Expert and Non-Expert Attitudes towards (Secure) Instant Messaging

Alexander De Luca, *Google;* Sauvik Das, *Carnegie Mellon University;*
Martin Ortlieb, Iulia Ion, and Ben Laurie, *Google*

https://www.usenix.org/conference/soups2016/technical-sessions/presentation/deluca

This paper is included in the Proceedings of the
Twelfth Symposium on Usable Privacy and Security (SOUPS 2016).

June 22–24, 2016 • Denver, CO, USA

ISBN 978-1-931971-31-7

Expert and Non-Expert Attitudes towards (Secure) Instant Messaging

Alexander De Luca[1], Sauvik Das[2], Martin Ortlieb[1], Iulia Ion[1], Ben Laurie[1]
[1]Google; [2]Carnegie Mellon University, Pittsburgh, United States
{adeluca,mortlieb,iuliaion,benl}@google.com,sauvik@cmu.edu

ABSTRACT

In this paper, we present results from an online survey with 1,510 participants and an interview study with 31 participants on (secure) mobile instant messaging. Our goal was to uncover how much of a role security and privacy played in people's decisions to use a mobile instant messenger. In the interview study, we recruited a balanced sample of IT-security experts and non-experts, as well as an equal split of users of mobile instant messengers that are advertised as being more secure and/or private (e.g., Threema) than traditional mobile IMs. Our results suggest that peer influence is what primarily drives people to use a particular mobile IM, even for secure/private IMs, and that security and privacy play minor roles.

1. INTRODUCTION

Due to increasing processing power, modern smartphones offer access to manifold services like games, navigation and even office applications. Despite this multi-faceted functionality, communication is still one of the most important reasons why people use smartphones [1, 10] and, as opposed to most other smartphone activities, is in constant use throughout the whole day [1].

Mobile instant messaging (MIM), a highly popular form of communication, is steadily growing with service providers such as WhatsApp[1] broaching more than 800 million active users.[2] With their expansive feature sets, current mobile instant messengers (mobile IMs) have manifold uses, including group chats [22], sharing media files [5], dwelling with friends [13], and even fleeting encounters with strangers [25].

As these applications see more use, the privacy and security problems associated with their use become increasingly important. More and more apps that promise advanced security/privacy over traditional mobile IMs have entered the app market. However, there are, as yet, few insights about how and why users do or do not use these messengers.

To bridge this gap in the literature, we performed two studies – an online survey with 1,510 participants and a set of in-person interviews with 31 participants. For the interviews, we recruited a balanced sample of people from the general public and IT security experts. Furthermore, to better represent arguments both for and against using secure or private mobile messengers, we recruited a balanced sample of people who either used or did not use mobile IMs advertised as secure or private. Our primary goal was to understand the reasons why people use mobile IMs in general, as well as whether and how privacy and security influenced people's decisions to use particular mobile IMs. Furthermore, we also wanted to explore the differences between IT security experts, i.e., people who have the knowledge to make informed privacy and security decisions, and non-experts and whether they behaved differently in their use of mobile IMs (e.g., more or less secure).

The results of our study show that privacy and security play a minor role in people's decisions to use a mobile IM. Security-optimized mobile IMs are not widely adopted and participants who use them have them for a variety of reasons, such as for communicating with a person who is important to them. We also show that while experts are more aware of possible risks, they do not necessarily behave more securely than non-experts.

While some of our work extends existing insights, such as the importance of peer influence on technology adoption, into the context of secure/private IMs, our work offers several novel contributions. For instance, we offer a detailed understanding of why people choose secure IMs and how this process differs between lay users and security experts.

2. RELATED WORK

Privacy and security in mobile instant messaging has been approached from different directions. For this work, we are mainly interested in privacy and security attitudes towards common IMs as well as reasons for migrating to more secure IMs or staying with old, potentially insecure messengers.

In their work, Patil et al. [14] state that IM users (not exclusively on mobile) have three main desires for privacy: privacy from non-contacts, privacy of availability (e.g., their status) and privacy of messaging content. For instance, people are worried that they can be contacted without their explicit consent, something that most current mobile IMs rely

[1] Please note that at the time of the studies reported in this paper, WhatsApp had not yet introduced end-to-end encryption and was encrypted in transit.

[2] Announced by founder Jan Koum on Twitter on April 17, 2015.

Symposium on Usable Privacy and Security (SOUPS) 2016, June 22–24, 2016, Denver, Colorado.

on (e.g., based on the mobile phone number). In follow-up work, the authors further found differences in privacy attitudes towards various categories of contacts [15].

Grinter et al. [9] showed that teenagers' privacy perceptions are centered around data protection. They are worried what happens to their messages after they have been received. This includes how a message is stored, whether it is ephemeral or long-lived and whether it is further shared by the receiver. They often consider possible negative outcomes of such data leaks and thus want their messages safe. This might explain the success of messaging apps promising zero data retention like Snapchat.[3] Technically, these services cannot live up to their promises, creating a potentially problematic false sense of security [17].

Related to this, proving the identity of the communication partner is a difficult task. However, identity is an important factor as users share specific data with specific people but not with others [15]. This has influenced research effort in using behavioral biometrics to ensure that two communication partners are who they claim they are [3].

Interestingly, simple features like the "last seen" indicator in WhatsApp, that are meant to positively support interaction, can be considered problematic by users [2] (despite being bad predictors for actual attentiveness and causing social pressure [16]). For instance, users turn such features off to avoid trouble with their partners.

It was also shown that for convenience reasons, some messengers like WhatsApp and Viber employ practices that might have negative consequences on privacy and security, e.g., when they upload whole address books from the smartphone to enable friend finding [21]. Thus, it is not surprising that many users consider mobile instant messaging to be less secure and less privacy-respectful than SMS[4] [6].

Reasons for using secure mobile IMs or reasons for migrating to them have rarely been explored. The most notable work is by Schreiner et al. [20] who created a model based on the Push-Pull-Mooring migration framework on privacy reasons that would make a user migrate from WhatsApp to Threema. Roughly said, this framework considers pulling factors (privacy advantages of Threema), pushing factors (privacy problems of WhatsApp) and mooring factors (reasons for staying where you are, for example, different costs). They showed that financial costs had no significant effect on the decision. Psychological and emotional switching costs had the strongest impact. In addition, peer influence (i.e., where the users' friends are) was a strong facilitator for switching, something that was identified as an important factor of using a messenger in the first place [6].

A factor not covered in their study is that the bad usability of many available solutions [23] can have a negative influence on user retention – a finding that we also identified among our interview participants.

However, participants in Schreiner et al.'s study [20] were all well-informed before they study. For instance, they received detailed privacy and security information about both messengers and how these worked, thus creating an unrealistic situation. While their study provides many useful insights, we were more interested in decision making processes and current practices based on the actual, unbiased knowledge of the users.

3. MESSENGER SECURITY

This paper is not meant to provide technical details on messenger security and privacy (see Unger et al. [24] for a comprehensive list of messenger security features). However, it is important to mention two kinds of encryption in order to better understand this work: encryption in transit and end-to-end encryption (e2e).

Most modern IMs use encryption in transit. That means the messages are sent encrypted from the sender to the server and the server to the recipient. On the server, they remain in clear text or in a way that enables at least the service provider to read the information. In many cases, this fact is used to improve service quality and usability.

End-to-end encrypted IMs encrypt the message on the sender's phone and it remains in this state until it is decrypted on the recipient's phone. No third entity has access to the information, not even the service provider. End-to-end encryption comes with some challenges like how to exchange the required keys between the communication entities. For further important security attributes and a list of mobile IMs and their security properties, please refer to the EFF secure messaging scorecard.[5]

The difference between a secure and insecure IM is fuzzy. For this work, we used a rather conservative definition: IMs are secure and/or private if they are actively advertised as secure/encrypted/privacy-preserving. This advertising has to be visible on either the website or the store page without scrolling or clicking any links. In most cases, these were even part of the title, like for Threema which, at the time of the study, was titled "Threema. Seriously secure messaging." All interview participants who used a "secure IM", by the above definition, mentioned that they had seen these labels.

While the promise of security or privacy is no guarantee of actual security or privacy, we consider these promotional messages as the main source of information with which an average person decides whether a messenger is secure and/or private. This assumption is supported by "the paradox of the active user" [4], which states that users never read manuals. Thus, we did not expect that our participants used any more information than the one immediately visible during download to inform themselves. Our results show that there were in fact other sources of information (like knowledgeable peers) that non-experts used but no one mentioned further information from the official websites/manuals.

4. ONLINE SURVEY

The main goal of the online survey was to inform the design of the interview study, to ensure that the interview questions were meaningful and appropriate. In addition, the survey was used to gain first insights into current practices around reasons for choosing mobile IMs and attitudes towards secure mobile IMs.

[3] https://www.snapchat.com/ (last access: February 8, 2016)

[4] The actual security of SMS depends on the encryption employed by the service provider.

[5] https://www.eff.org/secure-messaging-scorecard (last access: February 10, 2016)

	US	UK	DE
18-24	19.4%	27.1%	19.3%
25-34	24%	32.2%	33.6%
35-44	20%	30.4%	28%
45-54	21.2%	7.3%	11.3%
55-64	14.4%	2.4%	5.4%
65+	1.2%	0.6%	2.4%

Table 1: Online study participants: Age.

	US	UK	DE
Female	49.2%	51.5%	45.7%
Male	50.8%	48.5%	54.1%

Table 2: Online study participants: Gender.

We used Google Consumer Surveys (GCS) to run the survey.[6] We picked GCS as it is a fast and convenient tool to collect survey responses and was shown to have a user base that is close to the demographic profile of internet users of major research facilities like the Pew research center [12]. In addition, participants on GCS have similar privacy attitudes to other major online sample providers [19].

GCS enables us to target the survey to respondents from the internet or from Android phones only. As we were specifically interested in mobile IMs, we limited respondents to the latter. Android participants are compensated with play store credits, the amount of which is unknown to us.

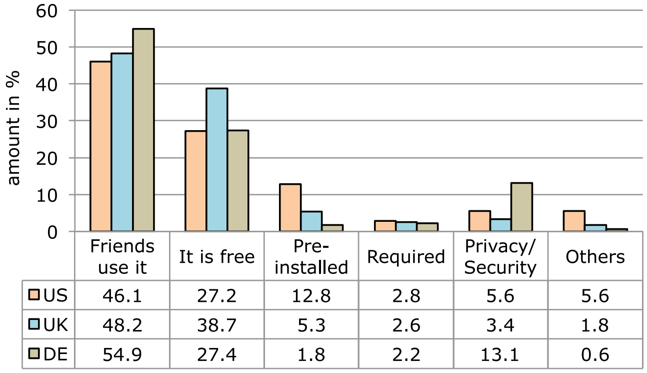
We ran our survey in three countries, Germany, UK and USA, between March 20 and April 2, 2015. As opposed to the interview study, we did not explicitly recruit for experts or distinguish experts and non-expert users as we were interested in general insights and attitudes.

4.1 Survey Design

In general, GCS studies are kept short to avoid click-through answers, i.e., participants who click anything just to receive their incentives. Therefore, we limited the survey to the following four questions. We checked the language in several iterations with different German and English native speakers. We then pre-tested the questions in our lab for language and understanding using the think aloud methodology:

Q1: *"Which of the following mobile instant messengers are you using actively (more than once a week)?"* together with a list of some of the most common secure and standard IMs plus an "other" text field. The order of the answers to this question was randomized with "other" always being shown last.

Q2: *"What is the main reason for your decision to use an instant messenger?"* allowing only one answer (for all options see figure 1). We are aware that this way, prominent answers can mask other options. However, we only meant to collect main reasons and single-response questions work better in GCS, further reducing the chance of dishonest or random answers. In the interviews, we extended these results by exploring all possible reasons instead of focusing on main reasons.



	Friends use it	It is free	Pre-installed	Required	Privacy/ Security	Others
🟧 US	46.1	27.2	12.8	2.8	5.6	5.6
🟦 UK	48.2	38.7	5.3	2.6	3.4	1.8
⬜ DE	54.9	27.4	1.8	2.2	13.1	0.6

Figure 1: GCS survey results: main reasons for using IMs.

Q3: *"Please name the mobile instant messenger you are using most frequently."* to identify which of the previously mentioned mobile IMs they are using as their main messenger (same answer options as Q1 and also randomized order).

Q4: *"Have you heard of encrypted or secure mobile instant messaging?"* on a 5-point scale: "I am currently actively using it", "I have tried, but don't use it often", "I have tried, but no longer use it", "I have heard of it, but I am not using it", "I have not heard of it". We also allowed "other" responses. This question mainly served as a baseline to judge whether they are aware of what they are using or not.

4.2 Participants

We set a quota of 500 participants per survey. As GCS slightly over-recruits to make sure you get your quota as fast as possible, we ended up having 1,510 participants (Germany (503), UK (506), USA (501)). The age and gender ratios for the three countries are listed in tables 1 and 2.

4.3 Results

4.3.1 Main Usage Reasons

The responses to question 1 can be found in figure 1. The main factor for using a mobile IM in all countries was whether friends were using the messenger, which is in line with results from related work [6, 20]. Whether the messenger was free was another important factor in all countries.

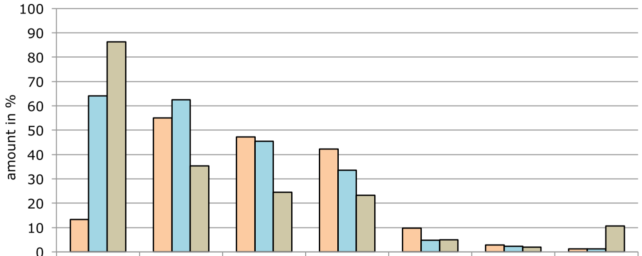
When it comes to privacy and security, only a small fraction of participants stated this being their main factor. An exception is Germany, in which it is the third most important factor with 13.12%.

The "other" reasons include nice integration with the smartphone, being required (for instance by an employer), communication with family members, being associated with other accounts of other apps like Facebook et cetera.

4.3.2 Messenger Use

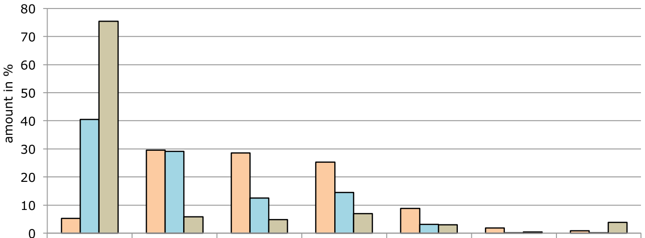
The picture is similar when looking at the numbers of mobile IMs used by the survey participants as shown in figure 2 and their main IMs (figure 3). Please note that since participants were allowed to mention several messengers, the numbers in figure 2 do not add up to 100%. Also, to allow for comparisons with SMS use, these numbers are included in the figures as well.

[6] http://www.google.com/insights/consumersurveys/home (last access: February 8, 2016)



	WhatsApp	Facebook Messenger	SMS App	Hangouts	others	TextSecure	Threema
US	13.4	55.1	47.3	42.3	9.8	2.8	1.2
UK	64.0	52.5	45.5	33.6	4.7	2.4	1.2
DE	86.3	35.4	24.5	23.3	5.0	2.0	10.7

Figure 2: IMs used by participants of the GCS survey. Multiple selections possible.



	WhatsApp	Facebook Messenger	SMS App	Hangouts	others	TextSecure	Threema
US	5.2	29.5	28.5	25.4	8.8	1.8	0.8
UK	40.5	29.1	12.5	14.4	3.2	0.2	0.2
DE	75.4	5.8	4.8	7.0	3.0	0.4	3.8

Figure 3: Main IMs of the GCS survey participants. Only one selection per participant.

The three main messengers in all countries are WhatsApp, Facebook Messenger and Hangouts with WhatsApp being less frequently used in the US. The only two applications in the list that are advertised as being secure (and that provide end-to-end encryption) are Threema and TextSecure. In all three countries, use of these messengers is limited with Germany leading the lists with 10.7% of participants using Threema (compared to 1.2% in the US and 1.2% in the UK). Furthermore, 3.8% of participants in Germany used Threema as their main messenger (compared to 0.8% in the US and 0.2% in the UK).

In the "other" group, we identified 9 users of secure mobile IMs (US: 0, UK: 3, DE: 6) who stated to use them as their main messengers. In all instances this was Telegram. No other messengers that are advertised as being secure or private were named.

4.3.3 Security and Messenger Use

Table 3 depicts the frequencies of the five options of question 4. It shows that with the exception of "I have heard of it but I am not using it", the German participants differ in their self-perception of security adoption (data points marked with *).

The association between country and level of secure or encrypted IM knowledge/use is significant ($\chi^2(8) = 115.6656$, $p < .001$). This means that we can reject the null hypothesis that the two variables are independent. For instance, German participants are 2.4 times more likely than UK participants and 2.2 times more likely than US participants to judge themselves as using secure instant messaging.

	not heard	heard but not using	tried but not using	not often	act. using
US	249	174	12	27	28
UK	256	180	8	23	37
DE	138	181	33	64	84

Table 3: Answers to "Have you heard of encrypted or secure mobile instant messaging?" (Q4).

As mentioned before, we also allowed "other" responses to Q4. Participants used this option in 6 instances. For instance, P284 (DE) stated "I would like to use it but too few of my friends do".

Looking further at the data, we identified a discrepancy between participants stating to actively use encryption and the fact that they had no secure or private messenger in their list of actually used messengers. This was the case for almost all participants in the US (35) and UK (31) stating to use secure instant messaging and around half of the German contingent (38). For instance, P459 (DE) mentioned to be actively using secure instant messaging but only used WhatsApp.

Contrary to this finding, some participants who used secure IMs mentioned they would not use secure/encrypted instant messaging. One of them, P407 (DE), uses Threema and stated to not having heard of secure/encrypted instant messaging (again, the Threema logo stated "seriously secure messaging" at the time of this study) and named "friends use it" as the main reason for using an IM.

Overall, there were 21 participants who used Threema or TextSecure and stated to use secure or encrypted messaging (US: 1, UK: 1, DE: 19) and 17 participants who used Threema or TextSecure but stated to not know or not use secure or encrypted messaging (US: 12, UK: 2, DE: 3).

4.4 Takeaways

There are several things we learned from the online survey that influenced the design of the interview study, as we wanted to learn more about these aspects and find out the rationale behind specific decisions:

Security is not the most dominant reason for choosing mobile IMs. Even in the German sample with a higher proportion of secure IM users, the numbers are comparably low with most participants using insecure messengers in addition to secure ones. Due to the survey setup, participants could only provide one answer. In the interviews, we wanted to explore all reasons in detail, not only the main reasons to find out what role security and privacy really play.

The survey showed **discrepancies between what participants assumed and the reality**. For instance, 104 participants stated to use secure/encrypted mobile IMs while in fact the IMs they listed were not. The main question here is whether this discrepancy is a real effect, i.e., users do not know about possible risks, or whether the security provided by their apps is enough for them and if yes, what are the reasons for it.

Our survey supports the finding that **peer influence** is one of the most important factors in the decision making process on which communication tool to use, but also left some questions unanswered. For instance, we wanted to shed more light on the overall decision making process and the reasons why this factor is so dominant. Accordingly, our interview protocol questions reflect these goals.

Finally, the data we collected is from a general internet population [12]. Inspired by work in other areas, we were interested in whether security experts behave differently from non-expert users, which is sometimes not the case despite their advanced risk knowledge (e.g., [11]).

5. INTERVIEW STUDY

As mentioned before, we used the results of the online survey to inform the design of the interview study. Please note that none of the online study questions was directly reused for the interviews. We rather used the results of the online survey to define where to uncover additional, more granular, insights into why people decide to use certain mobile IMs. We specifically focused on comparing IT security experts with non-experts.

5.1 Study Design

We designed two sets of questions for the semi-structured interviews (one for experts and one for non-experts) based on the open questions of the online surveys. We also added questions, for instance to test for technical knowledge and security/privacy perception of the participants.

While most questions in the two sets were identical, the experts had an additional row of questions that asked them to answer specific questions from the point of view of an "average user". For instance, they were asked both *"What does the term secure instant messenger mean to you?"* as well as *"What do you think the term secure instant messenger means to a user?"*. For this second type of question, the interviewer explicitly told them to answer them from the point of view of a typical end-user.

To avoid influences of specific questions on one another, the order in which these specific questions were asked was counterbalanced (i.e. participants answered them in different orders). We identified four such questions including *"What does the term private instant messenger mean to you?"* and *"What does the term secure instant messenger mean to you?"*.

We had several rounds of language checks and pre-tested the interviews with two participants (one for each set) based on which we created the final questions.

5.2 Procedure

All interviews were conducted in-person by the same interviewer. That is, the interviewer traveled to the countries and locations where the participants lived. At the beginning of each session, each participant read and signed an NDA and consent form. The interviewer then explicitly asked for permission to record audio for the interview. It was explained that the recordings were only used for creating transcripts of the interviews that were needed for the analysis and that they were not shared with anyone outside the research team. We also de-identified recordings to protect participants' privacy. All participants agreed to this procedure.

After that, the interviewer assigned an anonymous ID to each participant and encouraged each interviewee to talk aloud everything that came to their minds. It was also highlighted that they could skip any question they did not feel comfortable answering (this possibility was not used). Participants were not interrupted until they finished answering. After all questions were answered, the participants were debriefed and were given the chance to ask questions themselves. Depending on the replies, the interviews lasted between 30 and 60 minutes.

		ID	Age	M/F	Job
Non-Experts	Normal IM	2	55	m	clerical assistant
		3	38	f	real estate agent
		5	36	m	advisor
		6	23	f	student
		11	39	f	assistant
		12	50	m	clerical assistant
		13	50	f	engineer economics
		14	20	f	student
	Secure IM	1	46	f	secretary
		4	27	m	student
		7	34	f	tanning studio manager
		8	44	m	human resources
		9	51	m	receptionist
		10	44	m	legal advisor
		15	31	f	translator

		ID	Age	M/F	Years in IT Sec.
Experts	Normal IM	1	30	m	7
		2	27	m	4
		3	38	m	7
		4	40	m	3
		5	33	m	8
		6	42	m	1
		7	37	m	16
		8	47	m	30
	Secure IM	9	27	m	4
		10	38	m	8
		11	31	m	12
		12	32	m	6
		13	38	m	15
		14	34	m	20
		15	31	m	10
		16	32	f	6

Table 4: Demographics of the interview study participants.

Participants received a compensation of around EUR 50 for their time, either cash or in the form of a voucher. As the compensation was adapted to the respective country, it slightly varied between participants. Some participants in the IT experts group did not want/take the compensation for different reasons.

5.3 Participants

We recruited 31 interview participants, 15 non-experts and 16 experts. To recruit non-experts from the general public, we worked together with an external recruiting agency providing them with a detailed screener. For instance, we provided a list of mobile IMs that fulfilled our definition of secure or privacy-respectful IMs, in order to get an equal split of secure and non-secure mobile IM users. We also targeted for gender diversity and different professions and education. Non-expert users were recruited in Germany as, based on the online survey, we considered them more privacy and security aware when it comes to mobile instant messaging. The interviews were also conducted in German and then translated to English for coding.

Recruiting IT security experts was more complex and did not allow for equal gender splits and naturally did not allow for diversity in professions and education as well. For this work, our definition of an IT security expert was someone who had a respective education (e.g., computer science) and was currently working in IT security. We ended up recruiting IT security professionals in several EU countries. Again, we made sure that half of the experts used secure IMs while the other half did not.

Table 4 lists the demographics of all interview study participants.

5.4 Results

In order to analyze the open-ended questions, we used an inductive coding approach. At first, two researcher independently coded the transcribed answers. They then met and discussed discrepancies in their codes to create the final codebook. They then used the final codebook to do the final round of coding for each answer.

5.4.1 Messenger Use

On average, non-experts started using mobile IMs 2.8 years ago (SD=1.7; MIN=0.5; Max=6). Experts started 7.1 years ago (SD=3.3; MIN=0.5; Max=13). All non-experts stated that their first mobile IM was WhatsApp. For experts, the picture is more diverse with 11 different mobile IMs including Skype, TextSecure, iMessage and BlackBerry messenger.

Non-experts stated to have 3.3 messengers that they use more than once a week (SD=1.3; MIN=1; Max=6). Experts use 3.1 mobile IMs (SD=0.9; MIN=1; Max=4). Three non-experts reported their main messenger being a secure IM. With two, this number was even lower for experts. As in the GCS study, the only secure/private messengers named were Threema, TextSecure and Telegram. Note again that secure/private refers to whether they are being advertised as such and not to their actual technical security properties.

Out of the five participants who stated to use secure mobile IMs as their main messenger, three also frequently used other messengers, mainly to stay in contact with specific people. The two (one in each group) who do not use other IMs for this purpose still have fallback strategies in case they want to reach other people, including SMS and email.

5.4.2 Main Usage Reasons

We first asked participants which mobile IM they used as their first ever IM and why they picked that specific messenger. After that, we went through the list of all their currently used IMs and asked them to name the reasons why they used each of them. As opposed to the GCS survey, the interview participants were encouraged to name all reasons.

Table 5 lists the top reasons for messenger use in three categories: reasons for starting to use IMs, reasons for using the IMs being advertised as secure or private, and reasons for using non-secure IMs. The first category allowed us to identify drivers that made participants migrate from other forms of communication to mobile IMs.

	Non-Experts		Experts	
	Reason		**Reason**	
First IM	Everyone uses it	9	Everyone uses it	7
	Free	6	Convenient	6
	Convenient	3	Free	5
	Worldwide use	2	Worldwide use	2
Non-Secure IM	Everyone uses it	9	Specific people use it	11
	Worldwide use	6	Specific functionality	8
	Specific people use it	7	Everyone uses it	7
	Free	5	Groups	7
	Share media	5	For work	7
	Specific functionality	4	Passive use	4
	Convenient	3	Convenient	3
	Groups	3	Integrated	3
	Fast	3	Cross-device	3
	Usability	3	Share media	3
Secure IM	Specific people use it	5	Specific people use it	6
	Distrust in other IMs	3	Security/Privacy	4
	Encryption	2	Encryption	3
	Sharing secrets	2	Audited/Open Source	2
	Security/Privacy	2		

Table 5: Top reasons for mobile IM use, mentioned by the interview study participants, divided into three categories: a) First IM - reasons why they startes using mobile IMs. b) Non-secure IM - reasons they named for the IMs that are not advertised as secure/private. c) Secure IM - reasons for using IMs that are advertised as secure/private.

The data shows that security or privacy were not major considerations in the decision making process when participants started to use mobile IMs. In both groups, the main reason was other people (mainly friends) using the respective messengers and the subsequent desire to stay in contact with them. Furthermore, free conversations (as opposed to SMS), convenience and the ability to be in contact with people worldwide (again without added costs) were major reasons in both groups.

When looking at the results for messengers that are not advertised as secure or private, the main important factors, again, have to do with the participants' peers. In both groups, "everyone uses it" and "specific people use it" are within the top 3 reasons. "Specific people use it" refers to statements like *"Person x does not use my main messenger but I want to stay in contact with this person."*.

This factor is even more prominent when it comes to reasons why people in both groups chose to use secure messengers. Participants accept additional costs (financial and setup/use) even though sometimes it is only for a small group or even one important person. The following quote highlights this: *"My security junkies said they send me sensitive data and don't want to be wiretapped. So if I want to communicate with them, I have to use this messenger [Threema]. It's only around 5 people but I would have done it even for one of them who is an old friend"* (P9, non-expert).

The participants' own privacy and security considerations only play a secondary role in the decision to use a messenger advertised as being secure or private.

Non-Experts		Experts	
Difference		**Difference**	
Functionality	7	Encryption	6
Usability	7	Security/Privacy	6
Security/Privacy	4	Identification/Contacts	6
Technology	4	Technology	5
Costs	3	Costs	3
User base	1	Functionality	3
		Trust	3
		Cross-device	3
		Usability	2
		Availability	2
		User base	2

Table 6: Major mobile IM differences reported by the interview study participants.

5.4.3 Messenger Differences

All participants acknowledged differences between the different messengers they use (see table 6). Non-experts experience strong differences in usability (all non-secure IM users) and functionality. They also repeatedly mentioned that specific functionality worked better in some messengers while they then lacked other features.

Experienced differences in usability had a negative influence on whether participants used secure IMs. Five (2 experts) out of the 16 participants who did not use secure IMs explicitly mentioned that those would be more difficult to use. Usability problems included complex setup phases as well as the lack of a searchable message history.

The expert view on messenger differences was focused on technical and security properties (often related). For instance, the top three differences were: 1. whether the messengers used encryption and if yes, which kind (e.g., end-to-end or in transit); 2. general security and privacy properties (e.g. how and how long data is stored); 3. identification/contacts, i.e., how communication partners were identified and whether this process was protected or not.

5.4.4 Message Sending

To better understand where security and privacy factor into people's rationales for choosing mobile IMs, we also asked participants questions to gauge their understanding of how messengers work (and where security and privacy play a role).

One such question was focused on the mental model participants had about the process of sending mobile instant messages: *"What do you think happens between pressing send and the moment the message arrives on the recipient's phone?"*

All non-experts assumed that the messages would go through an intermediary for several reasons like storage until the message can be sent. In 11 instances, non-experts stated that this would be servers and the remaining four were not sure what the intermediary was but they were sure it existed. Five non-experts assumed (or hoped) that the data transmission would be encrypted in some way.

Seven non-experts thought that their data being read, stored or processed (e.g., for profiling or other analysis) was a normal part of the process that one simply has to accept when "sending messages over the internet". Three explicitly mentioned that this was acceptable as they had nothing to hide. While seven experts mentioned this possibility as well, the difference is that they had a clearer picture why this was done (and sometimes necessary).

In general, experts had a very thorough and technology-focused mental model of the process which was well-informed and based on the fact that they were all educated in this matter. Another major difference was that 11 experts mentioned encryption (or sometimes the lack thereof), and which encryption exactly was used as part of the sending process. They also stated that not using end-to-end encryption enabled advanced features like searching their old messages on a server for specific information. However, this requires a certain amount of trust in the respective service provider.

When asked what a non-expert knows about the sending process, 13 experts stated that they would know little to nothing and if they would think about it, they would most likely assume a direct connection between the two smartphones (8 mentions). Six of them even assumed that normal users would consider it "magic". Furthermore, only one expert thought that normal users would think about whether the communication was encrypted or not. Interestingly, the experts highly underestimated the non-experts' knowledge.

5.4.5 Message Importance

Ten participants in each group stated that they considered it important to keep old instant messages. The main reasons were for non-purposeful lookups, e.g., to re-experience old conversations for emotional reasons. Furthermore, 18 participants (12 experts) look up information, most of which is short-term (5) unimportant information like grocery shopping lists. No participants stated to have information in their instant messages that would be important in the long run.

Three participants in each group considered instant messages not important enough to keep them, not even for emotional reasons. Two participants in the non-expert group considered losing old instant messages to be a cleanup of their mobile device. Seven participants (4 experts) stated that only a few selected messages are important while the majority of them would be expendable.

As opposed to this, most participants considered emails highly important, more or much more important than instant messages (10 experts, 11 non-experts) as in many cases, emails are for non-personal (e.g., business) communication (4 experts, 5 non-experts). Additionally, 7 participants (4 experts) explicitly mentioned that the importance of email was usually long-term or permanent. In 5 cases, the importance of emails and instant messages was either similar or the same, mainly since those participants observed a slight shift from conversational use to business use of instant messages.

Related to the fact that participants consider instant messages short-term information, 5 of them (2 experts) stated that such messages were usually time-sensitive, meaning that they should be read or received as fast as possible. Therefore, 10 participants (6 experts) highlighted that message delivery for them was more important than security and if

	Non-Experts		Experts	
	Statement		Statement	
"Secure IM"	Confidentiality	10	Confidentiality	10
	Encryption	5	Encryption	8
	No analysis/profiling	2	Identification	3
	Secure storage	2	Secure storage	3
	Control	1	Control	2
	Authentication	1	Non-existent	2
			Audited	2
"Private IM"	Confidentiality	7	Confidentiality	10
	Encryption	4	Non-existent	5
	Visibility: hidden	3	Encryption	4
	Anonymity	2	Anonymity	4
	No data sharing	2	No leakage	3
	No leakage	2	Marketing	2

Table 7: Main themes reported by the interviewees when asked what they thought the terms "secure instant messenger" and "private instant messenger" meant.

security features would keep their messages from being delivered in a timely fashion, they would consider changing or uninstalling the respective messenger (4 experts, 5 non-experts).

5.4.6 Content Sharing

When asked whether there was specific content that participants would not share over mobile IMs, 26 of them (14 experts) agreed with that statement. In the expert group, all non-secure IM users were among those who agreed. Two of the experts added that this was content that they would not share over any channel.

Examples of sensitive content they would not share include banking information, sexual content or sensitive content that could be used for blackmailing them in case it was leaked. Leakage to people who know the participant was often considered more problematic than leakage to unknown entities as highlighted by the following statement: *"[Leakage to] state agencies is not as bad as they are not interested in what I do and write. People who know me should not be able to get access though."*

In order to avoid such problems and still be able to transmit the information (if necessary), participants named several alternative strategies. These included SMS, telephone, fax, writing letters and even email (PGP or encryption not mentioned) which was mentioned by 7 non-experts and 1 expert.

Out of the remaining 5 participants (2 experts) who answered "no", 3 were secure IM users (2 experts). That means that 2 of the non-experts who would share anything over instant messaging used IMs of which they didn't know whether they were secure or not.

5.4.7 Privacy/Security

One part of each interview focused on the participants' mental models about the terms "secure instant messenger" and "private instant messenger". Table 7 shows the main themes that we identified during coding. For both terms and in both groups, confidentiality was the most important property. This meant that the communication should be protected against any third party but the sender and the recipient. Encryption was another important factor in all groups and for both terms.

A theme that only popped up in the experts group was disbelieve (coded as "non-existent"). For the term "private instant messenger", this was the second most prominent statement. Experts referred to perfect privacy as something technically extremely difficult or even impossible. For instance, control over how recipients handle messages they receive was hard to achieve. Thus, two experts explicitly stated that whenever they read the term, they thought it was simple marketing and they would not trust those promises. This was similar for the term "secure instant messenger", which one expert referred to as "snake oil".

When asked whether these terms influence their impression of an IM (e.g., if the terms are shown as part of the description), 7 experts stated they would check the technical details of the messenger. Furthermore, 6 experts said that messengers need to be audited in order to verify such claims. In the non-expert group, only one participant mentioned audits as a necessary feature. All other participants in the non-expert group would trust the service providers to use the terms correctly or would base their decisions on recommendations by tech-savvy peers they trusted or information they got from the news.

Participants also compared the terms with each other. Eight (2 experts) said the terms referred to the same or highly similar things. Seven participants (2 experts) defined the terms as referring to different parts of the overall process, e.g., *"Security refers to the messages and how they are sent and privacy is the way my data is treated."* (P3, non-expert). The remaining participants either stated that privacy meant more and encapsulated security (2 non-experts, 6 experts) or the other way round (2 non-experts, 8 experts).

6. DISCUSSION

6.1 Peer Influence No. 1 Usage Reason

In both studies, we identified peer influence as the number one reason for choosing and using an IM. In the interview study, this was consistent across both groups, experts and non-experts.

Overall, there were two main types of peer influence. The first has to do with the largest group of people using the same messenger and the subsequent desire to use this messenger as well, irrespective of whether the messenger provides adequate security or privacy. The second type of peer influence was specific (important) people using the service. Often, the groups of people the participants used the respective messenger with was very small, in some cases only a single friend or partner.

This effect works in both directions. If a messenger is not used by a critical mass of contacts (or important people) it will not be used or users will decide to abandon it. For instance, one of the non-expert participants in the interviews mentioned having switched to a secure messenger after a privacy incident with another messenger was reported in the media but then switch back due to peer influence: *"... but it [the privacy incident] had no long-term consequences because [old messenger] is too dominant. At some point, you need to come back."*

Related to literature on social influence in the adoption of technology (e.g., [7, 18]), our participants' did consider their peers' opinions in their decision process. However, the simple desire to stay connected with their friends or specific (important) people was their main consideration which even made them use IMs that they considered inferior to other IMs they had.

6.2 Bad Usability Leads to Abandoning IMs

While usability was only in three instances mentioned as an important factor for choosing an IM, it was mentioned as an important factor in which mobile IMs differed from one another. Specifically secure IMs were repeatedly attributed with having worse usability properties. Consequently, bad usability was a major factor when it came to dropping messengers or not using them at all.

Many of the reported usability problems had to do with security-related properties. For instance, when P15 (non-expert) discussed why he/she had few contacts in his/her main messenger Threema, the explanation was that *"People often don't understand why specific things don't work in Threema"*.

Participants in both groups also repeatedly reported that in order for secure messengers to be better accepted, they should have feature and usability parity with existing major players like WhatsApp.

6.3 Unclear Terms: Privacy vs. Security

The results of the interviews showed that the definitions of the two terms "security" and "privacy" are very fuzzy. This is highlighted by the fact that almost no two definitions given by our participants were identical. Neither the experts nor the non-experts gave identical descriptions.

Furthermore, some participants defined privacy as being a subset of security while others defined security as a subset of privacy. Others, in turn, thought the terms were synonyms or at least highly similar.

Being such highly overloaded terms had two main implications in our study: 1) They have no or only limited effect on experts. They do not trust the terms and require additional (technical) details and information. 2) For non-experts, the fuzziness of the terms had no negative influence as they lack understanding of the technical details anyway. The terms gave them a positive and reassuring feeling.

As a consequence, using both terms in addition to optional details (most likely ignored by non-experts) could be a possible conclusion from these insights.

6.4 (In)Secure Behaviour

Despite experts showing a much higher level of understanding of technical details and possible threats, (voluntarily conducted) insecure behaviour exhibited by the participants in our study was roughly identical across both groups.

For instance, experts are aware of the fact that keeping an (unencrypted) history can be a security/privacy problem but they are willing to accept this for improved service quality like easier backup/recovery and search functionality. In general, participants were mostly happy with the level of security and privacy their messengers provided, even if they did not know the real security properties.

Several interview participants mentioned a trade-off between connectivity and security. Delayed or impossible message delivery due to problems with encryption was unacceptable for them. In such cases, they would prefer unencrypted message transfer in order to keep message delivery timely. They would even go as far as deleting and changing IMs if this remained a problem. In many cases, participants even reported to use "backup messengers" in order to stay connected with certain people, even if they did not trust the security properties of these messengers.

We assume that this behaviour strongly relates to the fact that instant messages are considered short-term information that is only useful for a limited period of time (e.g. shopping list sent by spouse). They are mainly thought of as being of conversational nature and most participants mentioned not sending sensitive information (or information they considered sensitive) through IMs, even with those that are advertised as secure or private.

It has to be noted here that we did not check whether the reported sensitivity of the data participants sent over IMs and the real sensitivity of this data matched. As shown by Egelman et al. [8], self-reported data sensitivity of smartphone data often highly underestimates real risks. Thus, we assume this could be similar in the case of instant messaging.

Our data nevertheless suggests that participants (voluntarily) behave insecurely. This is in line with related work. For instance, Kang et al. [11] found that technical people know more about security risks on the internet but do not spend more effort on protecting their systems.

6.5 Security vs. Reality

When further looking at results related to message importance and security of a user's data, we found that security properties as imagined by the study participants and reality, that is how secure a software really is, often conflicted. This effect was almost exclusively found in the non-experts group.

For instance, 7 non-experts thought that email was a much more secure medium, simply based on the fact that emails contain more important information. For instance, booking information, invoices, bank statements and other (possibly sensitive) information is sent to them through this channel. That is, their rating of email security was based on information independent of actual security.

However, the truth is that most IMs are as technically secure as email, or even more secure. Most mobile IMs (almost all that participants mentioned to use in our study) are in fact at least encrypted in transit, while for email, it depends on both, the provider of the sender and the provider of the recipient. Often, users have no way of knowing whether their emails will be encrypted in transit or not.

This unclarity can lead to users choosing a less secure channel due to confusing cues provided to them in their everyday lives. One way to solve this issue would be to advertise this information better. For instance, even if a messenger was not designed to provide advanced security like end-to-end encryption but provides encryption in transit, this should be highlighted both on the user interface level and in the information available through the service's media channels like its websites.

A current example of more clearly highlighting the security status of a message is the introduction of end-to-end encryption in WhatsApp, which was accompanied by a UI change to display this new property to users[7].

6.6 Sources of Security Information

The security (and to a smaller extent the privacy) properties of mobile IMs were very difficult to judge for the non-experts and multiple participants in the GCS survey. For instance, five interview participants hoped but were unsure that their data was transmitted in an encrypted form.

Non-expert interview participants often referred to security and privacy related terms such as encryption, without actually knowing what they exactly meant. For instance, one user (P4, non-expert) explained encryption in the following way: *"It's when, for instance, my password is changed to those stars [asterisks] so no one can read it."*

Overall, we identified two main forms of sources of information for non-experts: 1) peers like "security junkies" who not only recommend software to them but also help them with other computer related problems like which updates to do and which not; 2) incidents reported in the news.

In the security experts group, the main source of information (other than trusting what they know and checked themselves) were security audits, mainly performed by famous people or organizations they trusted.

7. LIMITATIONS

Using an online survey like GCS does not allow to directly control whether participants correctly fill out the questionnaire or if they just click through it without reading the questions. To avoid such problems, we employed several methods to mitigate the presence of careless answers.

As mentioned in the survey design section, we kept the questionnaire short and the single questions easy to answer (e.g., avoiding multiple choice where possible). GCS also comes with precise timing information about how long it took a participant to answer the whole questionnaire and a specific question. We used this information to eliminate all answers that came to fast to actually read the question. Overall, 4 responses were removed.

Limiting the recipients of the GCS surveys to Android allowed for better control of the fact whether participants were indeed smartphone users or not. On the downside, this meant that we excluded users of other platforms from this sample. For instance, iMessage users are thus not represented in the results.

It also has to be mentioned that both studies were conducted in western democratic countries and thus, the results have to be interpreted with this limitation in mind. For instance, participants living with oppressive regimes or people from specific concerned populations (e.g., journalists working with people who need protection) are likely to respond completely different to our questions.

However, in this study, we were interested in reasoning of the wider general public and thus, decided to recruit for this population rather than the extreme ends of the spectrum. Nonetheless, this is important and we argue that such populations should be investigated in future work.

8. CONCLUSION

Our results provide insights into the decision making process of whether, how and why people choose and use certain mobile IMs. Most importantly, despite security and privacy playing a role in the decision making process for some people, they were only seldom the primary factor, while peer influence, i.e., who and how many people use the IM, was identified as the most important factor. We also found that while, not surprisingly, experts had advanced knowledge about possible privacy and security risks related to using mobile IMs, their behaviour did not notably differ from how non-experts used mobile IMs.

The main factor pulling people away from using secure IMs in our study was usability. That is, if a secure IM does not provide the features desired by the users or if it is more difficult to use than a common IM, it drives people away from it. Both, the general usability and the feature set provided by an IM need to be comparable to major players in order to avoid this effect.

Some study participants, specifically the ones who reported to sometimes use IMs for work, noted a trend that in their opinion, IM use slightly shifted to becoming a replacement for email and other communication channels. Based on the fact that some participants (mainly non-experts) thought of email as a secure communication channel just because important information was sent through it, this leads to the question of whether attitudes towards mobile IM will change once it is more integrated into our everyday work lives.

Future work should focus on groups who already made this transition and find out whether privacy and security requirements are different for those groups. Another highly important group for future research is at-risk users. That is, populations who for different reasons require enhanced security and privacy in their communication (like journalists who work in risky parts of the world). Their attitudes towards communicating with mobile IMs are likely to be quite different from the ones of the general population.

9. REFERENCES

[1] M. Böhmer, B. Hecht, J. Schöning, A. Krüger, and G. Bauer. Falling asleep with angry birds, facebook and kindle: A large scale study on mobile application usage. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, MobileHCI '11, pages 47–56, New York, NY, USA, 2011. ACM.

[2] A. Buchenscheit, B. Könings, A. Neubert, F. Schaub, M. Schneider, and F. Kargl. Privacy implications of presence sharing in mobile messaging applications. In *Proceedings of the 13th International Conference on Mobile and Ubiquitous Multimedia*, MUM '14, pages 20–29, New York, NY, USA, 2014. ACM.

[3] U. Burgbacher and K. Hinrichs. An implicit author verification system for text messages based on gesture typing biometrics. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 2951–2954, New York, NY, USA, 2014. ACM.

[7] Again, this feature was not implemented by the time of the studies.

[4] J. M. Carroll and M. B. Rosson. *Paradox of the active user.* The MIT Press, 1987.

[5] Y.-Y. Chen, F. Bentley, C. Holz, and C. Xu. Sharing (and discussing) the moment: The conversations that occur around shared mobile media. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '15, pages 264–273, New York, NY, USA, 2015. ACM.

[6] K. Church and R. de Oliveira. What's up with whatsapp?: Comparing mobile instant messaging behaviors with traditional sms. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services*, MobileHCI '13, pages 352–361, New York, NY, USA, 2013. ACM.

[7] R. B. Cialdini. *Influence: Science and practice*, volume 4. Pearson Education Boston, 2009.

[8] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner. Are you ready to lock? In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 750–761, New York, NY, USA, 2014. ACM.

[9] R. E. Grinter and L. Palen. Instant messaging in teen life. In *Proceedings of the 2002 ACM Conference on Computer Supported Cooperative Work*, CSCW '02, pages 21–30, New York, NY, USA, 2002. ACM.

[10] A. Hang, E. von Zezschwitz, A. De Luca, and H. Hussmann. Too much information!: User attitudes towards smartphone sharing. In *Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design*, NordiCHI '12, pages 284–287, New York, NY, USA, 2012. ACM.

[11] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 39–52, Ottawa, July 2015. USENIX Association.

[12] S. Keeter and L. Christian. A comparison of results from surveys by the pew research center and google consumer surveys, 2012.

[13] K. P. O'Hara, M. Massimi, R. Harper, S. Rubens, and J. Morris. Everyday dwelling with whatsapp. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work &#38; Social Computing*, CSCW '14, pages 1131–1143, New York, NY, USA, 2014. ACM.

[14] S. Patil and A. Kobsa. Instant messaging and privacy. In *Proceedings of HCI*, pages 85–88, 2004.

[15] S. Patil and A. Kobsa. Uncovering privacy attitudes and practices in instant messaging. In *Proceedings of the 2005 International ACM SIGGROUP Conference on Supporting Group Work*, GROUP '05, pages 109–112, New York, NY, USA, 2005. ACM.

[16] M. Pielot, R. de Oliveira, H. Kwak, and N. Oliver. Didn't you see my message?: Predicting attentiveness to mobile instant messages. In *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems*, CHI '14, pages 3319–3328, New York, NY, USA, 2014. ACM.

[17] N. A. Poltash. Snapchat and sexting: A snapshot of baring your bare essentials. *Rich. JL & Tech.*, 19:1, 2012.

[18] E. M. Rogers. *Diffusion of innovations.* Simon and Schuster, 2010.

[19] S. Schnorf, A. Sedley, M. Ortlieb, and A. Woodruff. A comparison of six sample providers regarding online privacy benchmarks. In *SOUPS Workshop on Privacy Personas and Segmentation*, 2014.

[20] M. Schreiner and T. Hess. Examining the role of privacy in virtual migration: The case of whatsapp and threema. In *Proceedings of the 21st Americas Conference on Information Systems*, AMCIS '15, 2015.

[21] S. Schrittwieser, P. Frühwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, and E. R. Weippl. Guess who's texting you? evaluating the security of smartphone messaging applications. In *NDSS*, 2012.

[22] M. E. Smith and J. C. Tang. "they're blowing up my phone": Group messaging practices among adolescents. 2015.

[23] R. Stedman, K. Yoshida, and I. Goldberg. A user study of off-the-record messaging. In *Proceedings of the 4th Symposium on Usable Privacy and Security*, SOUPS '08, pages 95–104, New York, NY, USA, 2008. ACM.

[24] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith. Sok: Secure messaging. In *2015 IEEE Symposium on Security and Privacy*, pages 232–249, May 2015.

[25] Y. Wang, Y. Li, and J. Tang. Dwelling and fleeting encounters: Exploring why people use wechat - a mobile instant messenger. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '15, pages 1543–1548, New York, NY, USA, 2015. ACM.