Exploring User Mental Models of End-to-End Encrypted Communication Tools

Ruba Abu-Salma
University College London

Elissa M. Redmiles
University of Maryland

Blase Ur, Miranda Wei
University of Chicago

Abstract

End-to-end (E2E) encrypted communication tools can help users keep their communications secure from government or corporate surveillance. In this work, we conduct a quantitative survey (n=125) to assess general mental models and understandings of a hypothetical E2E encrypted communication tool. We find that the vast majority of respondents had adopted E2E encrypted tools in the real world, but lacked confidence and accuracy in their mental models of E2E encryption. Two key misconceptions include (1) three-quarters of respondents believing that their E2E encrypted communications could be accessed by unauthorized entities, and (2) one-half of respondents feeling that SMS and landline phone calls were *more secure than, or as secure as,* E2E encrypted communications. These findings raise concerns that respondents may not feel threatened by proposals of "backdoors" since they already feel that different entities can access their communications. More broadly, our findings suggest that the primary user-related challenge for E2E encrypted tools may no longer be adoption, but helping users who already have these tools avoid sending sensitive information over less secure channels.

1 Introduction

Secure communication tools empower people to resist surveillance. Encrypted email was one of the first forms of secure communication; it was followed by Off-the-Record (OTR) messaging [7], which then spawned a variety of secure communication tools (e.g., Signal). Such tools offer various security properties such as confidentiality (secrecy of communication), integrity (accuracy and completeness of communication), and user authentication. Secure communication tools are critical for activists, journalists, and others who seek to avoid corporate or government surveillance.

Prior work has shown that incorrect mental models are a key obstacle to the adoption of secure communication tools and other privacy-enhancing technologies [1, 26]. Prior qualitative work has explored users' familiarity with secure communication tools and gaps in their mental models [1]. In our work, we seek to quantitatively validate and expand on these findings. We do so by studying both users and *non-users* via a quantitative survey through which we assess high-level mental models of E2E encryption and its security properties. We focus specifically on one type of secure communication, E2E encrypted communication, abstracted away from detailed predispositions of any specific tool created by any particular brand.

To this end, we surveyed 125 respondents about a hypothetical E2E encrypted communication tool. The description of our hypothetical tool was based on a systematic review of the descriptions of 20 real E2E encrypted communication tools (e.g., WhatsApp, Telegram); we chose this method in order to minimize bias from brand-based perceptions of specific tools. Using this hypothetical tool as a foundation, we explore people's understanding of E2E encryption and the security properties of E2E encrypted communication tools.

The majority of respondents currently use at least one E2E encrypted tool, most frequently WhatsApp. Only 12%, however, felt they could confidently explain E2E encryption. Most surprisingly, only one-quarter of our respondents believed that no one could compromise the security of communications in our hypothetical tool. This is concerning, because a belief that E2E encrypted tools are already insecure could mislead users about the danger of proposed measures that would build in insecurity (e.g., backdoors).

Further, one-half of respondents mistakenly thought that SMS messages and landline phone calls would be *more secure than, or as secure as,* E2E encrypted communications. Such misunderstandings may lead users to unknowingly select insecure communication tools in situations where they most require privacy. In some cases

(e.g., activists communicating under threat of imprisonment or death), such mistakes can be life-threatening.

Overall, our results suggest that E2E encrypted tools are widely used but not accurately understood. Thus, the key struggle for E2E encrypted communication tools may no longer be spurring adoption, but emphasizing appropriate use, by helping users send sensitive information using only secure tools.

2 Related Work

Poor usability has traditionally hampered the adoption and use of secure communication tools. In their seminal paper, Whitten and Tygar found that only one-third of respondents were able to use PGP correctly [35]. They concluded that making secure email usable requires the refinement of user interface design principles. Additional studies have evaluated the usability of other secure mail systems as well as various user interface principles, finding that transparency into system operation – e.g., showing ciphertext after encryption – was particularly effective [19, 27, 29].

Bai et al. investigated mental models of non-expert users when making security and privacy trade-offs between two encryption models: a traditional key-exchange model (analogous to PGP) and a registration model (analogous to iMessage) [5]. They found that respondents understood both models fairly well, but preferred the more usable, but less secure, model even for very sensitive communications.

Other studies [4, 18, 28, 30, 32] have considered PGP further, as well as explored usability and user understanding of contact verification in OTR [3], secure communications in two-way radios [9], opportunistic email encryption [17], and public-key fingerprints [12,34]. The majority of these were lab-based studies, where participants were asked to complete a specific set of tasks.

Additional work has employed qualitative methods to understand why people use, or do not use, secure communication tools. Gaw et al. conducted a qualitative study to explore users' decisions about whether and when to encrypt emails [20]. They interviewed nine members of an activist organization under the presumption that the organization's employees would have a strong incentive to encrypt emails. Instead, they found that participants' perceptions of those who used encrypted email (i.e., only "paranoid people" or "people who are up to no good") influenced participants' decisions to use encryption.

Renaud et al. interviewed non-expert students and staff members, as well as computer science students [26]. They found that the key barriers to the adoption of E2E encrypted email were usability issues, incomplete threat models, and a lack of understanding of the email architecture. They concluded that security researchers should focus on building "*comprehensive mental models of email security*," but did not study these mental models. Further, investigations by De Luca et al. found that peer influence was the primary driver of instant messenger adoption, regardless of whether such messengers (e.g., Threema) were advertised as secure or private [11].

Most relevant to our work, Abu-Salma et al. interviewed users of different communication tools about their experiences with those tools and their perceptions of the tools' security properties [1]. They found that barriers to adoption include small and fragmented user bases, lack of interoperability, low QoS (Quality of Service), and incorrect mental models of how secure communication works. We build on Abu-Salma et al.'s qualitative work to conduct a quantitative survey of *both* users' and non-users' mental models of E2E encrypted communication tools.

3 Methodology

We conducted an online survey of 125 people in the UK in April 2018. Our institution's Research Ethics Team approved this study. In this section, we describe the survey methodology, details of our data analysis, and limitations of our work.

3.1 Survey Methodology

The survey questionnaire was developed through an iterative process.

3.1.1 Questionnaire Structure

We asked respondents to answer questions about a hypothetical E2E encrypted tool. We chose to use a hypothetical tool to avoid bias from respondents' preconceived notions of specific tools or tool providers. We introduced respondents to this tool using the following description: "Imagine you are considering using a new tool named Soteria to communicate with your family members, friends, work colleagues, and others. When you install Soteria, the following message is displayed: '*Soteria communications (messages, phone calls, and video calls) are end-to-end encrypted*.' "

We constructed the Soteria message (i.e., the italicized text) by conducting a cognitive walkthrough[1] of the

[1]Cognitive walkthroughs are a usability inspection method actively used in human-computer interaction research to identify and evaluate design components [23]. In our case, we sought to identify how information about message security and privacy was conveyed to the user. For example, WhatsApp advertises itself as E2E encrypted by displaying a message when the user begins a chat, which explains that messages sent using WhatsApp "are secured using end-to-end encryption."

user interfaces of 20 different communication tools included on the Electronic Frontier Foundation (EFF) Secure Messaging Scorecard [14]. We then worded the Soteria display message to closely match wording used by the majority of tools (e.g., WhatsApp, Telegram) to advertise, or provide feedback to users about, the security of their communications. We asked respondents to answer a list of questions about Soteria based on one of the scenarios below (randomly assigned to each respondent) to determine whether respondents' answers would vary based on the described context of use:

- Chatting (not necessarily gossiping) and making plans with family members, friends, or colleagues.
- Sharing account credentials (e.g., usernames, passwords, PINs) with family members, friends, or colleagues. Examples of accounts include personal email account, personal banking account, or personal payment account (e.g., PayPal, Venmo).
- Discussing salary with work supervisor.
- Discussing politics.
- Buying/selling illegal substances (e.g., drugs).
- Whistleblowing – a whistleblower is an employee who reports their employer's misconduct (e.g., an illegal or unethical activity).

However, we saw no effect on responses, which may have been due to our sample size.

Our survey aims to assess the following constructs:

General mental models. First, we aimed to investigate respondents' conceptual understanding of E2E encryption. To do so, we asked whether respondents had heard of "end-to-end encryption," and if so, whether they felt confident explaining what the term meant. We then asked them to explain what it meant for communications to be "end-to-end encrypted" and what the ends refer to in "end-to-end encryption".

To assess mental models of tools that are E2E encrypted, we asked respondents whether different types of communication (e.g., text messages, phone calls, video calls) sent using Soteria have the same level of security or not. We also asked whether different types of non-Soteria communication (e.g., landline phone calls, mobile phone calls, SMS, and email) are as secure as Soteria text messages. Further, we investigated whether respondents' familiarity with E2E encrypted tools affected the robustness of their mental models. Hence, we asked respondents to list the communication tools they regularly use, as well as those that they consider to have the same security guarantees as our hypothetical tool, Soteria.

Security properties of E2E encryption. Second, we aimed to explore respondent understanding of the security properties offered by E2E encryption regarding confidentiality, integrity, and authentication. We asked respondents about the entities, if any, who could read their Soteria messages, listen to their Soteria phone calls, modify the contents of their Soteria communications, and/or impersonate them (i.e., communicate with others using their Soteria account). We provided respondents with examples of different entities, such as people who work at Soteria, people with a technical background, people who are up to no good, governments, Internet service providers (ISPs), and corporations other than the company that develops Soteria. We also asked respondents how they would verify the identity of a messaging partner in Soteria.

Gender	Age	Race	Education	Employment
Male	18–24	Black	B.Sc.	Student
Male	18–24	White	B.Sc.	Student
Male	25–34	Hispanic	M.Sc.	Employed
Male	25–34	White	Ph.D.	Student
Male	35–44	Black	B.Sc.	Employed
Male	35–44	White	Some college	Employed
Male	45–54	Asian	M.Sc.	Employed
Male	55–64	Black	Some college	Unemployed
Female	18–24	Asian	B.Sc.	Student
Female	18–24	Black	M.Sc.	Employed
Female	18–24	White	M.Sc.	Student
Female	25–34	Asian	B.Sc.	Employed
Female	35–44	White	B.Sc.	Employed
Female	45–54	Black	Some college	Unemployed
Female	65–74	Hispanic	Some college	Retired

Table 1: Cognitive interview participant demographics.

Demographics. Finally, we included a number of demographic questions about gender, age, race, educational level, and employment status. We aimed to assess whether age or education would affect respondents' answers to the survey. We also asked respondents to rate the overall difficulty of the survey.

3.1.2 Cognitive Interviews

After developing an initial questionnaire, we conducted cognitive interviews – a method used to pre-test questionnaires to glean insights into how survey respondents might interpret and answer questions [24] – with 15 demographically-diverse participants (see Table 1). The interviewer asked participants to share their thoughts as they answered each survey question. After answering each survey question, participants were asked the following questions: "Was this question difficult to answer?;" "Was there an answer choice missing?;" "How did answering this question make you feel?" We used the findings to iteratively revise and rewrite our survey questions to minimize bias and maximize validity.

3.1.3 Expert Reviews

After the tenth cognitive interview was complete, we asked five human-computer interaction researchers with survey expertise to review our survey questionnaire and

evaluate question wording, ordering, and bias. We also asked our institution's Research Ethics consultant to review the survey. Expert reviewing is a method that complements cognitive interviews in identifying questions that require clarification and uncovering problems with question ordering or potential biases [24]. Following these reviews, we updated some questions and then conducted the remaining five cognitive interviews to ensure no more problems emerged.

3.1.4 Survey Recruitment

We recruited survey respondents within the UK using Prolific Academic. We required that respondents be fluent in English and be at least 18 years old. We asked respondents to read an information sheet that explained the high-level purpose of the study and outlined our data-protection practices. The information sheet did not include the terms "security," "privacy," or "safety" to minimize response bias. Respondents had the option to withdraw at any point during the study without providing an explanation. A total of 125 respondents successfully completed the survey in April 2018. We paid each respondent £2.5 for their participation.

3.2 Data Analysis

Qualitative responses to all open-answer questions were independently coded by two researchers using Thematic Analysis [8], a common method used to analyze qualitative data sets. Coding was not mutually exclusive, as one response could express multiple themes. After coding all responses and creating the final codebook, we tested for the inter-coder agreement (or inter-rater reliability). The average Cohen's Kappa coefficient (κ) for all themes in our data was 0.87. A κ value above 0.75 is considered excellent agreement [10,16]. We report results of closed-answer questions descriptively, except for demographic comparisons (in which we use binomial logistic regression models to evaluate demographic effects, if any).

3.3 Limitations

We used Prolific Academic to recruit respondents. Hence, our sample is not necessarily representative of the demographics of the UK with regards to gender, age, race, educational level, and employment status. We chose to recruit from Prolific Academic as our cognitive interview results showed that questions about E2E encrypted communications were difficult for older and less-educated respondents to answer (who would be better sampled using other platforms). This intuition was confirmed by the results of a survey question assessing the difficulty of our survey, which revealed that despite the majority of respondents feeling satisfied (78%) or neutral (22%) about the survey and its level of clarity, 47% of our respondents were not confident that their responses were correct because they felt unfamiliar with the survey topic. Thus, our results are likely to provide an upper bound (best-case scenario) for user mental models.

Furthermore, traditional survey biases may have occurred. Some questions could have introduced a social-desirability bias, in which respondents feel social pressure to give the "desirable" response. Whenever possible, we carefully worded these questions. For example, we phrased a question asking whether respondents send emails with encryption to emphasize that there are different reasons people decide whether or not to use a given tool. Additionally, we asked demographic questions at the end to minimize sensitivity and bias [25].

4 Results

We present the results from our 125 respondents.

4.1 Demographics

Table 2 summarizes the demographics of our sample (n=125). 40% of respondents identified as male, 58% female, and 2% non-binary. Our sample skewed young; 28% were between 18 and 24 years old, 27% between 25 and 34, 25% between 35 and 44, 8% between 45 and 54, and 12% 55 and above. About one-half of respondents identified as white, one-quarter black, one-tenth Asian, and 7% mixed race. 34% of respondents had a college/undergraduate degree and 20% had a graduate/postgraduate degree. 19% reported having high-school education, 12% vocational training, and 11% some post-secondary education (no degree). Young respondents used a wide range of communication tools, as opposed to older respondents who frequently used only one or two tools.

Despite advertising our study broadly and with no mention of security or E2E encryption, 90% of our respondents currently use, or used in the past, an E2E encrypted tool. The vast majority (87%) of these respondents use, or used WhatsApp, which is very popular outside of the United States due largely to its minimal use of cellular data relative to other communication tools. Notably, 89% of respondents had used at least one E2E encrypted tool that is frequently advertised as such (e.g., Signal, Telegram[2], WhatsApp, Wickr). Furthermore, 55.5% of respondents had used at least one E2E encrypted tool that is not frequently advertised as encrypted (e.g., FaceTime, iMessage). Table 3 details the tools respondents use, or used.

[2]Telegram does not feature E2E encryption by default but does ad-

Category	Percentage
Female	58%
Male	40%
Non-binary	2%
18–24	28%
25–34	27%
35–44	25%
45–54	8%
55+	12%
Asian	10%
Black	26%
White	55%
Mixed race	7%
Prefer not to answer	2%
Some high-school education	2%
High-school education	19%
Vocational training	12%
Some college (no degree)	11%
Associate's degree	2%
College degree	34%
Graduate degree	20%
Employed	63%
Student	20%
Unemployed	10%
Retired	5%
Other	2%

Table 2: Demographics of survey respondents.

4.2 General Mental Models

Although a majority of respondents had used a tool advertised as E2E encrypted, only 12% felt confident explaining the term "end-to-end encryption." In contrast, 50% had heard of the term but did not feel confident explaining it, and 38% had not heard of it at all.

Despite a lack of confidence reported by the majority of respondents in their knowledge of E2E encryption, when we asked whether they would want to use our hypothetical tool (and why), 86% of respondents mentioned that Soteria would be a beneficial tool to use because it offers E2E encryption. In particular, 22% of respondents explained that E2E encryption was a benefit because no third-parties could access Soteria communications and 20% explained that only the sender and the recipient could access Soteria communications; the remaining 44% provided no further explanation. Furthermore, respondents mentioned that E2E encryption made Soteria secure (28%), private (19%), protected (19%), safe (16%), and reliable (1%). Finally, 10% wrote that Soteria could not be "hacked." A minority of respondents also identified some of the potential drawbacks of E2E encryption: 11% mentioned that the sender and the recipient both needed to use Soteria in order to communicate and 9% were worried that Soteria could be used for evading police or intelligence services in conducting cybercrime, cyber harassment, or terrorism.

When asked directly what it means that Soteria communications are E2E encrypted, 34% of respondents mentioned that no one could access the communications and 33% explicitly mentioned that only the sender and the recipient could access the information exchanged. Only 5% gave the most precise answer that only the communicating devices can access Soteria communications.

We then asked respondents to define the "ends" in "end-to-end encryption". Half of the respondents defined the ends as the sender and the recipient, 15% defined the ends as the communicating devices, and 15% as the two installed instances of Soteria on the sender and recipient's devices. Interestingly, 15% reported that the ends refer to the start and end of an exchanged Soteria message. Three-quarters of the respondents reported they were not confident they provided the correct answer to

vertise E2E encryption.

Tool	Currently	Previously	Heard of
Tools that support E2E encryption			
Adium	1	1	0
ChatSecure	0	0	5
Facebook Messenger	90	22	5
FaceTime	47	17	43
iMessage	32	12	25
Jitsi	0	0	1
Pidgin	0	1	10
Signal	5	0	3
Surespot	0	2	1
Telegram	3	6	20
Threema	0	0	3
Viber	1	17	27
WhatsApp	98	11	17
Wickr	1	0	9
Tools that do not support E2E encryption			
Blackberry Messenger	2	21	58
Blackberry Protect	0	5	5
Confide	0	1	0
eBuddyXMS	0	2	1
Google Hangouts	6	12	46
Instagram DM	29	6	32
Kik Messenger	2	14	35
LinkedIn Mail	15	3	32
Ostel	0	0	1
QQ	0	1	11
Skype	40	47	21
Snapchat	38	14	47
Twitter DM	19	16	40
Yahoo! Messenger	4	23	65
Other	2	0	0

Table 3: Respondents' familiarity with different communication tools, specifically whether they use each tool **currently**, used it **previously** (i.e., "used it before, but stopped using it"), or had **heard of** it (i.e., "have heard of it, but have not used it"). Some tools that support E2E encryption offer this mode by default, while others require users to open a special window (e.g., Facebook Messenger's Secret Conversations).

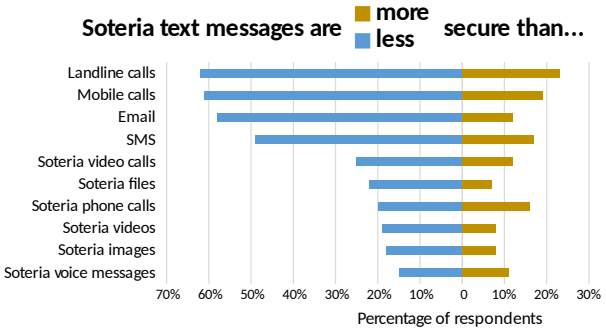

Figure 1: Proportion of respondents who reported that Soteria text communications were either more or less secure than another type of Soteria communication or non-Soteria communication. We omit respondents who considered the communications equally secure.

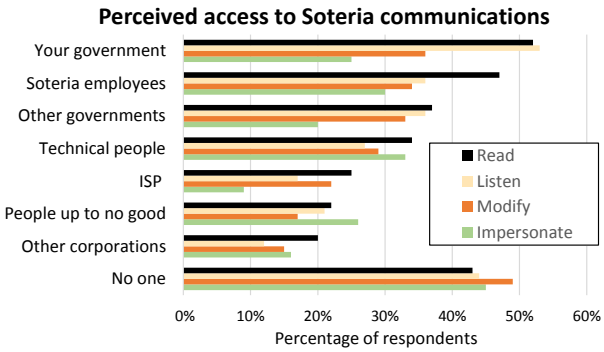

Figure 2: Percentage of respondents who thought each entity could gain a particular type of access to their Soteria communications.

this question. We also note that respondents answered all questions in the context of one-to-one communication; there was no mention of group communication.

We asked respondents to list three examples of tools, if any, that they consider having the same security guarantees as Soteria. 68% mentioned tools that are E2E encrypted: 58% mentioned WhatsApp. 15% mentioned Facebook Messenger and 10% Telegram, which can be used in an E2E encrypted way. However, 31% also mentioned non-E2E encrypted tools: 13% mentioned online banking, 9% mentioned Snapchat, and 9% mentioned commercial email that is not E2E encrypted.

Finally, we also explored whether respondents believed that different types of communication sent using Soteria had equivalent security guarantees. About three-quarters of respondents correctly believed that all types of Soteria communication (text messages, images, file attachments, phone calls, and video calls) would offer the same security guarantees. Additionally, about one-half of respondents incorrectly believed that SMS messages, landline phone calls, mobile phone calls (using cellular data), and email are more secure than, or as secure as, Soteria communications (see Figure 1).

We found that those who had less education were less likely to report being confident about explaining E2E encryption ($p=0.040$, binomial ordinal logistic regression). However, answer confidence did not vary significantly by respondents' gender, race, or age. We did not observe demographic differences in the accuracy of mental models (e.g., who could access E2E encrypted communications).

4.3 Security Properties of E2E Encryption

We asked respondents about entities that could compromise the confidentiality, integrity, and authentication of communications sent or received with Soteria. Figure 2 summarizes their responses. Only one-quarter of respondents believed no one could gain any kind of access (e.g., no one could read, listen, modify, *or* impersonate) their Soteria communications. A larger proportion (nearly half) thought that someone could gain at least one type of access (e.g., someone could read, but not listen, modify, or impersonate).

Roughly one-third of respondents believed that someone with a technical background or a computer science degree could compromise the confidentiality and integrity of Soteria communications, as well as impersonate users. When asked why, 60% of respondents explained that technical people have the necessary knowledge and skills to learn how an encryption protocol works and could thus "reverse-engineer" the protocol to recover the plaintext.

Furthermore, one-third of respondents believed that Soteria's security could be compromised by their country's government (in this case, the UK). Although we did not have a follow-up question to probe, we can speculate that respondents believed this would be possible because governments and intelligence services have the necessary resources and technical expertise to break an encryption protocol. Another reason could be that some respondents were aware of the ability of governments to pressure companies to insert backdoors into secure software and hardware to allow law enforcement agencies to bypass authentication and access data surreptitiously.

Finally, we asked respondents how they would verify the identity of a communication partner in Soteria. 55% mentioned that they would use the person's contact information (name, email address, or phone number), or personal traits (voice) as a method of verification. 22% would ask personal questions. 40% mentioned that tools should handle verification automatically without user engagement. Unfortunately, no respondents mentioned the QR codes or cryptographic fingerprints that many E2E encrypted tools provide for this purpose.

5 Discussion

Our results suggest that a high-level description of a secure communication tool as "end-to-end encrypted" is too vague, and insufficiently informs users of that tool's security properties. Inappropriate mental models of security derived, at least partially, from such descriptions could lead people to send important and sensitive information over less secure channels that users incorrectly perceive as more secure than an E2E encrypted tool. Abu-Salma et al. previously found that people use methods they perceive as most secure to communicate sensitive information [1], yet half of our respondents incorrectly perceived communication channels like SMS and landline phone calls to be more secure than, or at least as secure as, E2E encrypted communications. These results suggest that even if respondents have installed E2E encrypted tools, they may not realize they should be using them at the most security-critical moments.

Therefore, it is critical to communicate the security properties of E2E encrypted communication tools. While warning messages have been thoroughly explored in the literature [2,15], little work has investigated how to design descriptions of pro-security properties. In one of the few examples of work in this space, Ruoti et al. argue that making the ciphertext visible to users after encryption takes place increases user trust in the system [27]. In a similar vein, developers of E2E encrypted tools may seek to provide explicit examples or diagrams illustrating security properties by, for example, showing how an SMS message could be intercepted, compared to an E2E encrypted communication that could not. Furthermore, our findings concur with prior work [1] showing that the size of a user base is crucial for encouraging adoption of a communication tool. Hence, new descriptions might consider communicating, briefly, the size of a tool's user base in the tool description to encourage adoption.

Further, educational interventions included within a particular tool, independently targeted toward the most at-risk users (e.g., activists, dissidents) could provide more in-depth understanding of E2E encryption and its guarantees. We advocate for the development of such interventions through co-design studies with potential users as partners. Such educational tools may also be useful for policy makers, for whom it may be useful to understand E2E encryption prior to regulating it.

6 Summary and Implications

Our respondents used a wide range of real communication tools that provide E2E encryption and are often advertised as such. However, the vast majority of respondents did not feel confident explaining what E2E encryption is and what security properties it offers. Our results suggest that about half to two-thirds of respondents have partially correct general mental models of E2E encryption, specifically that it prevents third-party access and/or limits access to just the sender and recipient.

Nevertheless, only one-quarter of respondents reported believing that no one other than the sender and recipient could access Soteria communications. The belief that E2E encrypted communications can be accessed by many unauthorized entities may reduce users' resistance to the proposal of intentional backdoors. That is, if users believe that E2E encrypted communications are already accessible by governments or the creators of E2E encrypted tools, they may be less likely to resist or vote against proposals to allow backdoor access by these same entities.

Feelings of self-efficacy – which may arise from confidence in the privacy or security one has gained from tool adoption – have been shown to improve continued behavior adoption and the ability to protect oneself in other situations [6, 21]. We hypothesize that a sense that third parties can access communications that are supposed to be private may erode such self-efficacy. Thus, while we should be careful to avoid engaging in "privacy theater" [33] – increasing users' expectations of privacy beyond reality – if users do not feel private or secure when using E2E encrypted tools, or do not feel *as* private or secure as when using other tools, this may reduce their sense of online well-being and sustained engagement in privacy behaviors [31].

Finally, our community has developed an understanding of user mental models around a variety of privacy-enhancing tools, including E2E encryption [1, 13, 26], Tor [22], and private browsing [36]. While we have explored each tool independently, we have yet to consider the interplay between users' models of these different tools. Doing so may be a fruitful direction for future work. Additionally, user mental models of privacy-enhancing technologies have typically been explored in the Global North, especially in English-speaking countries. However, the mental models of people living in highly-censored countries, including some in the Global South, have not been studied. It is critical to study the Global South to enable the development of a more complete and cohesive set of interventions for ensuring privacy and protection against censorship.

References

[1] ABU-SALMA, R., SASSE, M. A., BONNEAU, J., DANILOVA, A., NAIAKSHINA, A., AND SMITH, M. Obstacles to the Adoption of Secure Communication Tools. In *Proc. IEEE Symposium on Security and Privacy* (2017).

[2] AKHAWE, D., AND FELT, A. P. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *Proc. USENIX Security Symposium* (2013).

[3] ALEXANDER, C., AND GOLDBERG, I. Improved User Authentication in Off-the-Record Messaging. In *Proc. WPES* (2007).

[4] ATWATER, E., BOCOVICH, C., HENGARTNER, U., LANK, E., AND GOLDBERG, I. Leading Johnny to Water: Designing for Usability and Trust. In *Proc. SOUPS* (2015).

[5] BAI, W., KIM, D., NAMARA, M., QIAN, Y., KELLEY, P. G., AND MAZUREK, M. L. An Inconvenient Trust: User Attitudes toward Security and Usability Tradeoffs for Key-Directory Encryption Systems. In *Proc. SOUPS* (2016).

[6] BODFORD, J. E. *Blurring Safety Between Online and Offline Worlds: Archival, Correlational, and Experimental Evidence of Generalized Threat in the Digital Age*. PhD thesis, Arizona State University, 2017.

[7] BORISOV, N., GOLDBERG, I., AND BREWER, E. Off-the-Record Communication, or, Why Not To Use PGP. In *Proc. WPES* (2004).

[8] BRAUN, V., AND CLARKE, V. Using Thematic Analysis in Psychology. In *Qualitative Research in Psychology* (2006), vol. 3, pp. 77–101.

[9] CLARK, S., GOODSPEED, T., METZGER, P., WASSERMAN, Z., XU, K., AND BLAZE, M. Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System. In *Proc. USENIX Security Symposium* (2011).

[10] COHEN, J. A Coefficient of Agreement for Nominal Scales. *Educational and Psychosocial Measurement 20*, 1 (1960), 37–46.

[11] DE LUCA, A., DAS, S., ORTLIEB, M., ION, I., AND LAURIE, B. Expert and Non-Expert Attitudes towards (Secure) Instant Messaging. In *Proc. SOUPS* (2016).

[12] DECHAND, S., SCHÜRMANN, D., IBR, T., BUSSE, K., ACAR, Y., FAHL, S., AND SMITH, M. An Empirical Study of Textual Key-Fingerprint Representations. In *Proc. USENIX Security Symposium* (2016).

[13] DEMJAHA, A., SPRING, J., BECKER, I., PARKIN, S., AND SASSE, M. A. Metaphors Considered Harmful? An Exploratory Study of the Effectiveness of Functional Metaphors for End-to-End Encryption. In *Proc. USEC* (2018).

[14] ELECTRONIC FRONTIER FOUNDATION (EFF). Secure Messaging Scorecard. `https://www.eff.org/secure-messaging-scorecard`. Accessed on: 09.01.2018.

[15] FELT, A. P., AINSLIE, A., REEDER, R. W., CONSOLVO, S., THYAGARAJA, S., BETTES, A., HARRIS, H., AND GRIMES, J. Improving SSL Warnings: Comprehension and Adherence. In *Proc. CHI* (2015).

[16] FLEISS, J. L., LEVIN, B., AND PAIK, M. C. *Statistical Methods for Rates and Proportions*. John Wiley & Sons, 2013.

[17] GARFINKEL, S. L. Enabling Email Confidentiality through the Use of Opportunistic Encryption. In *Proc. Annual National Conference on Digital Government Research* (2003).

[18] GARFINKEL, S. L., MARGRAVE, D., SCHILLER, J. I., NORDLANDER, E., AND MILLER, R. C. How to Make Secure Email Easier to Use. In *Proc. CHI* (2005).

[19] GARFINKEL, S. L., AND MILLER, R. C. Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express. In *Proc. SOUPS* (2005).

[20] GAW, S., FELTEN, E. W., AND FERNANDEZ-KELLY, P. Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted E-mail. In *Proc. CHI* (2006).

[21] LEE, D., LAROSE, R., AND RIFON, N. Keeping Our Network Safe: A Model of Online Protection Behaviour. *Behaviour & Information Technology* (2008).

[22] LEE, L., FIFIELD, D., MALKIN, N., IYER, G., EGELMAN, S., AND WAGNER, D. A Usability Evaluation of Tor Launcher. *PoPETs 2017*, 3 (2017).

[23] POLSON, P. G., LEWIS, C., RIEMAN, J., AND WHARTON, C. Cognitive Walkthroughs: A Method for Theory-Based Evaluation of User Interfaces. In *International Journal of Man-Machine Studies* (1992), vol. 36, pp. 741–773.

[24] PRESSER, S., COUPER, M. P., LESSLER, J. T., MARTIN, E., MARTIN, J., ROTHGEB, J., AND SINGER, E. Methods for Testing and Evaluating Survey Questions. In *Public Opinion Quarterly* (2004), vol. 68, pp. 109–130.

[25] REDMILES, E. M., ACAR, Y., FAHL, S., AND MAZUREK, M. L. A Summary of Survey Methodology Best Practices for Security and Privacy Researchers. Tech. rep., 2017.

[26] RENAUD, K., VOLKAMER, M., AND RENKEMA-PADMOS, A. Why Doesn't Jane Protect Her Privacy? In *Proc. PETS* (2014).

[27] RUOTI, S., ANDERSEN, J., HEIDBRINK, S., O'NEILL, M., VAZIRIPOUR, E., WU, J., ZAPPALA, D., AND SEAMONS, K. "We're on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users. In *Proc. CHI* (2016).

[28] RUOTI, S., ANDERSEN, J., ZAPPALA, D., AND SEAMONS, K. Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client. *arXiv preprint arXiv:1510.08555* (2015).

[29] RUOTI, S., KIM, N., BURGON, B., VAN DER HORST, T., AND SEAMONS, K. Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes. In *Proc. SOUPS* (2013).

[30] RYAN, J. F., AND REID, B. L. Usable Encryption Enabled by AJAX. In *Proc. IEEE International Conference on Networking and Services* (2006).

[31] SCHNEIER, B. In Praise of Security Theater. *Schneier on Security 25* (2007).

[32] SHENG, S., BRODERICK, L., KORANDA, C. A., AND HYLAND, J. J. Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software. In *Proc. SOUPS* (2006).

[33] SOGHOIAN, C. An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government. *Minn. JL Sci. & Tech. 12* (2011), 191.

[34] TAN, J., BAUER, L., BONNEAU, J., CRANOR, L., THOMAS, J., AND UR, B. Can Unicorns Help Users Compare Crypto Key Fingerprints? In *Proc. CHI* (2017).

[35] WHITTEN, A., AND TYGAR, J. D. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proc. USENIX Security Symposium* (1999).

[36] WU, Y., GUPTA, P., WEI, M., ACAR, Y., FAHL, S., AND UR, B. Your Secrets Are Safe: How Browsers' Explanations Impact Misconceptions About Private Browsing Mode. In *Proc. WWW* (2018).