tareq Aqarbeh, Marat Abilov, Viktor Dmitriyev, and Jorge Marx Gomez. A context-aware adaptive security framework for mobile applications. In *Proceedings of the 3rd International Conference on Context-Aware Systems and Applications*, pages 147–153. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2014.

[72] Carman Neustaedter and Saul Greenberg. Intimacy in long-distance relationships over video chat. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 753–762. ACM, 2012.

[73] John Podd, Julie Bunnell, and Ron Henderson. Cost-effective computer security: Cognitive and associative passwords. In *Proceedings Sixth Australian Conference on Computer-Human Interaction*, pages 304–305. IEEE, 1996.

[74] Jason Procyk, Carman Neustaedter, Carolyn Pang, Anthony Tang, and Tejinder K Judge. Exploring video streaming in public settings: shared geocaching over distance using mobile video chat. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2163–2172. ACM, 2014.

[75] Ariel Rabkin. Personal knowledge questions for fallback authentication: Security questions in the era of facebook. In *Proceedings of the 4th Symposium on Usable Privacy and Security*, pages 13–23. ACM, 2008.

[76] Jeffrey M Rzeszotarski and Meredith Ringel Morris. Estimating the social costs of friendsourcing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2735–2744. ACM, 2014.

[77] Stuart Schechter, Serge Egelman, and Robert W Reeder. It's not what you know, but who you know: a social approach to last-resort authentication. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1983–1992. ACM, 2009.

[78] Joseph Serna. Man convicted of hacking gmail and icloud accounts of at least 30 celebrities in l.a., 2016. Retrieved February 5, 2021 from https://www.latimes.com/local/lanow/la-me-ln-phishing-scam-conviction-20160928-snap-story.html.

[79] Chirag Shah, Jung Sun Oh, and Sanghee Oh. Exploring characteristics and effects of user participation in online social q&a sites. *First Monday*, 13(9), 2008.

[80] Pankaj Sharma. Mobile lifting rampant in delhi, 2010. Retrieved February 5, 2021 from http://www.dnaindia.com/india/report-mobile-lifting-rampant-in-delhi-1430169.

[81] Imani N. Sherman, Brianna Posadas, Simone A. Smarr, and Juan E Gilbert. My finger, my face, my choice: A preliminary study exploring the use of biometric authentication on mobile devices and the implications for voter verification. In *Who Are You?! Adventures in Authentication Workshop (WAY)*, 2018.

[82] Jordan Shropshire and Philip Menard. A new approach to mobile device authentication. In *Proceedings of the 10th annual Workshop on Information Security and Privacy*, 2015.

[83] Bijan Soleymani and Muthucumaru Maheswaran. Social authentication protocol for mobile phones. In *2009 International Conference on Computational Science and Engineering*, volume 4, pages 436–441. IEEE, 2009.

[84] Sabine Sonnentag, Carmen Binnewies, and Sandra Ohly. Event-sampling methods in occupational health psychology. 2013.

[85] Supasorn Suwajanakorn, Steven M Seitz, and Ira Kemelmacher-Shlizerman. Synthesizing obama: learning lip sync from audio. *ACM Transactions on Graphics (TOG)*, 36(4):95, 2017.

[86] John W Tukey. Comparing individual means in the analysis of variance. *Biometrics*, pages 99–114, 1949.

[87] Niels Van Berkel, Denzil Ferreira, and Vassilis Kostakos. The experience sampling method on mobile devices. *ACM Computing Surveys (CSUR)*, 50(6):1–40, 2017.

[88] Matthijs L Van Leeuwen and C Neil Macrae. Is beautiful always good? implicit benefits of facial attractiveness. *Social cognition*, 22(6):637–649, 2004.

[89] Paul Watters, Patrick Scolyer-Gray, ASM Kayes, and Mohammad Jabed Morshed Chowdhury. This would work perfectly if it weren't for all the humans: Two factor authentication in late modern societies. *First Monday*, 24(7), 2019.

[90] Wang Wei. ios vulnerability allows to disable 'find my iphone' without password, 2014. Retrieved February 5, 2021 from https://thehackernews.com/2014/02/ios-vulnerability-allows-to-disable_8.html.

[91] Sarita Yardi, Nick Feamster, and Amy Bruckman. Photo-based authentication using social networks. In *Proceedings of the First Workshop on Online Social Networks*, pages 55–60, 2008.

[92] Alexandros Zenonos, Aftab Khan, Georgios Kalogridis, Stefanos Vatsikas, Tim Lewis, and Mahesh Sooriyabandara. Healthyoffice: Mood recognition at work using smartphones and wearable sensors. In *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pages 1–6. IEEE, 2016.

[93] Justin Zhan and Xing Fang. Authentication using multi-level social networks. In *International Joint Conference on Knowledge Discovery, Knowledge Engineering, and Knowledge Management*, pages 35–49. Springer, 2009.

[94] Moshe Zviran and William J Haga. User authentication by cognitive passwords: an empirical assessment. In *Proceedings of the 5th Jerusalem Conference on Information Technology, 1990.'Next Decade in Information Technology'*, pages 137–144. IEEE, 1990.

A Pre-survey

A.1 Demographics

1. Gender
   ○ Male ○ Female ○ Other ○ Prefer not to answer
2. Age: _____
3. Race/Ethnicity
   Choose the option that best describes your race/ethnicity.
   ○ White ○ Black or African-American ○ White Hispanic

○ Black Hispanic ○ Asian or Pacific Islander ○ Native American/American Indian ○ Other ○ Don't Know ○ Prefer not to answer

4. Household Income
   From all sources, before taxes
   ○ Less than $10,000 ○ $10,000 to under $20,000 ○ $20,000 to under $30,000 ○ $30,000 to under $40,000 ○ $40,000 to under $50,000 ○ $50,000 to under $75,000 ○ $75,000 to under $100,000 ○ $100,000 to under $150,000 ○ $150,000 or more ○ Don't Know ○ Prefer not to answer
5. Educational Level
   ○ Less than High School ○ High School Diploma ○ Some College, No Degree ○ Two-Year Associate Degree ○ Four-Year College Degree or Bachelor's Degree ○ Some Postgraduate or Professional Schooling, No Degree ○ Postgraduate Degree or Professional Degree ○ Don't Know ○ Prefer not to answer
6. In which city do you currently live?
7. In which state do you currently live?
8. If your country is not the US, which country do you currently live?
   Note: Only answer this question if the country you are currently living in is NOT the United States.
9. Do you currently have a lock on your phone that unlocks via a passcode? ○ Yes ○ No
10. Have you ever used video chat on your phone before? ○ Yes ○ No
11. How many hours per week do you spend video chatting?
    Note: Seconds unnecessary
12. Please take out your phone and reference your phone for this question. List up to 10 of your frequently used mobile apps. Starting with 1 being the most frequently used, 10 being the least frequently used.
    App 1: _____
    How concerned are you about your privacy while you are using "App 1"?
    ○ Not at all concerned ○ Slightly concerned ○ Somewhat concerned ○ Moderately concerned ○ Extremely concerned
    Are you concerned about people you do not know obtaining personal information about you from "App 1"?
    ○ Not at all concerned ○ Slightly concerned ○ Somewhat concerned ○ Moderately concerned ○ Extremely concerned
    This set of questions was repeated ten times to ask from App 1 to App 10.

A.2 Invite Others

Please take this opportunity to invite other people within your social network (e.g. family, friends, coworkers, strangers, etc.), who also have access to a smartphone, and may be willing to participate in the study with you. We will contact them using the information you provide about them, mentioning your full name as the person who invited them. Their participation is entirely voluntary, and you providing their information only invites them to join - it does not enroll them. If you were included by another person, please also list their name here and answer the questions about them. *Note: You are required to list at least one other person (the person who invited you DOES count as this one person), and there is a 10 person maximum.*

1. First Name: _____ Last Name: _____
   Email Address: _____
   Do you know "Person 1" outside of the Internet?
   ○ Yes ○ No
2. If you had to categorize your relationship with "Person 1", which category BEST describes your relationship?
   ○ Family member ○ Spouse/Partner ○ Co-worker ○ Classmate ○ Romantic relationship ○ Close friend ○ Friend ○ Acquaintance ○ Stranger

Rate the degree to which you agree or disagree to the statements below (from 3 to 11): ○ 1. Strongly agree ○ 2. Agree ○ 3. Neither agree or disagree ○ 4. Disagree ○ 5. Strongly disagree

3. If "Person 1" gave me a compliment I would question if "Person 1" really meant what was said.
4. If we decided to meet somewhere for lunch, I would be certain "Person 1" would be there.
5. I would go hiking with in unfamiliar territory if "Person 1" assure me he/she knew the area.
6. I wouldn't want to buy a piece of used furniture from "Person 1" because I wouldn't believe his/her estimate of its worth.
7. I would expect "Person 1" to play fair.
8. I could rely on "Person 1" to mail an important letter for me if I couldn't get to the post office.
9. I would be able to confide in "Person 1" and know that he/she would want to listen.
10. I could expect "Person 1" to tell me the truth.
11. If I had to catch an airplane, I could not be sure "Person 1" would get me to the airport on time.
12. Add another person?
    ○ Yes ○ No

If participants chose to add another person, then we asked them the previous 12 questions again.

B Post-survey

Note: Q2 to Q3 and Q6 to Q8 were all measured in a five point Likert scale: ○ 1. Strongly agree ○ 2. Agree ○ 3. Neither agree or disagree ○ 4. Disagree ○ 5. Strongly disagree

1. Type of phone you used during the study: _____
2. I am comfortable interacting through video chat in general.
3. I am comfortable with the idea of seeking identification from another person through video chat.
4. Who did you prefer to identify you most often from your network group?
5. Why did you prefer him/her? *(check all that apply)*
   ○ Length of time we've known each other ○ What they

know about me ○ I knew they would recognize me effectively ○ They are responsive when I ask them to help me ○ We have lots of friends in common ○ We don't have many friends in common ○ I would have wanted additional contact with them ○ I thought they were attractive ○ Other: _____

6. I had fun helping others in my network group.
7. I would have liked seeing the other person on video chat when helping them.
8. I liked the opportunity to help other people in my network group.
9. Any other comments?

C ESM Questionnaire

C.1 Initiate Survey

1. Last 2 digits of your Participant ID: _____
2. App you are accessing: _____
3. Would you be willing to initiate a video chat session with someone in your network in order to access that app?
   ○ Yes ○ No
   [If "Yes", then Question 4 - 5 and 9 - 11; If "No", then Question 6 - 11]
4. Your Group
   [*In the survey, we showed participants the photos of their group members (See Figure. 1 for an example).*]
5. Who would be your first choice?
   Reference to the photos above when making your selection.
   ○ Person 1 ○ Person 2 ○ Person 3 ○ Person 4 ○ Person 5 ○ Person 6
6. Why did you decline to video chat?
   ○ I'm busy ○ I don't want to ○ I'm not in a location that could use video chat ○ I'm having network issues (e.g., no Wi-Fi, over date usage) ○ I'm having technical issues (e.g., phone is broken, camera won't work) ○ I don't trust anyone in my network ○ Other: _____
7. Your Group
   [*In the survey, we showed participants the photos of their group members (See Figure. 1 for an example).*]
8. If you had chosen to video chat, who would have been your first choice?
   ○ Person 1 ○ Person 2 ○ Person 3 ○ Person 4 ○ Person 5 ○ Person 6
9. What is your current mood:
   Rate the degree to which you: 1 - Definitely Do Not Feel, 2 - Do Not Feel, 3 - Slightly Feel, 4 - Definitely Feel, each of the categories below.
   [*In the survey, we showed participants a matrix. The x-axis is the Likert scale, the Y-axis is the list of BMIS items (See Figure. 1 for an example).*]
10. Which of the following best describes your current location?
    ○ At home ○ At work ○ At school ○ Driving a vehicle ○ Riding in a vehicle ○ In some other public location (e.g. a coffee shop, the grocery store) ○ Other: _____
11. At your current location, are there others around?
    ○ No, I'm alone ○ Yes, I know most or all of those around me ○ Yes, but I don't know most or any of those around me

C.2 Help Survey

1. Last 2 digits of your Participant ID: _____
2. Person you are helping: _____
3. Your Group
   [*In the survey, we showed participants the photos of their group members (See Figure. 1 for an example).*]
4. Will you help that individual access his/her mobile app by conducting a video chat session with him or her?
   ○ Yes ○ No
   [If "Yes", then Question 5 and 7 - 9; If "No", then Question 6 - 9]
5. Why are you willing to help?
   ○ Length of time we've known each other ○ What I know about them ○ I know I would recognize them effectively ○ They are responsive when I ask them to help me ○ We have lots of friends in common ○ We don't have many friends in common ○ I would want additional contact with them ○ I think they are attractive ○ Other: _____
6. What is the reason you declined to help him or her?
   ○ I'm busy ○ I don't want to ○ I'm not in a location that could use video chat ○ I'm having network issues (e.g., no Wi-Fi, over date usage) ○ I'm having technical issues (e.g., phone is broken, camera won't work) ○ I don't trust him/her ○ Other: _____
7. What is your current mood:
   Rate the degree to which you: 1 - Definitely Do Not Feel, 2 - Do Not Feel, 3 - Slightly Feel, 4 - Definitely Feel, each of the categories below.
   [*In the survey, we showed participants a matrix. The x-axis is the Likert scale, the Y-axis is the list of BMIS items (See Figure. 1 for an example).*]
8. Which of the following best describes your current location?
   ○ At home ○ At work ○ At school ○ Driving a vehicle ○ Riding in a vehicle ○ In some other public location (e.g. a coffee shop, the grocery store) ○ Other: _____
9. At your current location, are there others around?
   ○ No, I'm alone ○ Yes, I know most or all of those around me ○ Yes, but I don't know most or any of those around me