2017 IEEE Symposium on Security and Privacy

Obstacles to the Adoption of Secure Communication Tools

Ruba Abu-Salma
University College London, UK

M. Angela Sasse
University College London, UK

Joseph Bonneau
Stanford University & EFF, USA

Anastasia Danilova
University of Bonn, Germany

Alena Naiakshina
University of Bonn, Germany

Matthew Smith
University of Bonn, Germany

***Abstract*—The computer security community has advocated widespread adoption of secure communication tools to counter mass surveillance. Several popular personal communication tools (e.g., WhatsApp, iMessage) have adopted end-to-end encryption, and many new tools (e.g., Signal, Telegram) have been launched with security as a key selling point. However it remains unclear if users understand what protection these tools offer, and if they value that protection. In this study, we interviewed 60 participants about their experience with different communication tools and their perceptions of the tools' security properties. We found that the adoption of secure communication tools is hindered by fragmented user bases and incompatible tools. Furthermore, the vast majority of participants did not understand the essential concept of end-to-end encryption, limiting their motivation to adopt secure tools. We identified a number of incorrect mental models that underpinned participants' beliefs.**

I. Introduction

The majority of web traffic between clients and servers is now encrypted via TLS, however, the majority of communications between users are not yet end-to-end (E2E) encrypted [1], [2]. Whenever plaintext is processed or stored by remote servers, users are vulnerable to mass surveillance [3] or hackers. Their personal data is also subject to commercial analysis by service providers for advertising and enhanced personalization [4]. As a result, security experts have long advocated increased use of E2E encryption.

Usability has long been considered a key challenge for secure communications, especially E2E encryption. However, the design of most communication tools (and likewise most of the cryptographic literature on secure communication protocols) has typically not involved those who are ultimately meant to use these tools, certainly not in the early to middle stages of design [5], [6]. Several user studies (e.g., [7]–[9]) have examined why users fail to use existing secure communication tools (e.g., PGP) correctly, often concluding that significant security failures arise due to user interface (UI) design flaws.

Furthermore, there has been an effort to produce educational materials (e.g., [10]–[12]) to explain existing security tools and extensions, such as OpenPGP [13], Tor [14], Tails [15], off-the-record (OTR) messaging [16], and SecureDrop [17]. These guidelines provide step-by-step instructions to install and use these tools securely. However, documentation only helps the users who read it and are already motivated enough to adopt a new tool.

Recent mobile phone-based secure communication tools have often been designed to hide security from the user completely (albeit at some security cost [1]). WhatsApp famously deployed E2E encryption to approximately a billion users through a code update to its application for messages, voice calls and video communications [18], with only negligible changes to the user experience. Some other communication tools (e.g., Signal, Threema) have launched with security as an explicit selling point, but they also hide nearly all cryptographic details.

There are key differences in the security model of different E2E-encrypted tools, in addition to a large gap in security compared to competitors (e.g., Google Hangouts, Skype) which do not offer E2E encryption. Yet, we have little understanding of how users perceive the threats to their communications, or whether they believe secure communication tools protect against these threats. The Electronic Frontier Foundation (EFF) Secure Messaging Scorecard [2] is one attempt to provide security information to non-expert users, a kind of a "consumer guide" to secure communication tools. However, there has been no evaluation to see if the target users understand the scorecard, or will select more secure tools as a result of it.

We argue that to design and build communication tools that effectively protect users, we need to understand how users perceive secure communications, and what influences their decision to adopt (or not adopt) secure tools. To make a preliminary step in this direction, we used a qualitative approach [19]–[21]. We first conducted 10 unstructured face-to-face interviews (35 minutes on average), followed by 50 semi-structured face-to-face interviews (90 minutes on average).

The key qualitative insights from our interviews are:

- **Usability is not the primary obstacle to adoption.** Participants reported usability issues with different tools, but did not stop using the tools mainly because of them.
- **Fragmented users bases and lack of interoperability are significant obstacles.** The common trend of creating new secure communication tools and assessing the usability of these tools is a significant obstacle to adoption due to creating fragmented user bases. Also, to reach their communication partners, participants needed to use tools that are interoperable (i.e., work across different devices).

DOI 10.1109/SP.2017.65

- **Low Quality of Service (QoS) is an obstacle to adoption.** Participants assessed the reliability and security of a communication tool by the QoS of messages and voice calls they experienced. Low QoS does not only hinder adoption, but also creates general doubts about how reliable and secure the tool is.
- **Sensitivity of information does not drive adoption.** Perceived sensitivity of information should drive the adoption of secure communication tools, but this was not the case with our participants. Instead, they used voice calls (regardless of the tool) and other obfuscation techniques to exchange sensitive information.
- **Secure communications were perceived as futile.** Most participants did not believe secure tools could offer protection against powerful or knowledgeable adversaries. Most participants had incorrect mental models of how encryption works, let alone more advanced concepts (e.g., digital signatures, verification fingerprints). If the perception that secure communications are futile persists, this will continue to hinder adoption.
- **Participants' security rankings of tools were inaccurate.** We asked our participants to rank the tools they have used in terms of how secure they are. Many participants ranked the services (e.g., voice calls, messages) offered by the tools, rather than ranking the tools first. They perceived calls more secure than messages. Furthermore, they based their rankings on how large the tool's user base is, QoS, social factors and other criteria, rather than assessing the security properties a secure tool offers.
- **Participants did not understand the EFF Secure Messaging Scorecard.** The scorecard contains seven security properties. Four of these were misunderstood: participants did not appreciate the difference between point-to-point and E2E encryption, and did not comprehend forward secrecy or verification fingerprints. The other three properties reflecting open design (documentation, open-source code and security audits) were considered to be *negative* security properties, with participants believing security requires obscurity.

Our findings suggest not only a gap between users' understanding of secure tools and the technical reality, but also a gap between users' communication priorities and what the security research community imagines them to be.

II. Related Work

A. Secure Communications

For a detailed review of the literature on secure communication tools, we refer the reader to Unger et al. [1]. Secure communication tools became widely available with the release of PGP in 1991 [22], which was followed by the creation of a large ecosystem of PGP tools [13], [23], [24]. PGP was designed for asynchronous, high-latency email communications. OTR [16], originally released in 2004, was designed for low-latency messaging environments like chat clients, introducing additional security features (e.g., forward secrecy, deniability). OTR has influenced many secure communication tools designed since [25]–[30], including the Signal protocol [31], which has recently gained popularity.

The use of self-destructing messages was popularized by Snapchat, which was released in 2011. While popular with users who perceived this feature as an effective solution to some of their security and privacy needs, Snapchat offers little security against motivated attackers, and secure data deletion in messaging has proved elusive [32]–[34]. Other tools that appear to provide certain security properties fail to provide these properties in the face of government requests [3].

Usability has long been considered a challenge for secure communications, especially E2E encryption. The main UI challenge for E2E-encrypted communication tools is believed to be providing assurance that a user is truly communicating with the intended party (called *trust establishment* by Unger et al. [1]). This is often reduced to verifying ownership of cryptographic keys in some fashion. In traditional PKI, this assurance is delivered in the form of a signed certificate from a trusted authority [35]. However, there are many issues with PKI associated with certificate management, including key storage, distribution and revocation, as outlined in [36]. Popular E2E-encrypted tools (e.g., iMessage, WhatsApp, Signal) relieve users of key management; they simply query a trusted server that vouches for the authentic public keys of other users. Recent proposals attempt to limit the trust in these servers using transparency logs [37], [38], but this approach has not been deployed in practice.

The smartphone era has seen an explosion of new communication tools (typically called *messengers* or *messaging applications*). Many of these applications claim to be "secure", but they often do not provide specific security guarantees or documentation, and fail to draw upon the existing cryptographic literature [1], [39]. This led the EFF to develop the Secure Messaging Scorecard in 2014 – 2015 to attempt to provide objective information about what security properties communication tools actually offer, providing a Consumer Reports-style guide and encouraging adoption of tools that offer better security [2]. Yet, there was no evaluation of the scorecard with the target community (i.e., users who are not security specialists) to see if the scorecard was perceived as helpful, or did influence users' decision to adopt secure tools.

B. User Studies of Secure Communication Tools

Lack of usability has been shown to hamper both adoption of secure communication tools and the actual level of security in real-world use. In their seminal paper [7], Whitten and Tygar designed a case study to assess whether PGP 5.0 could be effectively used by non-specialist users to secure their email. They identified some problems in the UI design relevant to security risks (e.g., irreversible errors, lack of consistency and feedback). They also found that only one-third of participants were capable of using the PGP software to correctly sign and encrypt an email. They concluded that making security usable requires the development of domain-specific UI design principles and techniques.

Using a similar study to [7], Garfinkel and Miller studied CoPilot, an email prototype based on Key Continuity Management (KCM) [8]. KCM attempts to make secure communication tools more usable by making key generation, key management, and message signing automatic. Garfinkel and Miller concluded that KCM is a workable model for improving email security, and that the UI of CoPilot enables users to send protected emails easily because, for example, it visually distinguishes encrypted emails from unencrypted ones.

Ruoti et al. conducted a user study of two mail systems: Private Webmail (Pwm) and Message Protector (MP) [40]. They found both systems to be usable, but participants trusted MP more than Pwm because they "*could see the ciphertext after encryption takes place*", equating this with protection. More recently, Ruoti et al. conducted a lab-based study with pairs of novice users cooperating to send encrypted emails with a range of email tools [41]. Again, they found that hiding the details of how a secure system provides security reduces trust in the system, however, participants preferred integrated over standalone encryption solutions. They concluded that integrated encryption solutions are a key step to increase usability, but complete transparency (i.e., hiding security details) is counterproductive. The need for visible feedback matches the findings of Whitten and Tygar [7] as well as the "*visibility of system status*" usability engineering principle encouraged by Nielsen and Molich in 1990 [42].

Bai et al. investigated whether non-expert users can evaluate the security trade-offs between two encryption models: a traditional key-exchange model (analogous to PGP) and a registration model (analogous to iMessage) [43]. They asked participants to complete a set of encryption tasks using both models. They also described each model's security properties and asked participants for their opinion. They found that participants understood both models "*fairly well*". Even though participants recognized the benefits of the exchange model for "*very sensitive communications*", they preferred (and also trusted) the more usable, but less secure, registration model for "*everyday communications*". Bai et al. concluded that designers should explain the security properties an encryption tool offers, and that the EFF Secure Messaging Scorecard provides an "*excellent start in this direction*".

Other studies (e.g., [44]–[48]) have considered PGP further as well as contact verification in OTR [26], secure communications in two-way radios [9], opportunistic email encryption [49], and public-key fingerprints [50], [51]. Furthermore, several studies have explored users' perceptions of email signatures [52], browser security indicators (e.g., [53], [54]), and specific features of specific security tools (e.g., self-destructing messages in Snapchat [55]).

Gaw et al. explored the social context behind users' decisions about whether and when to encrypt emails [56]. They interviewed members of an activist organization under the presumption that the organization's employees would have a strong incentive to encrypt emails. They found that the perception of encryption behaviour by others (e.g., use of encryption for protecting secrets is seen as "justified", for general communications as "paranoid") influenced participants' decision to adopt encrypted email.

In [57], Renaud et al. proposed seven possible explanations for the non-adoption of E2E encryption in email, based on the literature and researchers' own observations. To validate these explanations, they interviewed students and staff members (not security experts), and surveyed computer science students. They found that, in addition to usability issues, incomplete threat models, misaligned incentives, and lack of understanding of the email architecture are key drivers of the non-adoption of E2E-encrypted email. They concluded that security researchers should focus on building "*comprehensive mental models of email security*".

Das et al. recently studied the role of social influence on users' decisions to adopt secure tools [58] and to use specific security features of a specific application (Facebook) [59], [60]. De Luca et al. also investigated how and why users use mobile instant messengers that are advertised as being secure (e.g., Threema) [61]. They concluded that peer influence, not security and privacy, primarily drives users to adopt a messenger. The objective of our study is to explore the user experience of secure communications in more depth, identify "other" factors that lead to the adoption and abandonment of communication tools, and understand how users perceive the "security" of communication tools, especially of those advertised as being secure.

It is worth to mention that Dourish et al. studied how users experience and practice security using a qualitative approach (semi-structured interviews analyzed using Grounded Theory [20]) in 2004 [62]. Similarly, we use a qualitative approach to understand how users manage their communications, secure or not, as an "*everyday, practical problem*". We "zoom out" to understand users' security needs and practices, and the background against which they decide to use or stop using a communication tool. We also explore what users look for in a secure communication tool.

We know that the decisions users make may not deliver on their actual security requirements. The gaps in mental models identified by Renaud et al. suggest that users may think they are more secure than they are [57]. Similarly, the folk models of home network security described by Wash led his participants to believe that their practices were secure when they were not [63]. Thus, we study users' knowledge of the threats to their communications, and their mental models of the tools and practices they use to protect against these threats.

III. Methodology

In this section, we discuss our research questions, recruitment process, interview procedure, data analysis, research ethics, and the limitations of our work.

A. Research Questions

In this work, we explore (1) why, when and how users use secure communications (Section III-C1), (2) what threats users want to protect against when communicating (Section III-C2), (3) which communication tools users perceive to be secure (or

insecure) and why (Section III-C3), and (4) how users think secure communications can be achieved, and how they can be breached (Section III-C4).

B. Participants

Our literature review (see Section II) shows that mainstream users' needs and practices of secure communications have not been investigated. Instead of focusing on a specific at-risk population, such as activists, whistleblowers, or journalists, our main focus is understanding the needs and practices of users of communication tools who do not consider themselves to be at risk of targeted surveillance. This is because our focus of enquiry is *widespread* adoption of secure communications.

We recruited our participants via posting flyers around University College London's buildings and emailing university staff members. We also distributed emails to staff members in collaborating public- and private-sector organizations (e.g., banks, hospitals, universities). We asked interested participants to complete an online pre-screening questionnaire, which 380 completed. The full questionnaire can be found in the Appendix. We assessed participants' technical knowledge and cyber-security threat exposure via a set of simple questions. We also provided them with a list of different communication tools (those evaluated by the EFF Secure Messaging Scorecard), asking them to select all the tools they currently use and the ones they stopped using. Additionally, we gave our participants the option to specify other tools they have used, but were not on the list.

We then divided the pool of eligible participants into subgroups, based on a number of variables: age, gender, education level, study area, employment status, technical knowledge, and previous cyber-security threat exposure. We conducted and analyzed 10 unstructured interviews first, followed by 50 semi-structured interviews. Tables 1 and 2 summarize the demographics of our recruited participants for both the unstructured and semi-structured interview sessions, respectively[1].

With 60 participants, our study represents the largest qualitative study on this topic. We interviewed 23 male and 35 female participants. Two participants preferred not to indicate their gender. Participants' ages ranged from 18 to 70. Two participants did not have a formal educational qualification, seven completed high-school education, 30 had a college degree (e.g., BA, BSc), and 21 had a higher degree (e.g., MA, MSc, PhD). 40 were high-school and university students, 17 were employed, and three were retired. Our participants used a wide range of communication tools on different computing platforms (e.g., Android, iOS, Mac OS X, Microsoft Windows). None of the participants used a PGP-based tool, such as Enigmail, GPGTools or Gpg4win. Only P23 and P57 used an OTR-based tool; both have adopted Pidgin for some time and then stopped using it.

We note that P2, P5 and P28 identified themselves as security experts, so they did not necessarily represent mainstream users of communication tools.

[1] Tables 1 and 2 can be accessed from the first author's webpage.

C. Interview Procedure

The value of conducting qualitative research lies in providing a holistic understanding of the phenomenon under enquiry using predominantly subjective qualitative data, which can be supplemented by observational and other quantitative data [64]. A single trained researcher conducted all 60 interview sessions in the UK in English, by first conducting 10 unstructured (open-ended) face-to-face interviews, lasting for 35 minutes on average. The emerging themes shaped the design of the script used for the 50 semi-structured face-to-face interviews, lasting for 90 minutes on average. The interviewer allowed participants to elaborate, share their thoughts, and ask any clarification questions. The interviewer also asked follow-up questions (or probed) where appropriate. This is a common practice in semi-structured interviews, in which the interviewer primarily uses a list of questions, but has discretion to ask follow-ups or skip questions that have already been covered. However, all interviews covered the following four areas in the same order. Below, we describe the script we used for the *semi-structured* interviews.

1) Adoption of communication tools: We asked participants to specify the communication tools they have used by giving them the same list of tools provided during the pre-screening stage. This allowed us to compare their answers with those in the pre-screening questionnaire. Also, we asked them to take out their mobile phones and check all the communication tools they have installed.

For each tool currently used or previously used by our participants, we asked why they decided to adopt it and why they stopped using it (if they had). The given answers helped us understand why specific tools were widely adopted and others were not. The key questions were:

- Why did you decide to adopt [this communication tool]?
- What computer platforms does the tool run on?
- Who do you communicate with?
- What is the context of use?
- Do you describe yourself as a regular user of the tool?
- Have you ever checked and/or changed the default settings of the tool? Please elaborate.
- What kind of information do you regard as "sensitive"?
- Have you ever sent sensitive information via a communication tool? If yes, why and how did you do so?
- Why did you decide to stop using [this communication tool], if applicable?

2) How users defined secure communications: "Securing" a communication tool is meaningless without defining a security policy and a threat model. Many communication tools are advertised as "secure" or "encrypted", but a recent academic survey suggested that many are not as secure as they claim to be [1]. The link between users' perceptions of secure communications and the actual security offered by different communication tools has not been investigated so far.

To address this gap, we asked our participants about the kind of protection (or security properties) a secure communication tool should provide, what they want to protect, with whom

they communicate, who the attackers (or adversaries) might be, and what their capabilities are.

We also elicited participants' mental models of how they think secure communications work. Mental models are cognitive representations of external reality that underpin people's cognition, reasoning, decision-making and behavior [65]. We invited our participants to draw how a communication tool works, and whether there is a distinction between calling someone and sending them a text (or multimedia) message. A message could be an SMS, an email or an instant message. We provided our participants with an iPad and a stylus pen. We also recorded and transcribed participants' verbal commentary while drawing, along with the rest of the interviews.

3) Security ranking of communication tools: We asked our participants to rank the communication tools they have used in terms of the security level each tool offers. We provided them with cards with the names and logos of the tools they have used, and asked them to sort the tools from the most to the least secure. We used this card sorting exercise to compare our participants' rankings with those on the EFF Secure Messaging Scorecard [2] and to elicit the rationale behind their rankings.

We also wanted to assess the effectiveness of the EFF Scorecard in communicating which communication tool is secure and why. After our participants ranked the tools and described their reasoning, we showed them the scorecard (printed on a sheet of paper) and gave them 10 minutes to explore it, compare their rankings, and ask any clarification questions they had.

4) Security properties and mechanisms: In the last part of the study, we wanted to probe our participants' understanding of how a security property can be achieved and how it can be violated. We also asked participants about several specific security mechanisms: encryption, digital signatures and cryptographic fingerprints. We wanted to check their broader understanding to see whether they can interpret the criteria on the EFF Scorecard correctly or not.

Finally, we debriefed our participants and gave them the time to ask any clarification questions about the study.

D. Pilot Study

We conducted a pilot study of five semi-structured interviews to check that the questions could be understood and identify any potential problems in the script (e.g., cost, time, adverse events) in advance, so that the methodology could be fine-tuned before launching into the main study. We used the common practice of convenience sampling [66] by selecting five colleagues for the pilot study. In addition to the five sessions, we asked six researchers to review the study.

E. Data Analysis

To develop depth in our exploratory research, we conducted multiple rounds of interviews, punctuated with periods of analysis and tentative conclusions [19]. In total, we conducted, transcribed (using an external transcription service) and analyzed all 10 unstructured and 50 semi-structured interviews. We observed data saturation [67] between the 40^{th} and 45^{th} interview; i.e., no new themes emerged in interviews 46–50, and, hence, we stopped recruiting. Data saturation provides a high degree of confidence that we observed the range of reasons for adoption (or non-adoption) of secure communications. The audio-recordings of the interview sessions were transcribed, and then independently coded by three researchers using Grounded Theory analysis [20], [21], an inductive/open-ended method to discover explanations, grounded in empirical data, about how things work. After coding all interviews and creating the final code-book, we tested for the inter-coder agreement (or inter-rater reliability). The average Cohen's Kappa coefficient (κ) for all themes in the paper is 0.83 [68]. A κ value above 0.75 is considered an excellent agreement [69].

F. Ethics

The Research Ethics Board at University College London reviewed and approved our research project (project ID no.: 6517/002). Before each interview, we asked our participants to read an information sheet and sign a consent form that explained the purpose of the study, and emphasized that all data collected was treated as strictly confidential and handled in accordance with the provisions of the UK Data Protection Act 1998 (registration no.: Z6364106/2015/08/61). Participants had the option to withdraw at any point during the study without providing any reason. We explained to them that in such a case, none of their data would be used in the analysis, and they would still receive the full reward of £10. No participant withdrew.

G. Limitations

Our study has some limitations. Although our sample size is large for a qualitative study, we did not cover a wide range of cultural backgrounds. One can argue that this limits the generalizability of our results. However, we have documented the study protocol step-by-step, meaning that it can be replicated with participants in different cultural contexts.

Additionally, our study has limitations common to all qualitative studies. Research quality depends on the researcher's individual skills and might be influenced by their personal biases. A single researcher, who was trained to conduct the interviews consistently and ask questions in an open and neutral way in order not to influence participants, conducted all 60 interviews. We note that the length of the interviews meant that fatigue set in during the final 20 minutes, so participants' answers tended to be less detailed. However, the interviewer prompted participants to give full answers to all questions. Furthermore, some participants could have been concerned about the interviewer's perception of them and, therefore, could have changed their answers in line with how they like to be perceived.

IV. Results

In this section, we present the key emerging and recurring themes we observed across our interviews. We report participants' statements by labeling them from P1 to P60. We additionally report how many participants mentioned each

theme to give an indication of the frequency and distribution of themes. However, the main purpose of qualitative research is to explore a phenomenon in depth, and not to generate quantitative results. We identified several misconceptions of secure communications among participants that underpinned their reasoning and decision-making. We report those in their respective sections: IV-A – IV-H.

A. Adoption Criteria of Communication Tools

We found nine main criteria influencing our participants' decision to adopt a communication tool, namely (1) large user bases and interoperability, (2) context of use, (3) services offered by the tool, (4) QoS, (5) cost of use, (6) type of communications (spontaneous or planned), (7) integration with email, (8) registration (telephone numbers vs. usernames), and (9) social influence.

Large user bases and interoperability. The ability to reach their intended communication partners is the primary communication goal of our participants. If most of their regular communication partners do not use the tool, it has little utility. As P5 put it, "*there is no point of using a chat service that not many people use*". 50 out of 60 participants explicitly mentioned that the tools they use most frequently are those that most of their contacts use. Thus, the small and fragmented user bases of current secure communication tools hinder adoption of secure tools. For example, P23 and P57 who used Pidgin (an OTR-based tool) in the past deserted it because of lack of utility, whereas almost all participants use WhatsApp.

Even iMessage, which is available on any device running iOS (or Mac OS X), is not used as frequently as WhatsApp because not all of our participants' contacts own such a device, and iMessage is not interoperable (i.e., does not work with non-iOS devices). The same applies to FaceTime. Because WhatsApp works across different platforms, it is the tool of choice; many participants who have an iOS device use WhatsApp to communicate with contacts who also have an iOS device, instead of using iMessage (or FaceTime). Although they perceive iMessage as more secure (see Section IV-G), they see the overhead of using two communication tools as not worth the better security offered by iMessage.

Context of use. Participants use communication tools in a variety of contexts: socializing, organizing events or creating study groups. They perceive some tools as "more suitable" for some types of communications: they use SMS and email for formal conversations, whereas they prefer IM to communicate informally with family members, friends and colleagues. Voice calls using the mobile phone network (whether the call is local or international) are preferred if the communication is urgent, or, as P2 described his parents and grandparents, the communication partner is "old-school". Participants perceive calling a contact as more convenient and "faster" than sending a message via IM because they do not have to check if the recipient is online. Also, our participants prefer SMS and IM to email if they want the recipient to be notified quickly.

Services offered. Our participants choose specific tools based on the services the tools offer. 55 out of 60 participants explicitly mentioned that they use email, instead of SMS, to send large volumes of data (e.g., media messages, files) although many of these participants (32 out of 55) perceive sending a message via SMS as "more secure" than sending an email (see Section IV-F). Furthermore, 20 participants who perceive Telegram as more secure than WhatsApp (see Section IV-G) explicitly mentioned that Telegram does not support calls, causing them to use the "less secure" option: WhatsApp.

Lack of utility fosters insecure behaviour: Telegram supports two chat modes: (1) default chat mode (messages are encrypted in transit), and (2) *Secret Chat* mode (messages are E2E-encrypted). However, the *Secret Chat* mode does not currently support group conversations. *All* participants who use Telegram do not use *Secret Chat* when communicating with individuals either because the overhead of switching between the two modes is high, or because they just forget to use *Secret Chat*, especially for participants who frequently use the default mode to send group messages. This can be conceived as a usability problem (i.e., mode error: a type of slip where a user performs an action appropriate to one situation in another situation, which is common in software with multiple modes), but is also caused by lack of utility (the secret mode does not support group conversations).

QoS. 47 out of 60 participants assess the reliability of a communication tool based on the QoS of voice calls and messages they experienced. For example, P9 and P12 prefer Google Hangouts because its audio has "high-quality", whereas P31 and P45 stopped using Google Hangouts because they experienced "bad-quality" audio in the past. This not only influences adoption, but also users' perceptions of how secure a tool is (see Section IV-G): 40 out of 60 participants said that a tool that offers high-quality services can also be assumed to be more secure. Thus, the perceived competence developers of tools demonstrate by delivering high QoS makes participants assume that they will also do a good job on security.

Cost of use. The financial cost of using a tool is another main factor influencing participants' adoption decision (47 out of 60). Participants mainly use IM when they are not in the same country as the recipient. P2, P30 and P41 mentioned that IM tools are not at "no cost" because they have to pay for the Internet service most of the time. P2 reported that the cost of the Internet service in developing countries is high.

Battery consumption is another cost our participants mentioned. 36 out of 60 participants said they never log out of most of their accounts, but they do log out of their Skype accounts because they see Skype as a "heavy" application that drains the device battery. This in turn means it takes time and effort to start Skype again and sign into the account. As a result, our participants rarely use Skype for spontaneous communications.

Type of communications: spontaneous vs. planned. Participants clearly distinguish between spontaneous and planned communications. Many participants who use Skype (30 out of 60) use it mainly for international calls and videoconferencing. These communications are usually pre-arranged, rather than spontaneous. P7, for instance, said she does not use Skype for communicating with others on a regular basis because

communication partners will not notice her messages unless they are logged in. However, the majority of our participants always log out of their Skype accounts (see the previous point on battery consumption).

Integration with email. Most participants have used Yahoo! Messenger for some time, but they stopped using it after moving away from Yahoo! mail. For example, P46 and P56 mentioned that they had to specifically log in to their Yahoo! mail account to access the chat service. 15 participants, on the other hand, use Google Hangouts because they frequently use Gmail (on their PC/laptop, not phone).

Registration: telephone numbers vs. usernames. Communication tools that require knowledge of a contact's phone number also have reduced utility. WhatsApp and Facebook Messenger are the most frequently used tools among our participants (45 out of 60) for sending messages. However, WhatsApp is only convenient to use when participants have the phone number of the person they want to communicate with, whereas in Facebook Messenger, they can search for a particular person by name, adding to the tool's utility.

Social influence. A social system is a combination of external influences (e.g., mass media) and internal influences (e.g., social relationships) that affects participants decision to adopt or stop using a particular tool (54 out of 60). A newspaper article or a friend can influence adoption decisions. Das et al. [58]–[60] have studied the role of social influence on users' decisions to adopt secure tools and to use specific security features; we found some evidence in the reasons our participants gave for adoption. For example, P56 said she adopted Telegram because her father recommended it as secure against eavesdropping by service providers. However, we found she does not use the *Secret Chat* mode and, as a result, her communications are not protected. She was motivated to adopt a secure tool, but was foiled by a usability issue (mode error).

B. Sensitive Information: Perceptions and Practices

Perceived sensitivity of information should drive the adoption of secure communication tools, but this is not the case with our participants. When we asked participants if they send sensitive information via communication tools, they started to use the terms "security", "privacy", "safety", and "protection", interchangeably. However, they do not select a secure tool to do so. Instead, they use different practices and obfuscation techniques. In this section, we explain how our participants define sensitive information, which practices they use to send this information, and the information's level of sensitivity.

How participants define sensitive information. Our participants said they want to protect all data they transmit, and all data stored on their personal devices. However, they regard some information as sensitive, such as personally identifiable information (PII), bank account details, authentication credentials (e.g., PINs, passwords), health data, their photos, and political views. Only P37 mentioned that any piece of information is potentially personal and sensitive.

Protection practices. The majority of participants (53 out of 60) believe that the best protection for sensitive information is to speak to the recipient directly, instead of using a communication tool. If they trust a communication partner with the information and need to send the information urgently, they regard voice calling or videoconferencing as most secure, regardless of the tool used. Voice calling and videoconferencing are seen as the "closest thing" to telling the recipient face-to-face because there is "no record" of calls, as opposed to messages (see Section IV-F for the reasons). Only seven out of 60 participants (P2, P5, P37, P42, P45, P47 and P51) mentioned that voice calls have the same security properties as messages giving the reason that the same communication tool and channel are used.

Other practices our participants perceive as secure include sending information by post (P46), sending a voice message in a foreign language (P17 and P48), or cutting the message into "chunks" and sending these via different communication tools (P20 and P43). P56 also reported sending different chunks of information using the different modes of Telegram: when sending a 4-digit PIN, she sends two digits via the *Secret Chat* mode and the other two digits via the default chat mode, believing the two modes of Telegram use "*two different channels*", which cannot be associated with each other.

P8 told us about using an encryption tool to encrypt a document, sending the "encrypted document" via one communication tool and the "encryption key" via another. The encryption tool turned out to be Microsoft Word's password-based document encryption feature, with the password serving as the encryption key. 10 participants have their own "code" to exchange sensitive information via *any* communication tool. They share the code (effectively a substitution cipher) with trusted parties in advance before sending any message. They said that the "design" of these codes or schemes must be kept secret, so that only the parties who know the schemes can decode the scrambled message. P13 also mentioned using the practice of sending her password to a trusted recipient as a text message via any tool and then changing her password later.

Level of sensitivity. 54 out of 60 participants said they share sensitive bank account details with trusted recipients via a phone call, but discuss political views only face-to-face. They believe that (1) neither the government nor service providers are interested in users' PINs and passwords, and (2) a government agency (especially with repressive regimes) can target a particular person and record their calls, as portrayed so memorably in the following movie: "*The Lives of Others*".

None of our participants mentioned meta-data (e.g., identity of sender and recipient) as worth protecting. Even when we hinted at the potential sensitivity of meta-data, they (except for P2 and P5) described them as "less sensitive". Clearly, they are not aware of the highly publicizing and debated "*we kill people based on meta-data*" comment [70]. Our participants' mental models of both the technology they are using and the threats to their communications seem very much influenced by traditional telephony, rather than digital communications.

C. Security Properties

Our participants used the terms "secure communications" and "security" in previous discussions. In this section, we analyze what security properties they expect from secure communication tools. Their discussion of security properties falls into three main categories: (1) secrecy of message content, (2) message integrity, and (3) "no impersonation".

Secrecy of message content. When our participants described this property, they did not use the terms "confidentiality" or "encrypted communications". Instead, they explained that exchanged messages via a secure communication tool should only be accessed by the sender and intended recipient(s). Third parties, including government intelligence agencies and service providers, should not be able to read the messages, or listen to voice calls. P5 mentioned that information exchanged via a communication tool should not be "*re-routed to unintended recipients*".

Message integrity. No participant mentioned unprompted that a message should not be modified in transit (for several reasons discussed later in Section IV-D.II). However, when we explained the threat to them, all agreed that integrity is an important property a secure communication tool must offer. Only three participants (P2, P5 and P28), who identified themselves as security experts, discussed man-in-the-middle attacks and digital signatures, the essential cryptographic mechanisms for assuring integrity.

"No impersonation". All participants believe a user will be impersonated if their username and password are used to log in to their account. They, therefore, want their passwords stored in a secure place (the service provider's server) where they cannot be compromised. Many participants used the term "hacking" in connection with this security property. Six participants (P15, 17, 32, 43, 49, 56) expect to be notified, and to be asked for consent, before the government or service provider accesses their accounts. This is an expectation of conduct by snoopers that in reality is unlikely to be met.

Our participants did not mention or describe plausible deniability (or repudiation), forgeability, forward or backward secrecy, recipient authenticity, or confidentiality of usernames. When we started discussing anonymous communications, all participants mentioned that anonymity is an unimportant security property. From our participants' perspective, anonymous communications mean sender-anonymity [71] and/or third-party anonymity [71] (expressed in their own words). P2, P6, P32, P39, P45 and P50 also mentioned that only people who engage in political discussions need sender anonymity. P2 incorrectly stated that Telegram and Signal (formerly known as TextSecure) offer sender-anonymity and third-party anonymity. He stated (also incorrectly) that Skype, Snapchat and Telegram's *Secret Chat* mode provide deniability because they do not offer "*evidence preservation*"; i.e., a sender can delete a message they have already sent.

P8, P11, P22, P27, P32, P43 and P60 suggested that anonymous communications can be achieved by using a public PC, creating a fake account, sending the data, and then logging out. However, they believe this only works for communication tools that do not require a phone number at registration time (e.g., Facebook Messenger).

Availability is hugely important to our participants, referring to it as "reliable connection". However, they regard it as a utility feature (see Section IV-A), not a security property.

D. Threat Models

Our participants described different types of adversaries that can violate the security of communications. We describe these adversaries and their capabilities in Section IV-D.I. In Section IV-D.II, we explain how participants think the security properties of secure communication tools (discussed in Section IV-C) can be breached.

D.I. Adversaries

All participants, except for P2 and P5, believe that the security of *any* communication tool can be breached by three types of adversaries: (1) intelligence agencies, (2) application service providers, and (3) technically-skilled attackers.

Intelligence agencies. 58 out of 60 participants believe government agencies (e.g., NSA, GCHQ) have the resources and capabilities required to monitor any citizen. They also believe that governments can coerce or compel service providers to hand over all the data related to a particular user. 21 participants believe governments do this to protect their national security; e.g., to prevent terrorism. P51 mentioned a "*universal decryption key*" that allows governments to decrypt and read any encrypted communication.

Application service providers. 54 out of 60 participants think that all messages pass through the service provider who "*knows how the communication tool works*" (P10) and, therefore, is able to access all messages. They also believe that service providers can access any account stored on their servers either because passwords are not encrypted, or encrypted in a way that can be "*reverse-engineered*" (P9). Eight participants mentioned that companies access the content of messages not for malicious, but commercial reasons (e.g., targeted advertisements, removing inappropriate content). P1, P12, P13, P35 and P42 reported that when they download an application to their device, the application asks for their permission to access PII, geo-location data, photo albums, and contact lists. To them, this means that providers have ways of circumventing the security properties of communication tools.

55 participants mentioned that they have to accept a provider's Terms and Conditions (T&Cs), which they do not read because they are "too long" and "intentionally vague", and contain "a lot of jargon" (like Data Privacy Policies and End-user Licence Agreements). 15 participants mentioned that these terms are regularly updated without users being notified. Our participants suspected they have agreed, because of a clause somewhere, that the provider can access their data. Hence, "*having my data anyway*" means trying to protect it is pointless (P47).

Technically-skilled attackers. All participants (except for P2 and P5) believe that the use of a secure communication

tool cannot protect against attackers with technical expertise, described as hackers, computer science students, or competing companies (e.g., Apple vs. Google).

Only P2 and P5 said that a secure communication tool is as secure as the device they install it on, provided that the security protocols are proved to be secure and implemented correctly. Reasons for the device not being secure that P2 and P5 are aware of include software and hardware bugs, malware (e.g., viruses) and backdoors.

D.II. Violating the Security of Communications

Below, we explain how participants believe the security properties of secure communication tools (discussed in Section IV-C) can be violated.

Secrecy of message content. Almost all participants (except for P2, P4, P5, P6, P9 and P28) believe that information exchanged via *any* tool can be accessed and read by (1) physically accessing the user's mobile phone or PC, and reading messages from the chat history, (2) a communication partner colluding with a third party and sending them the chat history, (3) accessing the microphone and speaker to listen to phone calls using some "sophisticated techniques", (4) using CCTV cameras to capture exchanged messages on a users' device screen, or (5) falling for a social engineering attack.

Some participants also believe that confidentiality (i.e., secrecy of message content) can be easily breached by the service provider because when users download an application, it asks for their permission to access the device's contact list, camera, microphone and photo gallery. According to P1, if the user decides not to agree to such a request, they will not be able to exchange photos with others. This finding is in line with the threat model explained earlier in Section IV-D.I. P8 also reported that providers access log files to perform quality monitoring of the service, hence, they can read the information exchanged if they want to. She also mentioned that a law enforcement agency that has a subpoena can "obviously" access users' information.

Only P2, P4, P5, P6, P9 and P28 mentioned eavesdropping, wiretapping or decrypting cipher-texts. No participant explicitly talked about man-in-the-middle attacks (although we cannot rule out that these attacks could have been part of the "sophisticated techniques" mentioned above). P6 believes that confidentiality can be breached by wiretapping the communications between one point and another, though he believes that as long as "*basic encryption, which is signing in to an application*" is used, this attack can be avoided. He thinks the password used to log in to an account is a form of encryption to protect the data in transit against unsophisticated attackers (other members of the public).

P9 also mentioned that if many people use a communication tool (whether secure or not), there will be "*billions of messages being exchanged via the network*". This, he believes, makes it hard to identify a message sent by a particular person. He thinks that as long as a tool has a large user base, attackers cannot associate exchanged messages with specific parties, even if messages are sent in cleartext.

P2, P4 and P5 believe that confidentiality can be breached through social engineering attacks, exploiting vulnerabilities, using weak cryptographic schemes, or inserting backdoors.

Only P2, P4, P5 and P6 mentioned the terms "encryption" or "decryption", albeit with simplistic mental models. We discuss participants' mental models of encrypted communications in detail later in Section IV-E.

Message integrity. As discussed in Section IV-C, this security property was not mentioned by any participant. When we hinted at it, all participants said that messages should be protected from modification, but many did not think that messages can be modified in transit (50 out of 60). P3 believes her messages have never been modified because her phone has never been stolen, and her account "*has never been hacked*". Thus, no one can send modified messages from her account. She believes that integrity is assured as long as authentication takes place. 21 other participants share P3's belief. Many believe that their messages cannot be tampered with, which is in stark contrast to their other belief that confidentiality cannot be achieved.

P4 does not worry about integrity being breached because "*any message modification can be detected even after some point in time*" by the recipient (a belief shared by P11, P25, P49 and P60). P4 believes that if someone sends a message encrypted and then it gets modified in transit by an attacker, the recipient will receive "nonsense", and resending the message will resolve the problem. 30 participants said they have never thought of the possibility that messages can be tampered with because, as P11 put it, "*the chat history does not change when sending a message*".

P6, P12 and P18 believe that integrity does not get breached unless people live under a repressive regime. Hence, governments can modify or censor communications. 40 participants believe that service providers can tamper with messages, however, P12 thinks it is not worth the effort: "*this would require someone to have access to the intermediate server between me and the recipient, so it could probably only be done by someone within the company, who has access to the central server. But, this is unlikely, and I don't know why they would do it either, so I think it's a very small concern*". P13 reported that message integrity can be violated if the application software has a "bug".

None of the participants knows how integrity can be achieved, except for P2 and P5 who correctly explained hashing and digital signatures. We discuss participants' mental models of digital signatures in Section IV-E.

"No impersonation". All participants believe that as long as passwords are hard to guess or steal, authentication is achieved. Passwords can be stolen by hacking, social engineering, or brute forcing.

According to our participants (41 out of 60), hacking means (1) stealing the username and password by mounting a social engineering attack, guessing the password, intercepting the password when logging into the application, or stealing the password from the company's server, (2) logging into the account on behalf of the legitimate user, and then (3) reading

messages from the victim's chat history and accessing PII. Many participants (32 out of 60) believe that hacking generally happens over the "Internet"; the traditional network (3G) is more secure and, as a result, hacking is impossible.

All participants think social engineering attacks are possible, and that they need to be aware of these attacks. They believe security can be increased by not writing passwords down and by changing them regularly, but doing so is onerous.

43 out of 60 participants mentioned that passwords can be brute-forced. Furthermore, 21 out of 60 stated that an attacker can create fake accounts to impersonate others, but "*the company providing the service should be aware of this and ensure this does not happen*" (P4). 25 participants also believe that providers store passwords encrypted on their servers: "*they [service providers] are immune to brute-forcing attacks because encryption is used to protect credentials*" (P9).

E. Mental Models of (Secure) Communications

During the interview, we asked our participants how a communication tool works, and who the actors in a communication system are. We also asked about different security mechanisms, such as encryption, digital signatures and cryptographic fingerprints. We provided participants with an iPad and a stylus pen, so they would draw if they wished to explain a specific concept (e.g., encryption). This helped us identify whether our participants know the mechanisms used to achieve a particular security property, such as associating encryption with confidentiality, and how this relates to their threat models in Section IV-D. We also found a misconception about deleting accounts shared by most participants.

Actors in a communication system. All participants, except for P1 and P11, believe the actors in a communication tool are the sender, the recipient(s) and a single service provider, referred to as the "company providing the service". This architecture is the same, irrespective of whether the information exchanged is via telephony, SMS, email or IM. P12 mentioned that the topology of a 3G network is different from that of the Internet (or Wi-Fi). She incorrectly believes there are only the sender and the recipient(s) in a 3G network without a provider.

P1 has never thought of how a communication tool works. She said the process is "too complicated" for her to think about. As long as the message is "sent", "delivered" and "read", she will be satisfied. Also, P11 does not know how communications work.

An important finding of our study is that unlike experts' network centric view, our participants' mental models are somewhat "ego-centric": they see themselves as the centre of their personal communications universe and being able to choose across different tools, which they see as separate channels. For example, 18 participants think that segmenting information and sending different "bits" via different tools means segments cannot be intercepted by the same attacker. Participants assume that attackers can hack one tool or listen to one channel. Participants who have more technical expertise (P2, P4, P5, P16 and P28) showed the same basic mental models (i.e., ego-centric models).

Encrypted communications. When we asked our participants how secrecy of message content can be achieved, P2, P4, P5 and P6 mentioned the terms "encryption" or "decryption" (albeit with simplistic mental models). The remaining participants did not. Hence, we probed and asked what encryption is, why it is used, and how it works (including client-server and E2E encryption, as distinguished by the EFF Scorecard).

Ten participants confused encryption with authentication. Nine mentioned "multiple encryption": using a username and multiple passwords to log in to an account. P12 mentioned "double encryption" to describe two-factor authentication. In other words, "*encryption would be something like what banks use. I have a mobile banking app, but they send me a code in the post, so only I have it, so protection means only I can access it in a way with the unique code*" (P12). P19 stated that when encryption is used, "*it will be harder to get to the data because of the passcode and password used to log in to the account*". He believes that encryption is used to protect the company providing the service from other companies and "hackers". P17 also described encryption as using the account password in a way to protect the data in transit; the more passwords the account has, the stronger the encryption is.

P1 and P59 conflated encryption with data encoding. P1 explained encryption as sending messages in "*computer language: 01010011110100*" (i.e., binary representation) and said "*these messages can only be understood by computer scientists, hackers, service providers and governments. Lay people cannot*". P59 explicitly described encryption as sending text in "*binary language: 122121122*".

Other participants explained encryption as follows:

1) Turning a message into random text that people cannot understand (27 out of 60).
2) Using a special language, such that if someone (like a computer scientist) knows the language, they can decrypt the message (P26, P27, P32 and P35).
3) Using a special code (P14 and P27).
4) Making conversations "invisible" (P14 and P60).
5) Slowing down the process of understanding the data; "*encryption is (no encryption + adding some time to send the data packets)*" (P23).
6) Using proxies when accessing websites to protect against attackers (P29).

Seven participants said they have not heard of encryption and, hence, did not provide any definition.

All participants, except for P2, P4 and P5, believe that encryption protects against the unsophisticated attackers "*who do not know how to hack*" (P32). They believe that service providers should not be able to read exchanged messages in theory, but "*this sort of encryption*" (P9) is not offered by existing communication tools. They think that encrypted communications are futile because the designers who create the encryption scheme know how to decrypt messages. As P15 put it, "*even the ultimate encryption can be broken, like the ENIGMA machine in WWII*".

Only P2, P4 and P5 distinguished between client-server encryption and E2E encryption; they provided a good (although simplistic) understanding of both types of encryption and discussed private-key and public-key cryptography. They also stated that E2E encryption could protect against all types of attackers.

The 57 remaining participants either did not know the difference between both types of encryption or gave wrong answers. For example, P13 equated client-server encryption to SSL, and described E2E encryption as a special encryption program (or software) used to manually encrypt messages. P16 equated keys to passwords, describing client-server encryption as using one key (one password) for encryption and decryption, whereas E2E encryption as using two different keys (two passwords): one for encryption and one for decryption.

Passcodes, digital signatures and fingerprints. Some tools, such as Telegram, allow users to set up a passcode to lock their accounts. However, 45 participants said they do not set up a passcode because it is time-consuming to unlock accounts. They see the phone lock of their handset as sufficient (i.e., Apple's touch ID or passcode, Android's pattern/PIN lock). Others (P4, P11, P14, P15, P39, P40, P56) explicitly said that locking the application has the undesirable effect of being notified that a message has been received *without* the sender's name and text. This is another example of a security feature reducing the utility users are looking for.

57 participants (excluding P2, P4 and P5) provided various incorrect explanations of digital signatures: (1) inserting a USB stick into the PC to sign a document using a unique code, (2) scanning a hand-written signature and then adding the signature electronically to a document, or (3) signing a digital document using a stylus pen. P29 described a digital signature as a specific font type in Microsoft Word used to type names. Only P2 and P5 correctly explained what digital signatures are.

We also asked about verification fingerprints, and only P2 was able to explain them. All participants who use Telegram, for example, believe that the fingerprint in the *Secret Chat* mode is the encryption key shared between the sender and the recipient to encrypt and decrypt messages in transit, or the encrypted message itself.

Account Deletion. At the beginning of the study, we asked our participants to take out their mobile phones and check all the communication tools they have downloaded. All participants (except for P2, P4, P5 and P28) uninstalled a communication tool when they decided to stop using it, believing their accounts and chat history have been removed. We can attribute this misconception to misleading feedback from devices: both iPhone and Nexus warn their users that their data will be deleted if they "delete" a particular application. The warning message does not specify whether "all" the data deleted is the application-related data stored on the phone, or the data associated with the account on the provider's servers.

F. Security Ranking of Communication Services: Calling vs. Messaging

We asked our participants to rank the communication tools they have used in terms of how secure they are. Many participants ranked the services offered by the tools first, rather than ranking the tools. Our participants exhibited high agreement on the relative ranking of services (calling and messaging). All, but seven participants, agreed on the following ranking, ordered from the most to least secure:

1) Voice calls via the mobile network.
2) Voice calls via the Internet (e.g., Wi-Fi).
3) SMS messages (mobile network).
4) Emails (Internet).
5) Instant messages (Internet).

Seven participants (P2, P5, P37, P42, P45, P47 and P51) disagreed with the ranking above, noting that voice calls have the same security level as messages because several communication tools (e.g., WhatsApp, Google Hangouts) offer both services.

Calls are more secure than messages. Below, we discuss the reasons given by our participants for why calls are more secure than messages:

1) According to most participants (53 out of 60), there is no mass surveillance of phone calls. They are aware that phone calls can be intercepted, but think it is unlikely unless a government agency is monitoring a specific person. According to P17, the calling parties "*need to be targeted during their conversation. This requires special wiretapping equipment*".

2) Nine participants believe that routine recording of phone calls requires many resources, such as disk space. Hence, they do not consider phone calls being recorded and stored on the provider's servers a threat. P17 also mentioned that text and multimedia messages are "*discarded from the servers as long as they were not suspicious*". In fact, providers store messages for long periods of time [72].

3) Nine participants mentioned that a phone call requires a lot of time and effort to process and analyze, compared to a text message. They stated that a human has to listen to a phone call and extract the sensitive information (as portrayed in movies, perhaps most memorably "*The Lives of Others*"). It is onerous to convert audio to text for analysis, whereas text messages can be easily searched for specific keywords. We speculate this is because participants are used to word processors that scan text for words, but have never seen this technology for scanning audio.

4) Seven participants mentioned that there is a record of text messages stored on the user's device. They said that if the user's device gets compromised, the adversary can access all previously sent messages, unless the user deletes their chat history regularly (something none of our participants regularly does). P12 also mentioned that it should be common practice not to write sensitive information down on a piece of paper or as a text message, regardless of whether the tool is secure or not. Sensitive information should be shared in person, or via a phone call (if the situation is urgent)

"*because there is no chat history of calls*". 16 participants mentioned that it is possible to capture a sensitive exchange by taking a screen-shot of a message, not something attackers can do with a phone call. This finding suggests users have a rudimentary understanding of forward secrecy, unconnected to the cryptographic definition.

SMS is the most secure messaging service. We have discussed why users regard voice calls more secure than messages above. We here provide the rationale behind why SMS messages are perceived as the most secure, while emails the second most secure, and instant messages the least secure. According to our participants:

1) Telephone service providers, as opposed to email (and IM) service providers, are regulated by the government. Hence, the mobile phone network can protect against competing companies seeking intelligence, as opposed to the Internet (33 out of 60).

2) Many banks send banking details and notifications (regarded as sensitive information by our participants) via SMS messages, so SMS must be secure (32 out of 60).

3) SMS is accessible only through the "Messages" application on the phone, whereas email systems and IM tools can be accessed through the PC as well, increasing the scope of vulnerability (P21, P26, P29, P39 and P50).

4) Emails and instant messages (text and multimedia messages) are less secure than SMS messages because email systems and IM tools are "free" (30 out of 60), and the Internet is less secure than other networks (e.g., 3G) (see point 1 above). According to P12, "*privacy is a general problem of the Internet*". In contrast, P2 and P5 believe it is possible to communicate over the Internet securely if vulnerabilities do not exist.

5) Email was designed to send formal messages and not to socialize, as opposed to IM tools (28 out of 60). As far as our participants are concerned, formality of messages indicates better security. In contrast, P12 believes that Gmail (an email service) and Google Hangouts (an IM tool) are one entity, hence, they have the same level of security. Also, P17 and P24 mentioned that their Yahoo! email account has been hacked, hence, Yahoo! Messenger is perceived as insecure because Yahoo! email and Yahoo! Messenger are one entity. We discuss this theme in more detail in Section IV-G.

Some participants (29 out of 60) believe that "professional" email (e.g., Outlook, P11's university email) is more secure than "commercial" email services (e.g., Gmail), provided that the sender and the recipient have professional email accounts. According to P11, there is no clear evidence that Outlook is more secure than Gmail. However, since she receives more spam emails in her Gmail's spam folder, she believes that Gmail is less secure. Also, P11's university sends regular warnings about spam emails, which is interpreted as a sign that the university cares about protecting Outlook, as opposed to Gmail that "*only has a folder for spams*". Here, we have an example of effortful but visible security that makes the participant believe that Outlook is secure, whereas security being done automatically (i.e., the filtering done by Gmail) makes her perceive Gmail as insecure due to invisible security.

Other participants (15 out of 60) feel secure as long as they use their university email account, even if the recipient does not use the same email system. P14 and P18 believe that the university email account is more secure than Gmail because the university (an educational, non-profit organization) owns the service and is responsible for protecting it. This misconception can be attributed to the ego-centric models explained earlier in Section IV-E.

G. Security Ranking Criteria of Communication Tools

We here discuss the reasons for our participants' rankings of the communication tools they have used, not the services offered by the tools. We provided participants with cards with the names and logos of the tools, and then asked them to rank them from the most to the least secure. Our aim was not to analyze the rankings, but to elicit the rationale behind our participants' choices. We found that our participants base their security rankings of communication tools on several adoption criteria discussed earlier in Section IV-A, namely (1) users bases, (2) QoS, (3) cost of use, (4) registration: telephone numbers vs. usernames, and (5) social influence, rather than on the security properties they expect from a secure tool. Below, we discuss the different reasons given by our participants to justify their rankings of the tools (without necessarily mentioning the most recurrent reasons first).

User bases. 20 participants believe that popular communication tools (e.g., Facebook Messenger, WhatsApp) have large user bases and, hence, they are more likely to be targeted. 10 participants, on the other hand, believe that Facebook Messenger is more secure than Yahoo! Messenger because more people use the former and, hence, there is more investment to secure it.

QoS. The QoS our participants experience while using a tool influences their perceptions of how secure the tool is (40 out of 60). For example, P7 and P17 said that Viber has low audio/video quality: "*the signal is bad, and there are continuous disconnections*" (P7), which means it is also less secure compared to other tools. P12 believes that Google Hangouts is secure because its audio/video quality is better than that of, for example, Skype.

Cost of use. 40 participants mentioned that "cheap" tools should not be trusted. For example, P59 thinks that Blackberry Messenger Protected offers better security compared to "*other free tools*" because its subscription cost is high. 22 participants also said that tools with advertisements are insecure.

Registration: telephone numbers vs. usernames. 27 participants perceive WhatsApp as more secure than other tools because it requires a phone number when creating an account. They said that using the phone number is a guarantee the account can only be accessed from the users' phone. The phone is seen as strongly linked to the communication partner, whereas other IM tools that require a username and a password can be "easily hacked". P2, P5 and P48 see no difference between both methods.

Integration with other tools. 25 participants distrust tools used in combination with other less secure tools. For instance, 10 participants said that if a user imports their personal details from Facebook to WhatsApp, WhatsApp's security will drop to that of Facebook.

Tools integrated with SMS. Many participants believe that SMS is more secure than IM for several reasons previously discussed in Section IV-F. However, 12 participants who use iMessage and Google Hangouts on their phone have the misconception that these two IM tools are equivalent to SMS and, hence, have the same security level. For instance, P6 stated that "*iMessage is designed as part of Apple's SMS service*". He sends banking details via iMessage for this reason.

Attractive UIs. 22 participants stated that if the tool creators care enough to make the tool usable, they will also care about its security. A "bad" (unattractive) UI is a sign that the developer "does not care" or is not competent, so the security of the tool is also likely to be shoddy. P17 and P23 cited Kik and Ebuddy XMS as examples. This finding shows that a good user experience on one aspect of the tool increases trust in the competence and motivation of the developers.

Visible security. Visible security indicates "there must be a threat". 21 participants believe that the mobile version of a communication tool is more secure than other tools accessed via browsers because users do not have to deal with HTTPS locks and certificates. Hence, they prefer to have a standalone desktop application similar to that on the mobile phone. According to P27, "*the information is just on your device, it is not easy to access data on a personal device, as opposed to the web browser*".

An emerging theme is that our participants' experience of warning messages and need for security indicators lead them to perceive the services they access via web browsers as insecure. Applications on mobile phones have comparatively fewer indicators and warnings and are, thus, perceived to be more secure, despite this being technically incorrect [73], [74]. 30 participants also think that the probability of a mobile phone getting infected by a "virus" is lower than that of a PC because (1) they have never experienced any issue with their phones, unlike PCs, and have never installed a mobile phone version of an anti-virus program, and (2) the sender of an instant message is known, unlike SMS and email: "*there are spam emails, but not spam instant messages*" (P18).

Social influence. Social factors largely influence participants' perceptions of the security offered by a communication tool (54 out of 60). Some tools are deemed more secure and trustworthy than others because a friend, colleague, or newspaper article said so.

Geopolitical context. The local laws and practices that a service provider is subject to influence perception. P12 believes Facebook Messenger is less secure than other tools because Facebook is US-based. She believes that US government agencies, the NSA in particular, are able to read transmitted data. Hence, she does not share sensitive information via Facebook Messenger. Five participants mentioned that Threema is the most secure tool because Germans "who are more privacy-concerned" use it extensively, showing the "crowd follower" characteristics described in [75].

Self-destructing messages. P15 and P43 believe Telegram's *Secret Chat* mode deceives participants into thinking that messages are deleted from the recipient side, when they are actually stored on the server. They compare Telegram to Snapchat and believe both are insecure.

Open-source vs. proprietary tools. Kerckhoffs' principle of avoiding security-by-obscurity is well-established in the cryptographic literature. However, 51 out of 60 participants largely believe obscurity is necessary for security. P6, P12, P13, P18, P26, P36 and P59 explicitly stated that Apple products are secure because they are closed-source. However, Garman et al. found significant vulnerabilities in iMessage that can be exploited [76]. Our participants are not aware of the long line of cases where proprietary encryption schemes have been broken, despite recent high-profile cases, such as the Volkswagen key [77].

Finally, seven participants (P3, P4, P8, P11, P19, P22 and P26) did not rank the communication tools, perceiving them to have the same level of security for several reasons:

No clear understanding of security. P3, P4, P8, P11 and P26 did not compare the tools. They said they do not understand what makes a communication tool secure. P8 said that companies do not provide a clear definition of security because "*things are always changing*", and what is secure today will not be secure tomorrow. Legal liability is seen as another reason: P26 believes companies want to be able to change the definition of security in privacy policies in response to developments.

Security is expensive. P3, P19, P22 and P26 believe none of the tools are secure because security is expensive, and the companies who own these tools put profit first. They said that PII and conversations are not protected because most tools are free. Without data collection, advertisements cannot be generated and, hence, there will be no profits.

Past experiences. P19 and P22 believe that all messengers are secure because they have never experienced a breach. P24 and P46, in contrast, experienced a security breach with Yahoo! Messenger: "*But, talking about this Yahoo! thing, my Yahoo! email account is probably one of the least secure because actually, you know, it has got hacked again recently*" (P46). Hence, they believe all tools are insecure.

Security is not possible. P8 believes that "*completely secure*" tools exist only in theory. Due to bugs, software can be attacked and communications traced. P2 and P12 were the only participants to mention that one can evaluate the security of a tool based on how well the program is written, and that source code should be audited. P12, however, believes that audits need to be confidential because the designs of secure tools should not be published (see Section IV-D on threat models).

H. EFF Secure Messaging Scorecard

We provided our participants with the first-generation EFF Secure Messaging Scorecard [2] (printed on a sheet of paper), and invited them to compare their rankings with those

of the scorecard. Not a single participant gave a ranking that reflected the scorecard. The scorecard contains seven security criteria. Four criteria are completely misunderstood: participants do not appreciate the difference between point-to-point and E2E encryption, and do not comprehend forward secrecy and fingerprint verification. The other three criteria reflecting open design (documentation, open-source code and security audits) are considered to be *negative*, with participants believing security requires obscurity. We describe below how participants perceive the importance of the scorecard's criteria.

Encrypted in transit vs. encrypted so the provider can't read it. 57 participants (except for P2, P4 and P5) do not differentiate between point-to-point encryption and E2E encryption. Recent literature [41] suggests that users develop more trust in an encrypted communication system that makes the cipher-texts visible. However, whether the cipher-text is visible or not, our participants do not know what security properties each tool offers, and they (incorrectly) believe that encryption can be broken anyway (see Section IV-D).

Can you verify contact's identity? Recent studies [50], [51] have assessed the usability and security of various representations of verification fingerprints. However, no participant (except for P2) appreciates why some communication tools can verify a contact's identity (i.e., the role of fingerprints).

Are past communications secure if your keys are stolen? All participants (except for P2 and P5) do not recognize the importance of forward secrecy.

Open design. The EFF Scorecard has three explicit criteria to ensure the design and code have undergone independent reviews. Our participants, in contrast, said proprietary tools are more secure. This belief in "security by obscurity", an anathema to security researchers, stems from the fact that users perceive security properties to be akin to trade secrets: if a skilled attacker learns how a tool works, they can compromise it. This fundamental misconception feeds the perception of futility. Only P2, P5 and P28 appreciate open design.

V. Discussion

Most user studies of secure communication tools, in particular encrypted email, have been lab studies conducted following the same pattern (see Section II): assessing the usability of specific tools in an artificial setting, where participants are given a series of security tasks associated with those tools (e.g., managing keys, sharing keys, encrypting a message) with fictional communication partners (study coordinators) to accomplish a particular security goal (e.g., confidentiality) without errors, and then measuring success, or failure, based on the goals and tasks imposed on participants, rather than being their own.

Indeed, users will not adopt a communication tool if they cannot use it effectively and efficiently. Our study identified some usability problems (e.g., participants who used Telegram were not able to recognize the *Secret Chat* mode). However, our results also show that to be adopted, secure tools have to offer their intended users utility; i.e., the ability to reach their communication partners. Security may be part of users' primary communication goals, but given a choice between a usable and secure tool that does not offer utility and a usable but insecure tool that does, users choose the latter. Our results suggest it is unrealistic to expect that users will switch to secure tools and only communicate with those who do the same. Also, they will not expend the effort associated with maintaining two communication tools (one secure and one insecure) depending on whom they are talking to. For example, our participants with iOS devices used WhatsApp and Skype, instead of iMessage and FaceTime, even when communicating with other Apple users. Although they perceived the Apple services as more secure (see Section IV-G), they did not live in an Apple-only universe; using different tools was perceived as an overhead they were not willing to carry for security.

When a new tool is usable and attractive enough, users may accept the initial switching cost and adopt it. However, creating a new tool that will be adopted by a critical mass of users requires resources and a set of skills (e.g., user research, user experience design, communication, affective interaction, marketing) the creators of secure communication tools do not have at their disposal. If we want users to adopt secure communications in the near future, security engineers should consider putting their skills to securing tools that have a large use base. WhatsApp's implementation of E2E encryption for text, voice calls and video communications is an example of this more pragmatic approach [18].

In [61], De Luca et al. found that security and privacy are not a primary factor that drives users to adopt a particular messenger. We argue that this is not because users do not care about security at all. Users are aware of some threats and willing to make some effort to manage them (e.g., by chopping up credentials into segments and sending these via different tools). Our participants preferred these quite cumbersome processes, instead of using a secure tool, because they did not believe the tools available are actually secure. This impression was fed by several misconceptions (e.g., they believed service providers can read E2E-encrypted messages). Besides the lack of usability and utility, such misconceptions undermined the case for adoption in their eyes.

There are some users who want to be secure and are "shopping" for tools that offer specific security properties. The EFF Secure Messaging Scorecard [2] aims to tell users about what security properties various communication tools actually offer. Our findings show that the scorecard is not supporting typical users effectively because our participants did not understand these fine-grained security properties. Indeed, participants believed these properties are either impossible to achieve or detrimental to security (like open design). These misunderstandings cannot be fixed by just changing the wording on the scorecard, as our results show that participants had very inaccurate understanding of fundamental security properties, such as confidentiality (see Section IV-E).

The key takeaway from mental models research is that non-experts do not understand abstract security properties. They can only understand why a property matters in the context of a specific threat model that matters to them. For

example, if users do not want their service providers to be able to read their messages, we need to explain how E2E encryption protects against this threat. Based on our results, our participants' existing models were the "toxic root" of their belief that ultimately using any form of a secure tool is futile because they believed even the best encryption scheme can be broken by the resources and skills of governments and service providers. We need to make users understand that it is in their power to protect themselves because several security mechanisms have been developed based on the best available knowledge from security research, and are open to audits by security researchers and practitioners.

Based in part on our feedback, the EFF is redesigning the scorecard to group tools into general tiers from "most secure" to "insecure". Instead of check marks for specific properties, textual descriptions will be provided for what security properties each tool provides. The goal is to help casual readers correctly understand which tools are considered secure (e.g., E2E-encrypted) without needing to understand security mechanisms specifically, while also providing text to help readers acquire accurate mental models of confidentiality, integrity and authentication. The scorecard will also attempt to provide more non-security information that users desire: Does the tool have a large user base? What devices/platforms is it available on? Can it be used over 3G and Wi-Fi? Does it offer audio or video chats? Is the tool free? While not necessarily related to security and privacy, these items drive adoption and would be recommended to include them in the scorecard.

A final interesting high-level observation is that while efforts to secure email systems with PGP that were interoperable across email providers failed on the usability front, current approaches (e.g., iMessage) succeed on the usability front at the expense of interoperability with different devices. We believe examining whether some of the lessons learnt from securing these communication tools can be transferred to interoperable secure tools without sacrificing usability is an interesting open research question for the security community.

VI. Concluding Remarks

Our research, based on 10 unstructured and 50 semi-structured interviews, provides the broadest study of user perceptions of secure communications to date. Although our participants have experienced usability issues with different communication tools, these are not the primary obstacles to adopting secure tools. Low motivation to adopt secure communications is due to several factors (e.g., small user bases, lack of interoperability, incorrect mental models of how secure communications work). Based on our findings, we conclude with three concrete recommendations:

Secure tools with proved utility. We encourage the security community to prioritize securing the communication tools that have already been adopted by mainstream users over improving the usability of different secure tools. Users' goal to communicate with others overrides everything else, including security. Growing a user base for a new tool is difficult and unpredictable. Therefore, we encourage security researchers to work with today's existing popular tools.

Understand the target population. In the long run, if security developers want to develop new paradigms and secure communication tools using a user-centered design process, they need to understand users' goals and preferences. The technical security community must develop a deeper understanding of what is important (and not important) to users. Security properties and threats should be framed in terms that users can understand.

Improve QoS. Secure communication tools must feel professional. Security itself is difficult for users to evaluate directly; they often use proxy signals. This suggests that engineering effort spent on improving the performance of cryptographic tools still matters to the extent that it can reduce latency and dropped packets.

VII. Acknowledgments

We thank the reviewers for their helpful comments and suggestions. This work is supported by a gift from Google. Joseph Bonneau is supported by a Secure Usability Fellowship from the Open Technology Fund and Simply Secure.

References

[1] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith, "SoK: Secure Messaging," in *IEEE Symposium on Security and Privacy*, 2015, pp. 232–249.

[2] Electronic Frontier Foundation (EFF), "Secure Messaging Scorecard," https://www.eff.org/secure-messaging-scorecard, accessed on: 09.07.2016.

[3] D. Yadron, "Apple Transparency Report: Over 1,000 Government Requests for User Data," *The Guardian*, 2016.

[4] S. Gibbs, "Gmail Does Scan All Emails, New Google Terms Clarify," *The Guardian*, 2014.

[5] R. Anderson, "Why Cryptosystems Fail," in *ACM Conference on Computer and Communications Security*, 1993, pp. 215–227.

[6] S. Fahl, M. Harbach, H. Perl, M. Koetter, and M. Smith, "Rethinking SSL Development in an Appified World," in *ACM Conference on Computer and Communications Security*, 2013, pp. 49–60.

[7] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in *USENIX Security Symposium*, 1999.

[8] S. L. Garfinkel and R. C. Miller, "Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express," in *ACM Symposium on Usable Privacy and Security*, 2005, pp. 13–24.

[9] S. Clark, T. Goodspeed, P. Metzger, Z. Wasserman, K. Xu, and M. Blaze, "Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System," in *USENIX Security Symposium*, 2011, pp. 8–12.

[10] M. Lee, "Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance," *Freedom of the Press Foundation*, 2013.

[11] "Tips, Tools and How-tos for Safer Online Communications," https://ssd.eff.org/en, accessed on: 19.08.2016.

[12] McGregor, Susan E, "Digital Security and Source Protection for Journalists," http://towcenter.org/digital-security-and-source-protection-for-journalists-research-by-susan-mcgregor/, accessed on: 20.08.2016.

[13] "The OpenPGP Alliance Home Page," http://www.openpgp.org/resources/downloads.shtml, accessed on: 20.08.2016.

[14] "Tor," https://www.torproject.org/projects/torbrowser.html.en, accessed on: 20.08.2016.

[15] "Tails: The Amnesic Incognito Live System," https://tails.boum.org/, accessed on: 20.08.2016.

[16] "Off-the-Record Messaging," https://otr.cypherpunks.ca/, accessed on: 20.08.2016.

[17] "SecureDrop: The Open-source Whistleblower Submission System," https://securedrop.org/, accessed on: 20.08.2016.

[18] Natasha Lomas, "WhatsApp Completes End-to-End Encryption Rollout," https://techcrunch.com/2016/04/05/whatsapp-completes-end-to-end-encryption-rollout, accessed on: 09.09.2016.

[19] A. J. Onwuegbuzie and N. L. Leech, "Validity and Qualitative Research: An Oxymoron?" *Quality & Quantity*, vol. 41, no. 2, pp. 233–249, 2007.

[20] A. Strauss and J. Corbin, "Grounded Theory Methodology," *Handbook of Qualitative Research*, pp. 273–285, 1994.

[21] B. Harry, K. M. Sturges, and J. K. Klingner, "Mapping the Process: An Exemplar of Process and Challenge in Grounded Theory Analysis," *Educational Researcher*, vol. 34, no. 2, pp. 3–13, 2005.

[22] P. R. Zimmermann, *The Official PGP User's Guide*, 1995.

[23] "GPGTools," https://gpgtools.org/, accessed on: 11.07.2016.

[24] "GPG4WiN," https://www.gpg4win.org/, accessed on: 11.07.2016.

[25] "Off-the-Record Communication, or, Why Not To Use PGP," in *ACM Workshop on Privacy in the Electronic Society*, 2004, pp. 77–84.

[26] C. Alexander and I. Goldberg, "Improved User Authentication in Off-the-Record Messaging," in *ACM Workshop on Privacy in the Electronic Society*, 2007, pp. 41–47.

[27] J. Bian, R. Seker, and U. Topaloglu, "Off-the-Record Instant Messaging for Group Conversation," in *IEEE International Conference on Information Reuse and Integration*, 2007, pp. 79–84.

[28] R. Stedman, K. Yoshida, and I. Goldberg, "A User Study of Off-the-Record Messaging," in *ACM Symposium on Usable Privacy and Security*, 2008, pp. 95–104.

[29] I. Goldberg, B. Ustaoğlu, M. D. Van Gundy, and H. Chen, "Multi-party Off-the-Record Messaging," in *ACM Conference on Computer and Communications Security*, 2009, pp. 358–368.

[30] H. Liu, E. Y. Vasserman, and N. Hopper, "Improved Group Off-the-Record Messaging," in *ACM Workshop on Privacy in the Electronic Society*, 2013, pp. 249–254.

[31] "Open Whisper Systems: Signal," https://whispersystems.org/blog/signal/, accessed on: 11.07.2016.

[32] R. Perlman, "The Ephemerizer: Making Data Disappear," *Sun Microsystems, Inc.*, 2005.

[33] R. Geambasu, T. Kohno, A. A. Levy, and H. M. Levy, "Vanish: Increasing Data Privacy with Self-Destructing Data," in *USENIX Security Symposium*, 2009, pp. 299–316.

[34] J. Reardon, D. Basin, and S. Capkun, "SoK: Secure Data Deletion," in *IEEE Symposium on Security and Privacy*, 2013, pp. 301–315.

[35] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X. 509 Public-key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," Tech. Rep., 2002.

[36] P. Gutmann, "PKI: It's Not Dead, Just Resting," *Computer*, vol. 35, no. 8, pp. 41–49, 2002.

[37] M. D. Ryan, "Enhanced Certificate Transparency and End-to-End Encrypted Mail," in *Network and Distributed System Security Symposium*, 2014.

[38] M. Melara, A. Blankstein, J. Bonneau, M. Freedman, and E. Felten, "CONIKS: Bringing Key Transparency to End Users," in *USENIX Security Symposium*, 2015.

[39] G. Cluley, "WhatsApp Doesn't Properly Erase Your Deleted Messages, Researcher Reveals," https://www.hotforsecurity.com/blog/whatsapp-doesnt-properly-erase-your-deleted-messages-researcher-reveals-16169.html, accessed on: 02.08.2016.

[40] S. Ruoti, N. Kim, B. Burgon, T. Van Der Horst, and K. Seamons, "Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes," in *ACM Symposium on Usable Privacy and Security*, 2013, p. 5.

[41] S. Ruoti, J. Andersen, S. Heidbrink, M. O'Neill, E. Vaziripour, J. Wu, D. Zappala, and K. Seamons, ""We're on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users," in *ACM Conference on Human Factors and Computing Systems*, 2016.

[42] J. Nielsen and R. Molich, "Heuristic Evaluation of User Interfaces," in *ACM Conference on Human Factors and Computing Systems*, 1990, pp. 249–256.

[43] W. Bai, D. Kim, M. Namara, Y. Qian, P. G. Kelley, and M. L. Mazurek, "An Inconvenient Trust: User Attitudes toward Security and Usability Tradeoffs for Key-Directory Encryption Systems," in *ACM Symposium on Usable Privacy and Security*, 2016, pp. 113–130.

[44] S. L. Garfinkel, D. Margrave, J. I. Schiller, E. Nordlander, and R. C. Miller, "How to Make Secure Email Easier to Use," in *ACM Conference on Human Factors and Computing Systems*, 2005, pp. 701–710.

[45] J. F. Ryan and B. L. Reid, "Usable Encryption Enabled by AJAX," in *IEEE International Conference on Networking and Services*, 2006, pp. 116–116.

[46] S. Sheng, L. Broderick, C. A. Koranda, and J. J. Hyland, "Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software," in *ACM Symposium on Usable Privacy and Security*, 2006, pp. 3–4.

[47] E. Atwater, C. Bocovich, U. Hengartner, E. Lank, and I. Goldberg, "Leading Johnny to Water: Designing for Usability and Trust," in *ACM Symposium on Usable Privacy and Security*, 2015, pp. 69–88.

[48] S. Ruoti, J. Andersen, D. Zappala, and K. Seamons, "Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client," *arXiv preprint arXiv:1510.08555*, 2015.

[49] S. L. Garfinkel, "Enabling Email Confidentiality through the Use of Opportunistic Encryption," in *Annual National Conference on Digital Government Research*, 2003, pp. 1–4.

[50] S. Dechand, D. Schürmann, T. IBR, K. Busse, Y. Acar, S. Fahl, and M. Smith, "An Empirical Study of Textual Key-Fingerprint Representations," in *USENIX Security Symposium*, 2016.

[51] J. Tan, L. Bauer, J. Bonneau, L. Cranor, J. Thomas, and B. Ur, "Can Unicorns Help Users Compare Crypto Key Fingerprints?" in *ACM Conference on Human Factors and Computing Systems*, 2017.

[52] S. L. Garfinkel, J. I. Schiller, E. Nordlander, D. Margrave, and R. C. Miller, "Views, Reactions and Impact of Digitally-Signed Mail in E-commerce," in *Financial Cryptography and Data Security*, 2005, pp. 188–202.

[53] J. Sobey, R. Biddle, P. C. Van Oorschot, and A. S. Patrick, "Exploring User Reactions to New Browser Cues for Extended Validation Certificates," in *European Symposium on Research in Computer Security*, 2008, pp. 411–427.

[54] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. E. Acer, E. Morant, and S. Consolvo, "Rethinking Connection Security Indicators," in *ACM Symposium on Usable Privacy and Security*, 2016, pp. 1–14.

[55] F. Roesner, B. T. Gill, and T. Kohno, "Sex, Lies, or Kittens? Investigating the Use of Snapchat's Self-destructing Messages," in *Financial Cryptography and Data Security*, 2014, pp. 64–76.

[56] S. Gaw, E. W. Felten, and P. Fernandez-Kelly, "Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted E-mail," in *ACM Conference on Human Factors in Computing Systems*, 2006, pp. 591–600.

[57] K. Renaud, M. Volkamer, and A. Renkema-Padmos, "Why Doesn't Jane Protect Her Privacy?" in *Privacy Enhancing Technologies Symposium*, 2014, pp. 244–262.

[58] S. Das, T. H.-J. Kim, L. A. Dabbish, and J. I. Hong, "The Effect of Social Influence on Security Sensitivity," in *ACM Symposium on Usable Privacy and Security*, vol. 14, 2014.

[59] S. Das, A. D. Kramer, L. A. Dabbish, and J. I. Hong, "Increasing Security Sensitivity with Social Proof: A Large-scale Experimental Confirmation," in *ACM Conference on Computer and Communications Security*, 2014, pp. 739–749.

[60] ——, "The Role of Social Influence in Security Feature Adoption," in *ACM Conference on Computer Supported Cooperative Work and Social Computing*, 2015, pp. 1416–1426.

[61] A. De Luca, S. Das, M. Ortlieb, I. Ion, and B. Laurie, "Expert and Non-Expert Attitudes towards (Secure) Instant Messaging," in *ACM Symposium on Usable Privacy and Security*, 2016.

[62] P. Dourish, R. E. Grinter, J. D. De La Flor, and M. Joseph, "Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem," *Personal and Ubiquitous Computing*, vol. 8, no. 6, pp. 391–401, 2004.

[63] R. Wash, "Folk Models of Home Computer Security," in *ACM Symposium on Usable Privacy and Security*, 2010, p. 11.

[64] H. Sharp, Y. Rogers, and J. Preece, *Interaction Design: Beyond Human-Computer Interaction*, 2007, vol. 11, no. 4.

[65] P. N. Johnson-Laird, *Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness*. Harvard University Press, 1983, no. 6.

[66] R. H. Bernard, *Non-probability Sampling: Social Research Methods: Qualitative and Quantitative Approaches*. SAGE, 2006.

[67] C. Seale, "Quality in Qualitative Research," *Qualitative Inquiry*, vol. 5, no. 4, pp. 465–478, 1999.

[68] J. Cohen, "A Coefficient of Agreement for Nominal Scales," *Educational and Psychosocial Measurement*, vol. 20, no. 1, pp. 37–46, 1960.
[69] J. L. Fleiss, B. Levin, and M. C. Paik, *Statistical Methods for Rates and Proportions*. John Wiley & Sons, 2013.
[70] D. Cole, "'We Kill People Based on Metadata'," http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/, accessed on: 09.07.2016.
[71] G. Danezis and C. Diaz, "A Survey of Anonymous Communication Channels," Microsoft Research, Tech. Rep., 2008.
[72] "Snapchat Law Enforcement Guide," http://www.documentcloud.org/documents/717257-snapchat-law-enforcement-guide-12112-1.html, accessed on: 11.06.2016.
[73] S. Fahl, M. Harbach, T. Muders, L. Baumgärtner, B. Freisleben, and M. Smith, "Why Eve and Mallory Love Android: An Analysis of Android SSL (in)Security," in *ACM Conference on Computer and Communications Security*, 2012, pp. 50–61.
[74] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov, "The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software," in *ACM Conference on Computer and Communications Security*, 2012, pp. 38–49.
[75] A. Morton and M. A. Sasse, "Desperately Seeking Assurances: Segmenting Users by Their Information-Seeking Preferences," in *IEEE Annual International Conference on Privacy, Security and Trust*, 2014, pp. 102–111.
[76] C. Garman, M. Green, G. Kaptchuk, I. Miers, and M. Rushanan, "Dancing on the Lip of the Volcano: Chosen Ciphertext Attacks on Apple iMessage," in *USENIX Security Symposium*, 2016.
[77] R. Verdult, F. D. Garcia, and B. Ege, "Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer," in *USENIX Security Symposium*, 2015, pp. 703–718.

APPENDIX
PRE-SCREENING QUESTIONNAIRE

- Please indicate which of the following ranges your age falls within.
  - ☐ Under 18
  - ☐ 18 – 20
  - ☐ 21 – 30
  - ☐ 31 – 40
  - ☐ 41 – 50
  - ☐ 51 – 60
  - ☐ 61 – 70
  - ☐ 70+
- Please indicate your gender.
  - ☐ Male
  - ☐ Female
  - ☐ Prefer not to say
- What is your highest level of education? If you are currently enrolled, please specify the highest level/degree completed.
  - ☐ Some high-school education
  - ☐ High-school education or equivalent
  - ☐ Some college education (incomplete degree)
  - ☐ College degree (e.g., BSc, BA)
  - ☐ Graduate degree (e.g., MSc, MA, MBA, PhD)
  - ☐ Vocational training (e.g., NVQ, HNC, HND)
  - ☐ Other
- If you have (or are currently pursuing) a BSc or BA degree, what is your area of study?
- If you have (or are currently pursuing) an MSc, MA or MBA degree, what is your area of study?
- If you have (or are currently pursuing) a PhD degree, what is your area of study?
- What is your current employment status?
  - ☐ Student
  - ☐ Employed
  - ☐ Self-employed
  - ☐ Unemployed
  - ☐ Retired
- If employed, what is your current occupation?
- Do you own a desktop computer and/or a laptop?
  - ☐ Yes ☐ No
- Do you own a smartphone?
  - ☐ Yes ☐ No
- What communication tools have you ever used? Please select all that apply.
- What computing platforms do you use to communicate with your contacts via communication tools? Please select all that apply.
  - ☐ Android (e.g., Google Nexus, Galaxy Samsung)
  - ☐ iOS (e.g., iPhone)
  - ☐ Microsoft Windows
  - ☐ Mac OS X
  - ☐ Other

The following questions assessed participants' general technical expertise.

- Do you have an engineering or computer science background?
  - ☐ Yes ☐ No
- Have you ever configured a network firewall?
  - ☐ Yes ☐ No ☐ Do not know
- Have you ever written a computer program?
  - ☐ Yes ☐ No ☐ Do not know
- Have you ever changed your web browser's search engine (e.g., Google, Yahoo! Search, Bing, Ask.com)?
  - ☐ Yes ☐ No ☐ Do not know
- Have you ever changed your web browser's homepage?
  - ☐ Yes ☐ No ☐ Do not know
- Have you ever registered a domain name?
  - ☐ Yes ☐ No ☐ Do not know
- Have you ever designed a website?
  - ☐ Yes ☐ No ☐ Do not know
- Have you ever unscrewed anything on your PC or laptop?
  - ☐ Yes ☐ No ☐ Do not know

The following questions assessed participants' cyber-security threat exposure.

- Have you ever lost data because of an infected computer (e.g., Trojan horse, virus or worm infection)?
  - ☐ Yes ☐ No ☐ Do not know
- Have you ever been impersonated (or have your account credentials been stolen)?
  - ☐ Yes ☐ No ☐ Do not know
- Have you ever fallen for a phishing e-mail?
  - ☐ Yes ☐ No ☐ Do not know
- Has your personal data ever been misused?
  - ☐ Yes ☐ No ☐ Do not know
- Have you ever received an unsolicited e-mail (i.e., spam)?
  - ☐ Yes ☐ No ☐ Do not know