Designing User-Centered Privacy-Enhancing Technologies

Ruba Abu-Salma

A dissertation submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

of

University College London

Department of Computer Science
University College London
I, Ruba Abu-Salma, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the work.
Abstract

Computer security and privacy experts have always advocated the widespread adoption of privacy-enhancing technologies (PETs). However, it remains unclear if mainstream users\(^1\) understand what protection these technologies offer. Unlike prior work, we take a user-centered approach to evaluating the user experience, and improving the design, of two PETs: secure (mainly encrypted) communications and private browsing.

Prior studies have shown poor usability primarily hampers the adoption and use of secure communication tools. However, we found – by conducting five qualitative (n=102) and two quantitative (n=425) user studies – that, in addition to poor usability, lack of utility and incorrect user mental models of secure communications are primary obstacles to adoption.

Users will not adopt a communication tool that is both usable and secure, but lacks utility (due to, e.g., the tool’s small userbase). Further, most users do not know what it means for a usable and secure tool that is widely-adopted and offers utility (e.g., WhatsApp) to be end-to-end encrypted. Incorrect mental models of encryption lead people to use less secure channels that they incorrectly perceive as more secure than end-to-end encrypted tools.

Thus, we argue the key user-related challenge for secure communications is not only fostering adoption, but also emphasizing appropriate use – by helping people who already use secure tools avoid sending sensitive information over less secure channels. By

\(^1\)This thesis focuses on exploring the needs, practices, and perceptions of mainstream users who do not necessarily consider themselves to be at risk of targeted surveillance. This is because our focus of enquiry is widespread adoption of PETs. The thesis also focuses on users who mainly reside and live in the UK.
employing participatory design, we take a user-centered approach to designing effective descriptions that explain the security properties of end-to-end encrypted communications.

Additionally, we take a user-centered approach (as part of a validation study) to evaluating and improving the user experience of another PET: private browsing mode. We conduct a qualitative user study (n=25) to explore the adoption and use of private mode. We employ participatory design and propose guidelines to help create informative browser disclosures that explain the security properties of private mode.
Impact Statement

The findings of this thesis will benefit every-day people who would like to use some form of encrypted chat to communicate. In countries where freedom of speech is guaranteed, people may need encryption to discuss mental health issues. Alternatively, people living within repressive regimes need, for example, to discuss politics secretly. In this thesis, we qualitatively and quantitatively explore the barriers to the adoption and use of encrypted communication tools. We also raise concerns about government and corporate surveillance.

Further, the findings of this thesis will help people who have serious concerns about their online privacy and try to use different privacy tools to protect it. In this thesis, we focus on evaluating and improving the end-user experience of one of these privacy tools: private browsing. We conduct the first qualitative user study to explore the factors that influence users’ adoption and use of private mode in different modern web browsers, as well as investigate user mental models of private mode. We also show why most users of private mode overestimate the benefits of this privacy tool.

Finally, this thesis will help developers who are interested in designing and building PETs, such as encrypted communications and private browsing. We conduct constructive research by providing clear and concrete recommendations that will help developers address unmet needs among mainstream users, as well as improve the usability of existing tools. Current solutions are built by organizations, and, hence, they are not user-driven. We, in contrast, conduct user-centered research, with the aim to fill a gap in both knowledge and research of useful PETs.
Acknowledgements

This thesis has been shaped by the support and encouragement of a host of people, to whom I would like to express my profound gratitude.

I owe my deepest thanks to my family, who has always encouraged me to be curious, tenacious, and ambitious. My father taught me to love mathematics, from using an abacus to solve arithmetic problems to understanding differential calculus. My mother never accepted my excuses for not completing my schoolwork. At every stage of my academic life, my parents taught me resilience and hard work, and provided me with moral and financial support. My two sisters and brother are my confidants, my cheerleaders, and my best friends. I could not be luckier to have such a loving and supportive family. I love you, all.

I am immensely grateful to my postgraduate supervisor: Prof. M. Angela Sasse. She taught me how to formulate problems and identify feasible research directions. Her comments greatly contributed to the way I thought about the problems discussed in this thesis. I would also like to thank my postgraduate co-supervisors: Dr. Sarah Meiklejohn and Dr. Steven J. Murdoch. Sarah introduced me to members in the usable security and privacy research community. Steven taught me how to temper criticism with kindness and patience, especially when academia is sometimes harsh, hypercritical, and hostile.

I am very grateful for having the opportunity to work with many brilliant research collaborators over the past few years. For the projects I describe in this thesis, I was fortunate to have excellent collaborators (in alphabetical order): Joseph Bonneau, Anastasia Danilova, Steve Dodier-Lazaro, Juliane Kramer, Kat Krol, Benjamin Livshits, Alena Na-
Acknowledgements

I would like to thank the following individuals: Ishakina, Simon Parkin, Elissa M. Redmiles, Scott Ruoti, Kent Seamons, Matthew Smith, Blase Ur, Miranda Wei, Justin Wu, and Daniel Zappala. They introduced me to the joy of research, and I learnt a huge amount from them. Special thanks go to Joseph Bonneau who provided valuable feedback on my first publication [1], which helped me shape my future research. I would like to sincerely thank Cerys Bradley for taking the time to proofread some of my publications.

I was also fortunate to work with fellow students (in alphabetical order) at UCL: Victoria Koh, Kevin Kwan, Jazib Mahboob, Juan Ponce-Mauries, Danial Sabagh, and Zahra Traboulsi. I also enjoyed working with Nathan Bhak, a high-schooler at Westminster School (now at Stanford University).

To (in alphabetical order) Hadeel Al-Negheimish, Gaurav Misra, Jeremiah Onaolapo, and Lucky Onwuzurike, it has been a joy to have you as friends.

I would like to thank my thesis examiners, Prof. Alastair Beresford and Dr. Leonie Maria Tanczer, for their insightful and challenging questions, as well as their suggestions for improving this thesis.

I would like to acknowledge that this thesis would not have been possible without a generous research grant from Google. I was also supported by a SUDS (Supporting Usability and Design in Security) Fellowship from the Open Technology Fund and Simply Secure, as well as a Marie-Skłodowska Curie Research Fellowship.

Finally, I am deeply indebted to everyone who has provided me with support and encouragement.
# Contents

1 **Introduction** .................................................. 21  
   1.1 Research Problem ........................................... 21  
   1.2 Research Questions ........................................... 24  
   1.3 Thesis Contributions ......................................... 25  
   1.4 Published Material ......................................... 26  
   1.5 Research Ethics ............................................. 31  
   1.6 Thesis Structure ............................................ 31  

2 **Literature Review** ........................................... 33  
   2.1 Secure Communications ....................................... 33  
   2.2 User Studies of Secure Communications ...................... 38  
   2.3 Private Browsing Mode ....................................... 45  
   2.4 User Studies of Private Browsing Mode ...................... 48  
   2.5 Mental Models ............................................... 50  
   2.6 Security and Privacy Design .................................. 51  

3 **Why Do People Give Up on Secure Communication Tools? An Explanatory Study with Lapsed Users of Secure Tools**  
   3.1 Introduction .................................................. 57  
   3.2 Methodology .................................................. 61  
      3.2.1 Research Questions ...................................... 62  
      3.2.2 Recruitment ............................................. 62  
      3.2.3 Interview Procedure ..................................... 63  
      3.2.4 Pilot Study ............................................... 66  
      3.2.5 Data Analysis ............................................ 66  
   3.3 Results ..................................................... 67  
      3.3.1 Demographics ............................................. 67
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.2</td>
<td>Adoption Criteria of Communication Tools</td>
<td>67</td>
</tr>
<tr>
<td>3.3.3</td>
<td>Sensitive Information: Perceptions and Practices</td>
<td>71</td>
</tr>
<tr>
<td>3.3.4</td>
<td>Security Properties</td>
<td>73</td>
</tr>
<tr>
<td>3.3.5</td>
<td>Threat Models</td>
<td>74</td>
</tr>
<tr>
<td>3.3.6</td>
<td>Mental Models of (Secure) Communications</td>
<td>79</td>
</tr>
<tr>
<td>3.3.7</td>
<td>Security Ranking of Communication Services: Calling vs. Messaging</td>
<td>83</td>
</tr>
<tr>
<td>3.3.8</td>
<td>Security Ranking Criteria of Communication Tools</td>
<td>86</td>
</tr>
<tr>
<td>3.3.9</td>
<td>EFF Secure Messaging Scorecard</td>
<td>90</td>
</tr>
<tr>
<td>3.4</td>
<td>Discussion</td>
<td>91</td>
</tr>
<tr>
<td>3.5</td>
<td>Summary and Implications</td>
<td>95</td>
</tr>
<tr>
<td>3.6</td>
<td>Limitations</td>
<td>96</td>
</tr>
<tr>
<td>3.7</td>
<td>Contributions to Thesis</td>
<td>96</td>
</tr>
<tr>
<td>4</td>
<td>Dead on Arrival: Recovering from Fatal Flaws in Email Encryption Tools</td>
<td>99</td>
</tr>
<tr>
<td>4.1</td>
<td>Introduction</td>
<td>100</td>
</tr>
<tr>
<td>4.2</td>
<td>Methodology</td>
<td>102</td>
</tr>
<tr>
<td>4.2.1</td>
<td>Research Questions</td>
<td>102</td>
</tr>
<tr>
<td>4.2.2</td>
<td>Recruitment</td>
<td>102</td>
</tr>
<tr>
<td>4.2.3</td>
<td>Study Design</td>
<td>103</td>
</tr>
<tr>
<td>4.2.4</td>
<td>Procedure</td>
<td>104</td>
</tr>
<tr>
<td>4.2.5</td>
<td>Role of the Experimenter</td>
<td>104</td>
</tr>
<tr>
<td>4.2.6</td>
<td>Data Analysis</td>
<td>105</td>
</tr>
<tr>
<td>4.3</td>
<td>Results</td>
<td>105</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Demographics</td>
<td>105</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Task Completion and Times</td>
<td>105</td>
</tr>
<tr>
<td>4.3.3</td>
<td>Qualitative Results</td>
<td>106</td>
</tr>
<tr>
<td>4.4</td>
<td>Discussion</td>
<td>115</td>
</tr>
<tr>
<td>4.5</td>
<td>Limitations</td>
<td>117</td>
</tr>
<tr>
<td>4.6</td>
<td>Contributions to Thesis</td>
<td>118</td>
</tr>
<tr>
<td>5</td>
<td>The Security Blanket of the Chat World: An Analytic Evaluation and a User Study of Telegram</td>
<td>119</td>
</tr>
<tr>
<td>5.1</td>
<td>Introduction</td>
<td>121</td>
</tr>
<tr>
<td>5.2</td>
<td>Telegram</td>
<td>124</td>
</tr>
</tbody>
</table>
8 A Validation Study: Evaluating the End-User Experience of Private Browsing Mode 183

8.1 Introduction .................................................. 185
8.2 Methodology .................................................. 187
  8.2.1 Research Questions ...................................... 187
  8.2.2 Recruitment .............................................. 188
  8.2.3 Part 1: Usability Inspection ............................. 189
  8.2.4 Part 2: Interview-Based Study ......................... 190
  8.2.5 Part 3: Participatory Design Study .................... 192
  8.2.6 Pilot Study ............................................... 195
  8.2.7 Data Analysis ........................................... 197
8.3 Results ....................................................... 197
  8.3.1 Demographics ............................................ 198
  8.3.2 Part 1: Usability Inspection ............................. 199
  8.3.3 Part 2: Interview-Based Study ......................... 201
  8.3.4 Part 3: Participatory Design Study .................... 206
8.4 Discussion ................................................... 209
8.5 Limitations .................................................. 212
8.6 Contributions to Thesis ..................................... 213

9 Conclusion 215

9.1 Summary of Thesis .......................................... 215
9.2 Future Work ................................................... 218
  9.2.1 Designing User-Centered Secure Communication Tools Supporting Group Chat ........................................... 218
  9.2.2 Developing Culturally-Appropriate Educational Materials ........................................... 221

Bibliography 224

Appendices 245

A Pre-Screening Questionnaire (Secure Communications) 245

B Pre-Screening Questionnaire (Private Browsing) 261

C Survey: Evaluating the End-User Experience of Telegram 271
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>Survey: Exploring User Mental Models of End-to-End Encrypted Communi-</td>
<td>301</td>
</tr>
<tr>
<td></td>
<td>cation Tools</td>
<td></td>
</tr>
<tr>
<td></td>
<td>tices</td>
<td></td>
</tr>
</tbody>
</table>
List of Figures

3.1 The EFF Secure Messaging Scorecard. ............................................. 59

4.1 Task times in minutes for Mailvelope and Enigmail. ......................... 106
4.2 The user journey of setting up Enigmail. The graph shows timings for each step of the setup process with notable participant quotes. ........ 107
4.3 The user journey of setting up Mailvelope. The graph shows timings for each step of the setup process with notable participant quotes. .... 108
4.4 A screenshot of the user interface for Mailvelope displaying the encryption button on the right. ..................................................... 114

5.1 Secret Chat mode. ........................................................................ 126
5.2 Options to send a message in Telegram. ......................................... 144
5.3 The security properties of the default chat mode are not described (unlike the Secret Chat mode). ....................................................... 146
5.4 Sending a message in Telegram’s default chat mode (left) and Secret Chat mode (right). The only difference is the small padlock to the left of the contact’s name (here: Kat). .............................................. 147
5.5 Starting a Secret Chat session with a contact. .................................. 148
5.6 A verification fingerprint. ............................................................... 149
5.7 Locking/unlocking Telegram (notice the change in the padlock to the right of the word ‘Chats’). ......................................................... 150

6.1 Proportion of respondents who reported that Soteria text communications were either more or less secure than another type of Soteria communications or non-Soteria communications. We omit respondents who considered the communications equally secure. .................. 166
6.2 Percentage of respondents who thought each entity could gain a particular type of access to their Soteria communications. .................... 168

7.1 ‘End-to-end encryption’ descriptions in Telegram and WhatsApp. ...... 177

8.1 Brave browser disclosure. ............................................................. 194
List of Figures

8.2  Chrome browser disclosure. ............................................. 194
8.3  Firefox browser disclosure. ............................................. 195
8.4  New Firefox browser disclosure. ..................................... 213
List of Tables

2.1 Private browsing functionality in recent web browser versions. A checkmark indicates an item is locally deleted once a user exits private mode, whereas a crossmark indicates an item is locally saved. The table is not fully comprehensive; other items not shown include: browser cache, temporary files, HTML local storage, form auto-completion, client certificates, browser patches, phishing block list, and per-site zoom level. There has been no recent analysis of private browsing since the 2010 work of Aggarwal et al. [2]. The table was created based on the analysis conducted by the thesis author.

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Private browsing functionality in recent web browser versions. A checkmark indicates an item is locally deleted once a user exits private mode, whereas a crossmark indicates an item is locally saved. The table is not fully comprehensive; other items not shown include: browser cache, temporary files, HTML local storage, form auto-completion, client certificates, browser patches, phishing block list, and per-site zoom level. There has been no recent analysis of private browsing since the 2010 work of Aggarwal et al. [2]. The table was created based on the analysis conducted by the thesis author.</td>
<td>47</td>
</tr>
<tr>
<td>2.2</td>
<td>A detailed overview of user studies of private browsing mode (part 1 out of 2).</td>
<td>53</td>
</tr>
<tr>
<td>2.3</td>
<td>A detailed overview of user studies of private browsing mode (part 2 out of 2).</td>
<td>54</td>
</tr>
<tr>
<td>3.1</td>
<td>Unstructured and semi-structured interview participant demographics.</td>
<td>97</td>
</tr>
<tr>
<td>5.1</td>
<td>Participant demographics.</td>
<td>132</td>
</tr>
<tr>
<td>5.2</td>
<td>SUS scores given by novices and users of Telegram participating in the study.</td>
<td>132</td>
</tr>
<tr>
<td>6.1</td>
<td>Cognitive interview participant demographics.</td>
<td>161</td>
</tr>
<tr>
<td>6.2</td>
<td>Demographics of survey respondents.</td>
<td>163</td>
</tr>
<tr>
<td>6.3</td>
<td>Respondents’ familiarity with different communication tools, specifically whether they use each tool currently, used it previously (i.e., “used it before, but stopped using it”), or had heard of it (i.e., “had heard of it, but had not used it”). Some tools that support end-to-end encryption offer this mode by default, while others require users to open a special window (e.g., Facebook Messenger’s Secret Conversations).</td>
<td>164</td>
</tr>
<tr>
<td>7.1</td>
<td>Participant demographics.</td>
<td>178</td>
</tr>
<tr>
<td>8.1</td>
<td>Unstructured interview participant demographics.</td>
<td>187</td>
</tr>
<tr>
<td>8.2</td>
<td>Cognitive interview participant demographics.</td>
<td>197</td>
</tr>
</tbody>
</table>
8.3 Semi-structured interview participant demographics. . . . . . . . . . . 198
Chapter 1

Introduction

1.1 Research Problem

The computer security and privacy community has always advocated the widespread adoption of privacy-enhancing technologies (PETs). However, it remains unclear if users understand what protection these technologies offer, and if they value that protection. Unlike prior work, this thesis takes a user-centered approach to evaluating the end-user experience, and improving the design, of two PETs: secure (mainly encrypted) communications and private browsing.

Secure communications. In light of Edward Snowden’s revelations of mass state surveillance of phone and Internet communications, computer security and privacy experts have advocated the widespread adoption and use of secure communication tools. Many tools nowadays claim to provide secure communications; these include both a wide range of new tools that have been launched with security as a key selling point (e.g., Telegram) and several other widely-adopted tools (e.g., WhatsApp) that have added security features (e.g., end-to-end encryption). However, despite the demand for more secure tools, there is no clear winner in the race for the widespread development and deployment of communication tools.

Designers of computer security systems have typically concentrated on technical weaknesses, such as poor cryptographic algorithms and weak designs of operating sys-
tems, with scant attention to users’ needs. However, computer security tends to fail when interacting with the messiness of the real world, and not mainly due to weaknesses in the underlying systems. This means that security systems are only effective when used and used correctly. If users forget to click on the “Encrypt” button when sending an email or stop using a cryptographic protocol due to their confusion about which cryptographic keys to use, security will be lost, regardless of strong cryptography, unimpeachable access control, and provably correct protocols.

Thus, a user-centered design approach to secure communications is essential. In this endeavour, our aim is to help design cryptographic tools that are both secure and useful. Previous work has concentrated on making cryptography easier for non-security specialists to understand (analogous to explaining how a car engine works) [3]. However, effective security is achieved by involving users in the design activity to ensure their primary communication goals are met. Further, prior user studies of secure communications (e.g., [4–9]) have shown poor usability (mainly, difficulty of use) primarily hampers the adoption of secure tools. However, we found – by conducting five qualitative (n=102) and two quantitative (n=425) user studies – that, in addition to poor usability, lack of utility and incorrect user mental models of how secure communications work are primary obstacles to adoption.

Users will not adopt a communication tool that is both usable and secure, but lacks utility (due to, e.g., the tool’s small userbase, low quality of service, lack of interoperability). Further, most users do not know what it means for a usable and secure tool that is widely-adopted and offers utility (e.g., WhatsApp) to be end-to-end encrypted. Incorrect mental models of encryption lead people to use less secure channels that they incorrectly perceive as more secure than end-to-end encrypted tools.

Thus, we argue the key user-related challenge may no longer be fostering adoption, but emphasizing appropriate use. This does not mean that fostering adoption is not as important as highlighting correct use, but we argue that the usable security and privacy community has been focusing on spurring adoption of secure communications – especially, encrypted communications – for the past twenty years, operating under the ass-
sumption that once an encrypted communication tool has reached critical mass (i.e., has been widely adopted), adoptees will use or continue using that tool appropriately. Our findings show that this is not necessarily true due to users’ incorrect mental models of how encryption works, or what security properties or protection it provides. Hence, we should focus on emphasizing appropriate use – by helping people who already use secure tools avoid sending information, especially information they regard as sensitive, over less secure channels. By employing participatory design, we take a user-centered approach to designing effective descriptions that explain the security properties of end-to-end encrypted communications.

**Private browsing.** Prior work has extensively explored users’ online privacy concerns when using the Internet [10–17]. Several user studies (e.g., [14, 16, 18]) have shown that users have serious concerns about their online privacy and try to employ different strategies or use different privacy tools to protect it. In this thesis, we focus on evaluating the end-user experience of one of these tools: private browsing. Private browsing is a PET that allows a user to browse the Internet without saving information about the websites they visited in private mode on their local device. As of today, all major web browsers have a private browsing mode.

Previous user studies have quantitatively – mainly through survey studies – investigated whether users are aware of private browsing, what they use it for, and whether they understand what protection it provides [19–24]. However, these studies have not investigated why most users misunderstand the benefits and limitations of private browsing mode. Further, the vast majority of recruited participants in these studies were unaware of or had not used private mode. To address these research gaps, we take a user-centered approach to evaluating and improving the end-user experience of private browsing mode. We conduct the first qualitative user study (n=25 users and non-users of private mode) to explore the factors that influence users’ adoption and usage of private mode in different modern web browsers, as well as investigate user mental models of private mode. We also employ participatory design and propose guidelines to help create informative browser disclosures that explain the security properties of private mode.

†The reported numbers of participants we recruited for our qualitative and quantitative user studies do
1.2 Research Questions

The computer security and privacy community has advocated the widespread adoption and use of privacy-enhancing technologies. However, the design of most privacy tools, whilst having a rich research heritage, has typically not involved those who are ultimately meant to use these tools: mainstream users. Therefore, it remains unclear if users understand what protection different privacy tools offer, and if they value that protection. As such, we take a user-centered approach to exploring the factors that influence the adoption and use, as well as improving the design, of two privacy tools: secure (mainly encrypted) communications and private browsing. This thesis addresses the following open research questions:

1. What are the primary obstacles to the adoption of secure communication tools? (Chapter 3)

2. What usability issues beyond ‘difficulty of use’ should the computer security and privacy community look out for when assessing the usability of secure communication tools? (Chapter 4)

3. How does lack of utility (or functionality) negatively influence the use of a usable and secure communication tool? (Chapter 5)

4. Do users understand the security properties offered by secure (in particular, end-to-end encrypted) communication tools? (Chapter 6)

5. Should the computer security and privacy community focus on fostering adoption, without emphasizing appropriate use, of secure communication tools? (Chapter 6)

6. How can a user-centered approach to designing better descriptions of end-to-end encryption improve the end-user experience of encrypted communication tools? (Chapter 7)

not include participants recruited for pilot studies and cognitive interviews conducted to test study scripts and survey questionnaires. Also, every participant we recruited took part in only one of the user studies described in this thesis, to minimize bias and maximize validity.
7. Can a user-centered approach to understanding users’ mental models and usage of a privacy-enhancing technology – other than secure communications – improve the end-user experience and design of that technology? If so, how? (Case study: private browsing) (Chapter 8)

1.3 Thesis Contributions

Usability has long been considered a key challenge for secure communications, especially end-to-end encrypted communications. However, the design of most communication tools has typically not involved those who are ultimately meant to use these tools. One approach has been designing and conducting usability studies to examine why users fail to use existing secure communication tools (e.g., PGP) correctly, often suggesting mitigations involving changes to resolve user interface design flaws.

Another approach has been producing educational materials to explain existing security tools and extensions. 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.

We argue that to design and build communication tools that effectively protect users, we need to understand how mainstream users perceive secure communications, and what influences their decision to adopt (or not adopt) secure tools. Unlike prior work, we found that poor usability is not the only main barrier to adopting secure communication tools. Lack of utility and users’ inaccurate mental models of encrypted communications are also main barriers to adoption. After exploring and understanding the adoption barriers, we conducted a participatory design study to develop high-level educational materials to address user misperceptions of encrypted tools. Rather than waiting for users to find these tools and read long guides, we proposed user-centered, data-driven guidelines to help developers of secure communication tools design and deploy better descriptions that effectively communicate the security properties of end-to-end encrypted communications.

We also took a user-centered approach to designing private browsing. We conducted
the first qualitative study to explore users’ private browsing habits, and how their mental
models influence their understanding and usage of private mode in real life. We further
proposed data-driven guidelines to help developers design better browser disclosures that
communicate the actual protection of private mode.

1.4 Published Material

The content of this thesis is an edited version of the following published papers and poster
abstracts:

**Chapter 3:**

**Paper.** Abu-Salma, R., Sasse, M. A., Bonneau, J., Danilova, A., Naiakshina, A., and
Smith, M. Obstacles to the Adoption of Secure Communication Tools. In *IEEE Symposi-
um on Security and Privacy (Oakland)*, San Jose, CA, USA, 2017 [1].

**Author’s contribution.** The paper describes a qualitative user study (n=60) exploring
the barriers to adopting secure communication tools. The thesis author:

1. designed the study.
2. piloted the study and made all necessary changes to the study script.
3. conducted all 60 face-to-face interviews.
4. analyzed all 60 interview transcripts using Grounded Theory.
5. wrote and presented the paper at the IEEE Symposium on Security and Privacy
   (Oakland), 2017.

**Paper.** Dodier-Lazaro, S., Abu-Salma, R., Becker, I., and Sasse, M. A. From Paternal-
istic to User-Centered Security: Putting Users First with Value-Sensitive Design. In *CHI
Workshop on Values in Computing*, Denver, CO, USA, 2017 [25].
1.4. Published Material

Author’s contribution. The paper presents real-world examples of non-adopting or abandoning secure systems, including secure communications tools, under a paternalistic mindset. It argues why a user-centered approach is needed. The thesis author:

1. helped the first author write and proofread the paper.

2. helped the first author create the presentation slides.


Author’s contribution. The poster abstract presents a user-centered approach to improving the user-experience and design of secure communications. The thesis author:

1. wrote the poster abstract.

2. designed the poster.


Chapter 4:


Author’s contribution. The paper describes a three-part laboratory-based user study (n=10) evaluating the usability of two email encryption tools: Mailvelope and Enigmail. The thesis author:

1. helped design the study.
2. helped conduct the focus group study.

3. helped analyze the interview transcripts.

4. helped write the paper.

5. presented the paper at the Learning from Authoritative Security Experiment Results Workshop, 2017.

Chapter 5:


**Author’s contribution.** The paper describes a two-part study – a laboratory-based user study (n=22) and a usability inspection of the user interface of the Telegram instant messaging tool – evaluating the end-user experience of Telegram. The thesis author:

1. designed the study.

2. piloted the study and made all necessary changes to the study script.

3. conducted all 22 face-to-face interviews.

4. analyzed all 22 interview transcripts using Thematic Analysis.

5. wrote and presented the paper at the European Workshop on Usable Security, 2017.

**Paper.** Abu-Salma, R., Krol, K., Parkin, S., Koh, V., Kwan, K., Mahboob, J., Traboulsi, Z., and Sasse, M. A. Evaluating the User Experience of Telegram (under submission as a journal paper).
**Author’s contribution.** The paper describes a three-part user study – a qualitative user study (n=22); a usability inspection; a survey (n=300) – evaluating the end-user experience of the Telegram instant messaging tool. The thesis author:

1. designed the study.
2. piloted the study and made all necessary changes to the study script and survey questionnaire.
3. conducted all 22 face-to-face interviews.
4. deployed the survey using Prolific Academic and collected survey responses.
5. analyzed all 22 interview transcripts and 300 survey responses using Thematic Analysis.
6. wrote the journal paper.


**Author’s contribution.** The poster abstract summarizes the previous paper. The thesis author:

1. wrote the poster abstract.
2. designed the poster.

**Chapter 6:**

**Author’s contribution.** The paper describes a quantitative user study, a survey (n=125), exploring user mental models of end-to-end encrypted communication tools. The thesis author:

1. designed the study.
2. piloted the study and made all necessary changes to the survey questionnaire.
3. deployed the survey using Prolific Academic and collected survey responses.
4. analyzed all 125 survey responses using Thematic Analysis.
5. wrote and presented the paper at the USENIX Workshop on Free and Open Communications on the Internet, 2018.

**Chapter 8:**


**Author’s contribution.** The paper describes a three-part study – a usability inspection of the user interface of private browsing mode in different modern web browsers; a qualitative, interview-based user study (n=25); a participatory design study (n=25) – evaluating the end-user experience of private browsing mode. The thesis author:

1. designed the study.
2. piloted the study and made all necessary changes to the study script.
3. conducted all 25 face-to-face interviews.
4. analyzed all 25 interview transcripts using Grounded Theory.

1.5 Research Ethics

UCL’s Research Ethics Committee reviewed and approved all user studies described in Chapters 3–7. The Review Board at Brave Software revised and approved the user study described in Chapter 8. Before each interview/survey, we asked participants/respondents to read an information sheet that explained the high-level purpose of our studies. We also asked participants/respondents to sign a consent form that outlined our data-protection practices. We handled all collected data in accordance with the UK Data Protection Act (for studies conducted before May 25, 2018) or the EU General Data Protection Regulation (for studies conducted on/after May 25, 2018). Participants/respondents had the option to withdraw at any point during the studies without providing an explanation. We offered participants/respondents incentives in the form of cash or Amazon vouchers for taking part in our studies. After conducting the studies and analyzing our interview transcripts and survey data, we securely disposed of all collected data.

1.6 Thesis Structure

This thesis is structured as follows: Chapter 2 gives a detailed overview of the field of usable security and privacy, specific to secure communications and private browsing. Chapter 3 describes a qualitative user study to explore the barriers to the widespread adoption of secure communication tools. Chapter 4 presents a novel laboratory-based user study of two email encryption tools – Mailvelope and Enigmail – to investigate the usability issues in modern encrypted email tools. Chapter 5 describes a qualitative and quantitative study to evaluate the end-user experience of the Telegram instant messaging tool. Chapter 6 describes a survey to explore user mental models of end-to-end encrypted communication tools, and Chapter 7 presents a participatory design study to extract data-driven guidelines to help design more informative descriptions that explain the security properties of end-to-end encrypted communications. Finally, Chapter 8 describes a qualitative user study and a participatory design study to evaluate the end-user experience of private brows-
ing mode, and to propose a set of guidelines to help browser designers produce browser disclosures that better communicate the security properties of private mode.
Chapter 2

Literature Review

In this chapter, we give a detailed overview of the field of usable security and privacy, specific to secure communications and private browsing.

2.1 Secure Communications

Secure communication tools became widely available with the release of PGP in 5.0 [31], which was followed by the creation of a large ecosystem of PGP tools (e.g., Enigmail [32], GPGMail [33], GPG4WiN [34], Mailvelope [35], OpenPGP [36]). PGP, which was created by Phil Zimmermann, uses a combination of hashing, data compression, symmetric-key cryptography, and asymmetric-key cryptography. Each public key is bound to a username or an email address. PGP typically uses a web of trust – a decentralized trust model used to establish the association of a public key with its owner – for email encryption and signing. The web of trust is an alternative to the centralized trust model of public key infrastructure (PKI) (most notably supported by the X.509 system\(^1\)), which exclusively relies on a certificate authority or a hierarchy of authorities [37–40]. Current versions of PGP support both centralized and decentralized trust models through an automated key management server.

In classic communication tools, users have to reason about two simple tasks: send-

\(^1\) X.509 certificates are used in many Internet protocols, including SSL/TLS, which is the basis for HTTPS, the secure protocol for browsing the web.
ing and receiving messages (typically, text messages) [41]. In classic, rather old, secure/encrypted communication tools, such as systems based on OpenPGP or S/MIME, additional tasks might be added. If users of OpenPGP or S/MIME systems decided to secure their messages, they would need to manually generate, share, and manage their cryptographic keys, as well as encrypt/decrypt and/or digitally-sign their email. These additional tasks cause a wide range of usability issues, which we explore in Chapter 4.

In order to enable encrypted communications, users of PGP first have to perform trust establishment [41]. Trust establishment, one of the most challenging aspects of communication security, is the process of communication partners verifying that they are actually exchanging messages with or talking to the parties they intend to communicate with. Trust establishment consists of two processes: (1) long-term key exchange and (2) long-term key verification. Long-term key exchange refers to the process where each communication partner sends cryptographic key material to all other partners. Long-term key verification refers to the mechanism (e.g., key fingerprint verification) that allows partners to ensure each cryptographic long-term key is associated with the correct real-world entity (i.e., the partner they intend to communicate with). If trust establishment has been correctly achieved, man-in-the-middle attacks by local adversaries (attackers controlling local networks like owners of open wireless access points) and global adversaries (attackers controlling large segments of the Internet like powerful nation states, government intelligence agencies, or large Internet service providers) are prevented.

After trust establishment has been achieved, PGP provides three basic conversation security features:

1. **Confidentiality (or secrecy of content).** Only the sender and the intended recipient (or recipients in multi-party communications) are able to read exchanged messages or listen to phone calls. That is, any entity that is not a communication partner (or a conversation participant) – such as a government intelligence agency or a service provider – cannot access the content of exchanged messages or phone calls.
2. **Integrity.** Honest communication parties do not accept a message that has been modified or tampered with in transit.

3. **Authentication.** Each communication partner has “a proof of possession of a known long-term secret from every partner that they believe to be participating in a conversation [41].” Further, each partner is able to verify that a received message was authored and sent by the claimed source.

PGP was designed for asynchronous, high-latency email communications. Off-the-Record messaging (OTR) was in turn designed in 2004 for low-latency messaging environments, such as chat clients, introducing new security features or properties (e.g., forward secrecy [41], deniability [41]) [42]. OTR has influenced the design of many communication tools (e.g., [43–48]), including the Signal protocol that has recently gained popularity [49]. For a detailed review of the literature on secure communications, we refer the reader to Unger et al. [41].

The smartphone era has seen an explosion of new communication tools, typically called “instant messaging applications” or “messengers.” In light of mass surveillance, several messengers have deployed end-to-end encryption to their users through a code update (e.g., iMessage, WhatsApp). Other messengers have been launched with security (in particular, end-to-end encryption) as an explicit selling point (e.g., Signal, Telegram). Usability has long been considered a key challenge for end-to-end encryption. The main user-related challenge for end-to-end encrypted communication tools is believed to be key management (i.e., key storage, distribution, and revocation), as prior user studies of secure communications (see Chapter 2) have shown and this thesis later shows (see Chapter 4). Nowadays, however, popular end-to-end encrypted messengers, such as iMessage, Telegram, and WhatsApp, relieve users of key management; they simply query a trusted server that vouches for the authentic public keys of all communication partners.

Recent revelations of mass state surveillance of personal communications have spurred demand for secure communication tools. However, the spurring demand for quickly delivering secure communication tools over the past few years has resulted in
a wide range of tools with varying security policies, threat models, a lack of perspective on the existing literature on secure communications, and dubious security claims [41,50].

Tools that are being developed offer a narrow set of security goals and protect against specific types of adversaries. Many tools are released with new designs that fail to draw upon the cryptographic academic literature, repeat well-known design mistakes, or use weak cryptography. Further, the creators of several communication tools mislead users by advertising their tools using grandiose terms (e.g., “secure,” “private,” “encrypted,” “military-grade encrypted”) or by promising impossible features (e.g., “supporting self-destructing messages,” “leaving no trace on servers”). Recently, the Electronic Frontier Foundation (EFF) has released a scorecard that evaluates the security offered by several communication tools [51], and has found several tools that are advertised as “secure” do not support, for example, end-to-end encryption.

It is worth to mention that the use of self-destructing messages was popularized by Snapchat, which was released in 2011. While popular with users who perceive 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 [52–54]. Other tools that appear to provide certain security properties fail to provide these properties in the face of government requests [55].

In this thesis, we focus on one type of secure communications: end-to-end encrypted communications, where only the communication partners (i.e., the sender and the recipient(s)) can access data exchanged from one end system (e.g., a mobile device) to another. That is, end-to-end encryption prevents unauthorized entities or third parties, such as eavesdroppers, Internet service providers, application service providers, and intelligence agencies, from reading, listening to, or tampering with exchanged end-to-end encrypted data, including text messages, photos, voice notes/messages, videos, and phone calls.

In most messaging systems or communication tools, including email systems and instant messaging tools, exchanged communications pass through intermediaries before they are received by the recipient(s). They are also sometimes stored by a third party, such as the application service provider (e.g., Snapchat), allowing the third party to, for
example, search for specific content or provide search features. Without end-to-end encryption, a third party can secretly read or alter data exchanged between the sender and the recipient(s).

In end-to-end encrypted communication tools, the sender (the author of a message) encrypts outgoing data, and the recipient receives and decrypts end-to-end encrypted data. That is, even if end-to-end encrypted data passes through and is stored by third parties, only the recipient(s) has/have the means to decrypt the data.

In the context of one-to-one communications (the type of communications we focus on in this thesis) where we have one sender (e.g., Alice) and one recipient (e.g., Bob), Alice and Bob generate their own public/private key pair and store their pair locally on their device (e.g., mobile phone). The participating devices then use – most of the times – Diffie-Hellman key exchange [56] to exchange a long-term encryption key, which will only be known to Alice and Bob. After an end-to-end encrypted session has been established, communicating devices use this key to exchange end-to-end encrypted data. In some other implementations of end-to-end encryption protocols, Diffie-Hellman key exchange is not used and, instead, the public/private key pairs of Alice and Bob are used to exchange end-to-end encrypted data, such that Alice uses Bob’s public key (her private key) to encrypt (digitally-sign) her messages, and Bob uses his private key (Alice’s public key) to decrypt (verify) the messages he received from Alice. To ensure that a man-in-the-middle attack, where a third party impersonates one of the communication partners, does not occur, Alice and Bob exchange their public keys (or a hash of each one’s public key) over a secure channel (e.g., in-person using verification fingerprints).

Finally, the ends in “end-to-end encryption” refer to the sender’s device and the recipient’s device, where the public/private key pair of each communication partner is stored locally on their device. This means, end-to-end encrypted communications are secure as long as (1) the sender and recipient’s devices are not compromised (e.g., by exploiting a vulnerability on their devices) and, hence, keys are not leaked or tampered with, and (2) a backdoor has not been inserted – by, for example, the application service provider or the government – into the application software that provides end-to-end encryption.
Summary. In this thesis, we conduct the first largest (n=60 participants) and broad-est qualitative user study of secure communications, to explore the obstacles to the widespread adoption of secure tools (see Chapter 3). We then focus on evaluating the end-user experience and improving the design of end-to-end encrypted communication tools. First, we assess the usability of two PGP email encryption tools, Enigmail and Mailvelope (see Chapter 4). Second, we investigate the factors that influence the adoption of an instant messaging tool, Telegram, that is usable, secure (mainly, end-to-end encrypted), and perceived by most of its users as such (see Chapter 5). Third, we explore user mental models of a hypothetical end-to-end encrypted communication tool, Soteria (see Chapter 6). Fourth, we employ participatory design and propose data-driven guidelines to help design better user-centered descriptions that effectively communicate the security properties of end-to-end encrypted communications (see Chapter 7).

2.2 User Studies of Secure Communications

Poor usability has traditionally been shown to hamper the adoption of secure communication tools, as well as the actual level of security in real-world use. In their seminal paper [5], Whitten and Tygar argued that although user errors cause or contribute to most computer security failures, ineffective security is “inescapably a user interface design problem.” To test their hypothesis, they designed and conducted a user study to assess whether PGP 5.0 could be effectively used by non-specialist users to secure their email. They aimed to answer the following two research questions: “Why is there such a lack of good user interface design for security?” “Are existing general user interface design principles adequate for security?”

First, Whitten and Tygar offered a specific definition of usable security. “Security software is usable if the people who are expected to use it (1) are reliably made aware of the security tasks they need to perform, (2) are able to figure out how to successfully perform those tasks, (3) do not make dangerous errors, and (4) are sufficiently comfortable with the interface to continue using it.” Second, they employed two evaluation methods: (1) a hybrid analytical approach combining cognitive walkthrough [57] and heuristic
evaluation [58] to inspect the user interface of PGP and identify any issues with its user interface design; (2) a laboratory-based user study (n=12). In the user study, Whitten and Tygar gave participants a test scenario, and avoided interfering with participants’ attempts to carry out the security tasks. The scenario was as follows: each participant had volunteered to help with a political campaign, and had been given the job of a campaign coordinator (the party affiliation and campaign issues were left to each participant’s imagination, in order not to offend participants). The task of each participant was to send out plan updates to other members of the campaign team by email, using PGP for privacy and authentication. Because volunteering for a political campaign presumably implies a personal investment in the campaign’s success, Whitten and Tygar hoped that participants would be motivated enough to use PGP to protect the secrecy of their exchanged messages.

The user study was run with 12 participants, all of whom were experienced users of email, and none of whom was able to describe the difference between public and private key cryptography prior to the study sessions. Participant ages ranged between 20 and 49. All participants had attended at least some college, and some had graduate degrees. Participant professions were also diverse, including graphic artists, programmers, administrators, a medical student, and a writer.

Whitten and Tygar identified several security-related problems in the user interface of PGP 5.0 (e.g., irreversible errors, lack of consistency and feedback, use of technical jargon). They also found that only one-third of participants were able to correctly encrypt and sign their email messages using PGP during a 90-minute session. They concluded that making security usable required the development of domain-specific user interface design principles and techniques. They also argued that in order to effectively and quickly communicate a valid conceptual/mental model of an email encryption tool (like PGP), the computer security and privacy community should work on crafting visual metaphors (i.e., graphical descriptions) of public and private keys, as well as digital signatures, to help users, especially novices or first-time users, correctly encrypt/decrypt and digitally-sign their email.
Using a similar study to [5], Garfinkel and Miller studied CoPilot, an email prototype based on key continuity management (KCM) [7]. KCM attempts to make secure email usable (through reducing user effort and potential for error) by automating key generation, key management, and message signing. CoPilot has a unique user interface; it color-codes messages depending on whether they were signed, and whether the signer was previously known or unknown (e.g., if CoPilot receives an unsigned message from an email address for which it usually receives signed messages, the unsigned message is displayed with a gray border).

To test whether or not CoPilot can improve the effectiveness of email security, Garfinkel and Miller designed and conducted the first user study of “KCM-secured email.” They recruited 43 “crypto-naive” participants who were between 18 and 63 years old, and used a similar scenario to the one given to participants in Whitten and Tygar’s “Why Johnny Can’t Encrypt” user study. They found that KCM is a workable model for improving email security, and that the user interface of CoPilot enables users to send protected email messages easily because, for example, it visually distinguishes encrypted emails from unencrypted ones. However, CoPilot does not help users handle the circumstances when a new email address is simultaneously presented with a new digital certificate. Garfinkel and Miller concluded that work is needed to develop more effective user interface designs.

Ruoti et al. designed and conducted a user study to evaluate the user experience of two mail systems: private webmail (Pwm) and message protector (MP) [59]. Pwm is a browser extension that integrates with existing webmail services, and supports automatic key management and encryption, making security more transparent (e.g., users of Pwm are not exposed to the ciphertext). Pwm was designed to maximize usability so that users would be willing to adopt and continue using it. In contrast, MP is a standalone encryption software that supports manual encryption, and users are exposed to the ciphertext. Ruoti et al. aimed to answer two research questions: “How usable is Pwm’s tight integration with existing webmail systems using security overlays and its transparent encryption?;” “Would manual encryption in an application separate from the browser prevent users from mistakenly sending out sensitive information without encryption, compete with Pwm in
2.2. User Studies of Secure Communications

terms of usability, and reveal enough security details that users would have greater trust in the system?”

To answer these questions, Ruoti et al. conducted a user study, where they recruited a total of 113 participants (all were students): 57 students for assessing the usability of Pwm and 56 students for evaluating the usability of MP. They found that participants trusted MP more than Pwm because with MP participants could see the ciphertext after encryption had taken place, equating this with protection. Further, many participants who used MP avoided making the mistake of sending out sensitive messages unencrypted. However, most participants preferred that secure email systems be tightly integrated with the browser, like Pwm. Thus, in the effort to “balance usability and security,” Ruoti et al. argued that a combination of exposing some encryption details and tight integration would produce an email system that (1) users trust and (2) helps users secure their messages without making mistakes.

More recently, Ruoti et al. conducted a laboratory-based user study with pairs of novices (n=25 pairs of participants) [60]. They asked participants to send encrypted email messages using a range of email tools (Pwm, Tutanota, and Virtru). Each of these email tools represents a different philosophy related to the integration of secure/encrypted email with existing email systems. Pwm integrates secure email with users’ existing Gmail accounts, allowing them to compose and receive secure email with a familiar user interface. In contrast, Tutanota is a secure email depot that requires users to log into Tutanota’s website to interact with their secure messages. Virtru is a hybrid of these two approaches, allowing users who install the Virtru plugin to use secure email that is integrated with Gmail but also allowing non-Virtru users to receive encrypted email through a depot-based system on Virtru’s website.

All recruited participants were university students, who were between 18 and 34 years old. One-third were male, and two-thirds female. They were all users of Gmail. Ruoti et al. found that participants’ trust in an email tool was reduced when security properties were hidden from users. Further, participants preferred integrated over standalone email encryption solutions. Ruoti et al. concluded that integrated solutions improve the
usability of secure email, but complete transparency (i.e., hiding security properties) is counterproductive.

Bai et al. investigated whether non-expert users can evaluate the security trade-offs between a traditional key-exchange model (analogous to PGP) and a registration model (analogous to iMessage) [61]. They gave participants (n=52) a high-level explanation of the security properties of each model, and asked them to complete a set of encryption tasks using both models.

Of the 52 participants, 60% were male, and 80% were between 18 and 34 years old. Almost 85% of participants reported “primarily” growing up in the United States, South Asia, or East Asia. 40% of participants reported jobs or majors in computing, mathematics, or engineering (many participants had a strong technical background). Bai et al. found that although participants recognized the benefits of the key-exchange model for “very sensitive communications,” participants preferred the more usable, but less secure, registration model for “everyday communications.” They concluded that the computer security and privacy community “should encourage the adoption of usable, but imperfectly secure, [encryption] tools for the many scenarios where it may be appropriate.”

Unlike the above-mentioned work that has mainly focused on evaluating the usability of encryption tools, Gaw et al. explored the social context behind users’ decisions about whether and when to encrypt their email [62]. They interviewed members of an activist organization (n=9) under the presumption that the organization’s employees would have a strong incentive to encrypt their email because “their mission required secrecy.” Gaw et al. aimed to answer the following research questions: Is understanding social factors necessary to designing encryption technologies that can be more widely-adopted and, if so, why? Do people perceive the users of email encryption technologies as paranoid?

Gaw et al. found that users’ decisions about encryption are driven not just by technical issues, but also by social factors. They found that participants’ perceptions (e.g., only “paranoid people” or “people up to no good” used email encryption) influenced participants’ decisions to use encryption.
2.2. User Studies of Secure Communications

Das et al. conducted a user study to investigate the role of social influence on users’ decisions to adopt new secure tools [63–65]. They asked participants to share their experience with mobile application installation and uninstallation. Similarly, De Luca et al. explored how and why users choose to use mobile instant messaging applications that are advertised as secure [66]. They surveyed 1,510 respondents from the UK, USA, and Germany, and then interviewed a balanced sample of 31 IT security experts (from several European countries) and non-experts (from Germany). In both studies, it was found that peer/social influence, not security and privacy, primarily drives users to adopt a messenger. The objective of this thesis 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 secure.

In [67], Renaud et al. conducted a user study with non-expert students and staff members, as well as computer science students to explore the barriers to the adoption of end-to-end encrypted email. They found that, in addition to poor usability, incomplete threat models, misaligned incentives, and lack of understanding of email architecture are key barriers to adopting encrypted email. They concluded that computer security and privacy researchers should focus on building “comprehensive mental models of email security.”

Other studies (e.g., [8, 9, 68–70]) have considered PGP further as well as contact verification in OTR [44], secure communications in two-way radios [71], opportunistic email encryption [6], and public-key fingerprints [72, 73]. Furthermore, several studies have explored users’ perceptions of email signatures [74], browser security indicators (e.g., [75]), and specific features of specific security tools (e.g., self-destructing messages in Snapchat [76]).

Finally, 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 [77]) in 2004 [78]. Similarly, we use a qualitative approach to understand how users manage their communications, secure or not, as an “everyday, practical
problem” (see Chapter 3). 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.

Summary. Most user studies of secure communication tools – in particular, email encryption tools, have been laboratory-based user studies (similar to the Whitten and Tygar study [5]) that followed the same pattern: assessing the usability (mainly, ease of learnability and ease of use) of specific tools in an artificial setting, where participants are given a series of security tasks associated with those tools (e.g., generating/sharing/managing cryptographic keys, encrypting a message) with fictional communication partners (study coordinators) to accomplish a particular security goal (e.g., confidentiality or secrecy of message content) without errors. Success, or failure, is then measured based on the tasks and goals imposed on participants.

Further, the vast majority of these studies have cited Whitten and Tygar’s definition of usability for security software (see definition above). Whitten and Tygar claimed that most security failures are due to user interface design flaws. We agree that specific usability standards for user interface design are needed to achieve effective security. However, before doing so, the underlying design must match users’ needs and goals: users’ ability to reach all their communication partners using the same tool in a timely-manner. Thus, utility is key. Utility is an attribute that refers to the design’s functionality, and whether the system does what the user requires [79]. In contrast, usability is the extent to which a computer security system can be used by specified users to achieve specified goals in a specified context of use with learnability, effectiveness, efficiency, memorability, absence of errors, satisfaction, and safety. Clearly, Whitten and Tygar’s definition does not touch upon the utility an effective secure communication tool must provide. In Chapter 5, we show how lack of utility negatively affects the use of a usable and secure communication tool.

Further, we argue that a secure communication tool that is usable, offers the utility users need, and is widely-adopted can be incorrectly or inappropriately used. Most users do not know what it means for a usable and secure tool that is popular and offers
utility (e.g., WhatsApp) to be end-to-end encrypted. Incorrect mental models of encryption lead people to use less secure channels that they incorrectly perceive as more secure than end-to-end encrypted tools (see Chapter 6). Whitten and Tygar argued that crafting visual metaphors of public and private keys is necessary to help users – especially, first-time users – form accurate mental models of how an email encryption tool works and, hence, use it correctly. However, Demjaha et al. found that metaphors did not help survey respondents understand the difference between public and private keys [80]. We also argue that a user-centered approach to designing secure communication tools is necessary. Hence, we employ participatory design (see Chapter 7) and ask participants to critique existing descriptions of end-to-end encryption and then design new ones. We found that participants were more interested in understanding the actual protection (or security properties) of encrypted communications, and not how they worked. None of the participants suggested a visual metaphor of public/private keys or how encrypting a message works. Drawing from the findings of our study, we propose data-driven guidelines that would help designers develop descriptions that effectively communicate the security properties of end-to-end encrypted communications.

Finally, we would like to note that the threat model of secure messaging differs from one tool to another and, hence, we, in this thesis, investigate the threat model of secure messaging based on how mainstream users define it (see Chapter 3).

2.3 Private Browsing Mode

Private browsing is a privacy-enhancing technology that allows the user to browse the Internet without locally saving information (e.g., browsing history, cookies, temporary files) about the websites they visited in private mode [2]. Nowadays, all major web browsers support private browsing. Different browsers refer to it using different names. For example, private browsing is known as Incognito Browsing in Google Chrome, InPrivate Browsing in Microsoft Edge and Microsoft Explorer, and Private Browsing in Brave, Firefox, Opera, and Safari. Further, Brave distinguishes between a Private Tab and a Pri-
Private browsing goals. The primary security goal of private browsing is that a local attacker – such as a family member, a friend, or a work colleague – who takes control of the user’s machine after the user exits a private browsing session should find no evidence of the websites the user visited in that session [2]. That is, a local attacker who has (physical or remote) access to the user’s machine at time $T$ should learn nothing about the user’s private browsing activities prior to time $T$. Therefore, private browsing does not protect against a local attacker who controls the user’s machine before or during a private browsing session; a motivated attacker (e.g., a suspicious wife) can install a key-logger or a spyware and monitor the user’s (e.g., husband’s) private browsing activities.

Further, private browsing does not aim to protect against a web attacker who, unlike a local attacker, does not control the user’s machine but controls the websites visited by the user in private mode [2]. Even if the user is not authenticated to an online service, a website can uniquely identify them through their client’s IP address. Also, the user’s various browser features – such as screen resolution, timezone, and installed extensions – can easily enable browser fingerprinting [2] and, hence, website tracking.

Additionally, private browsing does not aim to hide the user’s private browsing activities from their browser vendor, Internet service provider (ISP), employer, or government.

To achieve the primary security goal of private browsing, once a user terminates a private browsing session, most web browsers claim to delete the user’s private browsing history, cookies, information entered in forms (e.g., login data, search items), and temporary files from the user’s local device. Further, some browsers do not locally store the bookmarks created and files downloaded in a private browsing session. Table 2.1 summarizes the functionality of private mode in seven browsers.

Private browsing implementations. While all major web browsers have a private mode, each browser’s implementation of private browsing is different [2]. Further, most browsers update their implementation based on user demand. For example, some browsers have recently added privacy features to help reduce website tracking (although
2.3. Private Browsing Mode

<table>
<thead>
<tr>
<th></th>
<th>Brave 0.55</th>
<th>Firefox 62.0.3</th>
<th>Google Chrome 69.0.3497.100</th>
<th>Internet Explorer 11</th>
<th>Microsoft Edge 44.17763.1.0</th>
<th>Opera 56.0.3051.36</th>
<th>Safari 12.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browsing history</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cookies</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Login data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Search items</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Bookmarks</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Downloads</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 2.1: Private browsing functionality in recent web browser versions. A checkmark indicates an item is locally deleted once a user exits private mode, whereas a crossmark indicates an item is locally saved.

The table is not fully comprehensive; other items not shown include: browser cache, temporary files, HTML local storage, form auto-completion, client certificates, browser patches, phishing block list, and per-site zoom level. There has been no recent analysis of private browsing since the 2010 work of Aggarwal et al. [2]. The table was created based on the analysis conducted by the thesis author.

Although these attacks are crucial to consider in order to achieve overall browser security, they are not the focus of our work. In this thesis (see Chapter 8), we evaluate the end-user experience of private mode.
2.4 User Studies of Private Browsing Mode

Prior work has quantitatively (mainly through survey studies) investigated whether users are aware of private browsing, what they use it for, and whether they understand what protection it provides. In [20], Gao et al. conducted a survey of 200 Mechanical Turk (MTurk) respondents in the US, examining their private browsing habits. They found that one-third of respondents were not aware of private browsing. Those who had used private browsing reported using it for protecting personal information, online shopping, or visiting “embarrassing websites.” Further, most respondents had misconceptions about private browsing – such as incorrectly believing that private mode protects from visited websites. Gao et al. concluded that browsers do not effectively inform users of the benefits and limitations of private browsing, and that “browser designers [should think of] various ways to [better] inform users.”

In 2017, DuckDuckGo, an Internet search engine, surveyed a sample of 5,710 US respondents, recruited via SurveyMonkey [21]. Respondents were asked to share their experience with private browsing. Again, one-third of respondents reported they had not heard of private browsing. Of those who had used private browsing, one-third used it frequently, and three-quarters were not able to accurately identify the benefits of private browsing. The report did not offer any recommendations beyond the study.

Using a similar study to [21], Bursztein ran an online survey of 200 US respondents (via Google Consumer Surveys) in 2017 [22]. He found about one-third of surveyed respondents did not know about private browsing. Of those who were aware of the technology, only 20% had used it. Further, about one-half preferred not to disclose what they used private browsing for. Additionally, only 40% claimed they used private browsing for its intended purpose: leaving no traces of the websites visited in private mode on the local machine. Bursztein concluded that the computer security and privacy community should raise awareness of what private browsing can and cannot achieve. He also mentioned that “surveys are clearly not the best approach to understand why people are using the private browsing mode because of the embarrassment factor.”
2.4. User Studies of Private Browsing Mode

Recently, Wu et al. surveyed 460 US respondents through MTurk [23]. Respondents were randomly assigned one of 13 different browser disclosures related to private mode. Based on the disclosure they saw, respondents were asked to answer a set of questions to assess their understanding of private mode. Wu et al. found that existing browser disclosures do not sufficiently inform users of the benefits and limitations of private mode. They concluded that browser disclosures should be redesigned to better convey the actual protections of private browsing. They also argued that the term “private browsing” could be misleading. In this work, we explore how users’ conceptual understanding of the terms “private browsing,” “private window,” “private tab,” and “private session” influences their understanding and usage of private mode in real life.

Habib et al. conducted a user study to observe the private browsing habits of over 450 US participants using software monitoring [24]. They then asked participants to answer a follow-up survey (using MTurk) to investigate discrepancies, if any, between observed and self-reported private browsing habits. They found that participants used private mode for online shopping and visiting adult websites. The primary use cases of private mode were consistent across observed and self-reported data. They also found that most participants overestimated the benefits of private mode, concluding by supporting “changes to private browsing disclosures.”

Finally, it is worth to mention that Aggarwal et al. [2] and Mozilla, Inc. [19] conducted two quantitative user studies using software monitoring to observe people’s private browsing habits in 2010. We explain the studies in detail in Tables 2.2 and 2.3. However, the authors did not provide any recommendations beyond the studies.

Summary. Prior work has employed quantitative methods – mainly through conducting surveys – to investigate whether users are aware of private browsing, what they use it for, and whether they understand what protection it provides (see Tables 2.2 and 2.3). However, prior work has not investigated why users misunderstand the benefits and limitations of private browsing. Further, most recruited participants in prior user studies either were unaware of or had not used private mode. In this work, we address these research gaps by designing and conducting a three-part user study: (1) the first usability inspection of pri-
private mode in different web browsers, (2) the first qualitative, interview-based user study, and (3) the first participatory design study. We also recruit both users and non-users of private mode.

2.5 Mental Models

Users make computer security- and privacy-related decisions on a regular basis. These decisions are guided by users’ mental models of computer security and privacy. A mental model is someone’s understanding or representation of how something works [89]. People cannot keep all the complex details of how something works in their brain and, hence, they develop and use their models to simplify complex concepts, consider some details more relevant than other, and make decisions. Different people have different models of the world surrounding them based on the information they receive from their family members, friends, colleagues, or media outlets.

In their seminal paper, Saltzer and Schroeder provided eight principles that guide the design and implementation of computer security (or protection) mechanisms [90]. One of these principles is psychological acceptability: if there is a mismatch between a user’s mental image of a protection mechanism and how the mechanism works in the real world, the user will be unable to use the mechanism correctly. Wash and Rader proposed a new way to improve user security behaviour: instead of trying to teach non-technical users “correct” mental models, we should explore their existing models [91]. Wash conducted a qualitative study to investigate users’ mental models of home computer security [92]. He identified eight “folk models” of security threats that are applied by home computer users to make security-related decisions. Zeng et al. qualitatively studied users’ security and privacy concerns with smart homes [93]. They found gaps in threat models, arising from limited technical understanding of smart homes.

Kang et al. undertook a qualitative study to explore users’ mental models of the Internet [18]. Oates et al. studied users’ mental models of privacy, asking end-users, privacy experts, and children to draw their models [94]. Through the use of interviews and surveys, Renaud et al. investigated users’ mental models of encrypted email, and found that,
in addition to poor usability, incomplete threat models, misaligned incentives, and lack of understanding of how email works are key barriers to adopting encrypted email [67]. Wu and Zappala conducted a qualitative user study to investigate users’ perceptions of encryption and its role in their life [95]. They identified four users’ mental models of encryption that varied in complexity and detail. Krombholz et al. qualitatively explored end-users and system administrators’ mental models of HTTPS, revealing a wide range of misconceptions [96]. Gallagher et al. qualitatively studied experts and non-experts’ perceptions and usage of the Tor anonymity network, identifying gaps in understanding the underlying operation of Tor [97].

Summary. Prior work has explored user mental models of different computer security and privacy concepts and tools. In this thesis, we qualitatively and quantitatively explore user mental models of secure communication tools (see Chapter 6). We also qualitatively investigate user mental models of private browsing and its security goals (see Chapter 8). We give participants the option to draw their models.

2.6 Security and Privacy Design

Within web browsers, prior work has investigated the design of alert messages and warnings [98–105], browser security indicators [75, 106, 107], site trustworthiness [108, 109], privacy policies [110, 111], storage policies [112], and ad personalization [113].

However, prior work has heavily focused on the design of warning messages – especially phishing warnings [98, 99, 102, 103] and SSL warnings [100, 101, 103–105] – in order to capture users’ attention, improve their comprehension, and warn them away from danger. For example, Egelman et al. recommended that phishing warning messages should be active (i.e., interrupt the user flow) and should be distinguishable by severity [99]. They also suggested it should be difficult for users to click-through phishing warnings, by requiring users to bypass several screens in an attempt to dissuade users from ignoring warnings. Additionally, Egelman and Schechter showed that changes to the look and feel of phishing warnings have resulted in more users noticing them [102]. Felt et al. recommended warning designers use opinionated design to improve user ad-
herence to warnings [105].

Further, several researchers have focused on reducing user habituation to security warnings [114–116]. Brustoloni and Villamarin-Salomon suggested the use of polymorphic and audited dialogues [117]. Bravo-Lillo et al. explored the use of attractors [118]. Anderson et al. varied size, colour, and option order [119].

Summary. The aforementioned work has mainly focused on the design of browser warning messages to improve their efficacy. However, our thesis focuses on designing (1) end-to-end encryption descriptions and (2) browser disclosures related to private browsing, to sufficiently inform users of the benefits and limitations of two privacy-enhancing technologies: encrypted communication tools and private browsing mode. Although we draw inspiration from this prior work, we answer a different important question of how to design descriptions and disclosures to help people appropriately use a privacy technology. We do so by employing participatory design [120], asking participants to critique encryption descriptions and browser disclosures, and then design new ones. Unlike warning designers who have explored different ideas – such as changing the design of a warning message or using attractors – to improve user attention to and comprehension of warnings, we choose, in this thesis, to engage users in the design of encryption descriptions and browser disclosures.
<table>
<thead>
<tr>
<th>Study</th>
<th>Research Questions</th>
<th>Methodology</th>
<th>Key Findings</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 An Analysis of Private Browsing Modes in Modern Browsers (USENIX Security, 2010)</td>
<td>- Are people aware of private browsing?</td>
<td>A measurement study</td>
<td>Participants often used private browsing to visit adult websites, and not online shopping or news websites.</td>
<td>No recommendations were provided</td>
</tr>
<tr>
<td></td>
<td>- How often do people use private browsing?</td>
<td></td>
<td>iE X and Safari 4.0 had high rates of private browsing usage, compared to Firefox 4 and Internet Explorer 8.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Do users of a specific web browser use private mode more frequently than, or less frequently than, users of another web browser?</td>
<td></td>
<td>Aggarwal et al. performed three measurement studies: Google Chrome, Internet Explorer, and Safari on three different types of websites: adult, online shopping, and news.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- What do people use private browsing for?</td>
<td></td>
<td>The measurement software detected if a website was visited in public or private mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Participants likely browsed in private mode during lunchtime (between 11:00 am and 2:00 pm) and after they had returned from school or work (around 5:00 pm).</td>
<td></td>
<td>Participants usually stayed in a private browsing session for about 10 minutes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Test Pilot was developed as an opt-in service for Firefox Beta users.</td>
<td></td>
<td>The study did not indicate the number of Beta users who opted-in.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- At what time of the day do people browse in private mode?</td>
<td></td>
<td>The name “private browsing” should be rethought.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- How long do people stay in a private browsing session?</td>
<td></td>
<td>Browser disclosures related to private browsing should be redesigned to better inform users of the benefits and limitations of private browsing.</td>
<td></td>
</tr>
<tr>
<td>2 Understanding Private Browsing (a study by Mozilla, 2010)</td>
<td>- Are people aware of private browsing?</td>
<td>A survey (quantitative)</td>
<td>Respondents who had used private browsing incorrectly believed that private mode hid their private browsing activities from visited websites.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Participants likely browsed in private mode during lunchtime (between 11:00 am and 2:00 pm) and after they had returned from school or work (around 5:00 pm).</td>
<td></td>
<td>Participants usually stayed in a private browsing session for about 10 minutes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Mozilla conducted a test pilot study in missile time (Firefox 3.5 users activated private browsing, as well as the time they deactivated it).</td>
<td></td>
<td>The duration of a private browsing session did not considerably fluctuate throughout the day.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Test Pilot was developed as an opt-in service for Firefox Beta users.</td>
<td></td>
<td>The study did not indicate the number of Beta users who opted-in.</td>
<td></td>
</tr>
<tr>
<td>3 Private Browsing: An Inquiry on Usability and Privacy Protection (WPES, 2014)</td>
<td>- Are people aware of private browsing?</td>
<td>A survey (quantitative)</td>
<td>About one-third of respondents were not aware of private browsing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- At what time of the day do people browse in private mode?</td>
<td></td>
<td>Respondents who had used private browsing incorrectly believed that private mode hid their private browsing activities from visited websites.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- How do people perceive the benefits and drawbacks of private browsing?</td>
<td></td>
<td>Participants who had used private browsing incorrectly believed that private mode hid their private browsing activities from visited websites.</td>
<td></td>
</tr>
<tr>
<td>4 A Study on Private Browsing: Consumer Usage, Knowledge, and Thoughts (a study by DuckDuckGo, 2017)</td>
<td>- Are people aware of private browsing?</td>
<td>A survey (quantitative)</td>
<td>About one-half of respondents had heard of private browsing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- About one-third of respondents were not aware of private browsing.</td>
<td></td>
<td>Respondents used private browsing on both desktop and mobile phone.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- How do people use private browsing?</td>
<td></td>
<td>Most respondents used private browsing to visit “embarrassing websites.”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- How do people use private browsing?</td>
<td></td>
<td>About one-third of respondents were not able to correctly identify the benefits and limitations of private browsing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Are people aware of private browsing?</td>
<td></td>
<td>Further research is needed to understand the benefits of private browsing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Participants incorrectly thought that private browsing prevented social websites from tracking them, as well as search engines from knowing their searches.</td>
<td></td>
<td>Some respondents incorrectly thought that private browsing prevented social websites from tracking them, as well as search engines from knowing their searches.</td>
<td></td>
</tr>
</tbody>
</table>

Table 2.2: A detailed overview of user studies of private browsing mode (part 1 out of 2).
### Table 2.3: A detailed overview of user studies of private browsing mode (part 2 out of 2)

<table>
<thead>
<tr>
<th>Study Type</th>
<th>Study Title</th>
<th>Methodology</th>
<th>Key Findings</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>A survey (quantitative)</td>
<td>Wu et al. 2018</td>
<td>A survey (via MTurk)</td>
<td>- Only 4% of SBO participants used private browsing.</td>
<td>- Browser disclosures should be redesigned to better communicate the actual protections of private browsing.</td>
</tr>
<tr>
<td>A survey (quantitative)</td>
<td>Bursztein et al. 2017</td>
<td>A survey (via Google Consumer Surveys)</td>
<td>- Respondents reported using private browsing to hide their online activity.</td>
<td>- Design better and more effective browser disclosures.</td>
</tr>
<tr>
<td>A survey (quantitative)</td>
<td>Habib et al. 2018</td>
<td>A survey of 460 US participants</td>
<td>- Almost all participants did not understand the primary security goal of private browsing.</td>
<td>- Design new browser disclosures.</td>
</tr>
<tr>
<td>A survey (quantitative)</td>
<td>Your Secrets Are Safe: How Browsers' Explanations Impact Privacy (SOUPS, 2018)</td>
<td>A survey of 460 US respondents</td>
<td>- The Google Chrome desktop disclosure led respondents to answer more questions correctly. However, only one-fifth reported using private browsing.</td>
<td>- Browser disclosures should be redesigned to better enable users to make informed decisions.</td>
</tr>
</tbody>
</table>

These studies highlight the need for improved browser disclosures to communicate the actual protections of private browsing.
Chapter 3

Why Do People Give Up on Secure Communication Tools? An Explanatory Study with Lapsed Users of Secure Tools

In light of recent revelations of mass state surveillance of phone and Internet communications, the computer security and privacy community has advocated the widespread adoption of secure communication tools. Several popular communication tools (e.g., iMessage, WhatsApp) 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.

Prior user studies of secure communication tools have shown that poor usability (mainly due to user interface design flaws) is the primary obstacle to the adoption of secure tools. In this chapter, we expand on this finding and investigate the factors that influence users’ decision to adopt, or not adopt, a communication tool, as well as their perceptions of secure communications. We design and conduct the largest (n=60) and broadest qualitative user study of secure communications to date. Unlike prior work, we
find that poor usability is not the only primary class of obstacles to adopting secure tools. Lack of utility (due to the tool’s small userbase, lack of interoperability, or low quality of service) and incorrect user mental models of secure communications are two other primary classes of obstacles to adoption.

The rest of this chapter is structured as follows:

- Section 3.1 describes the research objectives of this study.
- Section 3.2 describes our qualitative user study design.
- Section 3.3 presents the findings of our study.
- Section 3.4 discusses the findings of our study and shows why the computer security and privacy community should prioritize securing communication tools that have already been adopted by mainstream users over improving the usability of different secure tools that have a small userbase.
- Section 3.5 summarizes the chapter and concludes with three concrete recommendations for increasing the adoption of secure communication tools.
- Section 3.6 describes the principal limitations of the study.
- Section 3.7 describes the contributions this chapter makes to the thesis.

The content of this chapter is an edited version of the following publications:

3.1 Introduction

Nowadays, the majority of web traffic between clients and servers is encrypted via TLS (Transport Layer Security). However, the majority of communications between users are not end-to-end encrypted [41, 51]. This means that whenever plaintext is processed or stored by remote servers, users are vulnerable to mass surveillance [55] or hackers. Their personal data is also subject to commercial analysis by service providers for advertising and enhanced personalization [121]. As a result, the computer security and privacy community has long advocated the widespread adoption and increased use of end-to-end encrypted communication tools.

Usability has long been considered a key challenge for secure, especially end-to-end encrypted, communications. 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 [122, 123]. To attempt to address the usability challenge, there have been traditionally two approaches. One approach has been designing and conducting laboratory-based user studies (see Section 2.2 in Chapter 2), to examine why people fail to use an existing secure communication tool (e.g., PGP) correctly, often concluding that security failures arise due to user interface design flaws.

The other approach has been producing educational materials (e.g., [124–126]), to explain existing secure communication tools and security extensions (e.g., OpenPGP [36], Tor [127], Tails [128], SecureDrop [129]). These materials provide guidelines or step-by-step instructions to install and use these tools and extensions securely. However, docu-
mentation only helps the users who read it and are already motivated enough to adopt a new tool.

Secure communication tools became widely available with the release of PGP in 1991, which was followed by the creation of a large ecosystem of communication tools. The smartphone era has also seen an explosion of new communication tools (typically called messengers or instant messaging tools). Recent mobile phone-based communication tools have been often designed to hide security from the user completely (albeit at some security cost [41]). Some communication tools have adopted end-to-end encryption with only negligible changes to the user experience. For example, WhatsApp famously deployed end-to-end encryption to approximately one billion users in 2014 [130] (WhatsApp now has more than 1.5 billion monthly users [131]), through a code update to its application for messages, voice calls, and video communications. Some other communication tools, such as Signal and Telegram, have been launched with security as an explicit selling point, but they also nearly hide all cryptographic details from the user.

Many of these communication tools claim to be “secure” and are advertised as such. However, they often do not provide specific security guarantees and fail to draw upon the existing cryptographic literature [41]. Further, there are key differences in the security model of different secure, especially end-to-end encrypted, communication tools, in addition to a large gap in security compared to competitors (e.g., Google Hangouts, Skype) that do not offer end-to-end encryption. Yet, it is unclear if users understand what protection (or security properties) these different tools offer, and if they value that protection. This led the Electronic Frontier Foundation (EFF) to develop the Secure Messaging Scorecard in 2014 [51], to attempt to provide objective information to non-expert users about the security properties different communication tools actually offer. The scorecard provides a “consumer guide” to encourage mainstream users to adopt and use secure communication tools. The scorecard is a table (see Figure 3.1) that evaluates dozens of communication tools based on seven different criteria: “Encrypted in transit?;” “Encrypted so the provider can’t read it?” “Can you verify contacts’ identities?;” “Are past communications secure if your keys are stolen?;” “Is the code open to independent review?;” “Is security design properly documented?;” and “Has there been any recent code audit?”
3.1. Introduction

To this end, we argue that in order to design and build secure communication tools that effectively protect users, we need to follow a user-centered approach to secure communications, unlike the two traditional approaches: conducting laboratory-based user studies and producing educational materials. We first need to understand (1) what influences users’ decision to adopt, or not adopt, a particular tool and (2) how users perceive secure communications. Thus, we designed the largest \((n=60\) participants) user study of secure communications to date. We first conducted 10 in-person unstructured interviews – each interview lasted for 35 minutes on average. We then conducted 50 in-person semi-structured interviews – each interview lasted for 90 minutes on average.

Drawing from the findings of our study, we identified three main classes of obstacles to the adoption of secure communication tools:

- **Class 1: Poor usability is not the only primary obstacle to adoption.** Participants reported usability issues with different communication tools, but did not stop

---

**Figure 3.1:** The EFF Secure Messaging Scorecard.
using the tools only because of these issues.

- **Class 2: Lack of utility is a significant barrier to adoption.** Users’ inability to reach all their communication partners in a timely-manner using the same communication tool hinders the adoption of secure tools. For example, a tool that has a small userbase, is not interoperable, or has low quality of service (QoS) lacks utility:

  - **Small/fragmented userbases.** The common trend of creating new secure communication tools and then assessing the usability of these tools is a primary obstacle to adoption due to creating small and fragmented userbases.

  - **Lack of interoperability.** Users need to use communication tools that are interoperable; i.e., work across different devices/platforms. Secure tools that lack interoperability have low user adoption.

  - **Low QoS.** Participants assessed the reliability and security of a communication tool by the QoS of the messages and calls they experienced. Low QoS does not only hinder adoption, but also creates general doubts about how secure and reliable a tool is.

- **Class 3: Incorrect mental models of secure communications are a significant adoption barrier.** Users’ incorrect belief that secure communications are futile hampers the adoption of secure tools:

  - **Sensitivity of information and 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 and video chats (regardless of what tool they used), as well as obfuscation techniques (e.g., segmenting information and then sending different segments using different communication tools/channels) to send sensitive information.

  - **Futility of secure communications.** Most participants did not believe secure communication 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 hamper adoption.

- **Inaccurate security rankings of tools.** We asked our participants to rank the tools they had used in terms of how secure they were. Many participants ranked the services (e.g., text messages, voice calls) offered by the tools, rather than ranking the tools first. They perceived calls as more secure than messages. Furthermore, participants based their rankings on how large the tool’s userbase is, QoS, social factors and other criteria, rather than assessing the security properties a secure tool offers.

- **Misunderstanding the EFF Secure Messaging Scorecard.** The scorecard contains seven security mechanisms that achieve specific security properties. Four of these were misunderstood: participants did not appreciate the difference between point-to-point and end-to-end 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, with most participants believing security requires obscurity.

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

### 3.2 Methodology

In this section, we describe the research questions this study addresses, recruitment process, interview procedure, and details of our data analysis. The Research Ethics Board at UCL reviewed and approved our research study (project no.: 6517/002). We handled all data collected in accordance with the provisions of the UK Data Protection Act 1998 (registration no.: Z6364106/2015/08/61).
3.2.1 Research Questions

In this work, we address the following research questions:

- **RQ1**: Why, when, and how do people use secure communication tools (Section 3.2.3.1)?

- **RQ2**: What threats do users want to protect against when communicating (Section 3.2.3.2)?

- **RQ3**: What communication tools do users perceive to be secure (or insecure) and why (Section 3.2.3.3)?

- **RQ4**: How do users think secure communications can be achieved, and how they can be breached (Section 3.2.3.4)?

3.2.2 Recruitment

Our literature review (see Section 2.2 in Chapter 2) shows that mainstream users’ needs and practices with regards to 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 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 participants via posting flyers around UCL’s buildings and emailing university staff members. We also sent 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 Appendix A. 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 used and
the ones they stopped using. Additionally, we gave our participants the option to specify other tools they used (or had used in the past), but were not on the list.

We then divided the pool of eligible participants into sub-groups, based on a number of variables: age, gender, education level, study area, employment status, technical knowledge, and cyber-security threat exposure. We conducted and analyzed ten unstructured interviews first, followed by 50 semi-structured interviews. Table 3.1 in Section 3.3.1 summarizes the demographics of our participants for both the unstructured and semi-structured interview sessions.

We paid participants a reward of £10.

3.2.3 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 [132]. A single trained researcher (the thesis author) conducted all 60 interview sessions in the UK in English, by first conducting ten unstructured (open-ended) face-to-face interviews, which lasted for 35 minutes on average. The emerging themes shaped the design of the script used for the 50 semi-structured face-to-face interviews, which lasted 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. All interviews covered the following four areas in the same order. Below, we describe the script we used for the semi-structured interviews.

3.2.3.1 Adoption of Communication Tools

To answer RQ1 in Section 3.2.1, we asked participants to specify the communication tools they used (or had 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 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 are your communication partners?
- 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 so, why and how did you do so?
- Why did you decide to stop using [this communication tool], if applicable?

3.2.3.2 What Is a Secure Communication Tool?

“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 [41]. The link between users’ perceptions of secure communications and the actual security offered by different communication tools has not been investigated so far.
3.2. Methodology

To address this gap and answer RQ2 in Section 3.2.1, we asked our participants about the kind of protection (or security properties) a secure communication tool should provide, what they wanted to protect, with whom they communicated, who the attackers (or adversaries) could be, and what their capabilities were.

We also elicited participants’ mental models of how they thought secure communications worked. Mental models are cognitive representations of external reality that underpin people’s cognition, reasoning, decision-making and behavior [133]. We invited our participants to draw how a communication tool worked, and whether there was a distinction between calling someone and sending them a 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.

3.2.3.3 Security Ranking of Communication Tools

To answer RQ3 in Section 3.2.1, we asked our participants to rank the communication tools they used (had used) in terms of the security level each tool offered. We provided them with cards with the names and logos of the tools they (had) 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 [51], as well as to elicit the rationale behind their rankings.

We also aimed to assess the effectiveness of the EFF Scorecard in communicating which communication tool was 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 ten minutes to explore it, compare their rankings, and ask any clarification questions they had.

3.2.3.4 Security Properties and Mechanisms

To answer RQ4 in Section 3.2.1, we probed our participants’ understanding of how a security property could be achieved and how it could be violated. We also asked par-
ticipants about several specific security mechanisms: encryption, digital signatures, and cryptographic fingerprints. We aimed to check their broader understanding to see whether they could 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.

3.2.4 Pilot Study

We conducted a pilot study of five semi-structured interviews to check that the questions could be understood, and to identify any potential problems in the script (e.g., cost, time, adverse events) in advance, so that the methodology could be fine-tuned before conducting the main study. We used the common practice of convenience sampling [134], by selecting five colleagues for the pilot study. In addition to the five sessions, we asked six researchers to review the study.

3.2.5 Data Analysis

To develop depth in our exploratory research, we conducted multiple rounds of interviews, punctuated with periods of analysis and tentative conclusions [135]. In total, we conducted, transcribed (using an external transcription service), and analyzed all ten unstructured and 50 semi-structured interviews. We observed data saturation [136] between the 40th and 45th 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 (Anastasia Danilova, Alena Naiakshina, and thesis author) using Grounded Theory [77, 137], 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 [138]. A κ value above 0.75 is considered excellent agreement [139].
3.3 Results

We first describe the demographics of our participants in Section 3.3.1. We then present the key emerging and recurring themes we observed across our interviews in sections 3.3.2–3.3.9. 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 (although the main purpose of qualitative research is to explore a phenomenon in depth, and not to generate quantitative results).

3.3.1 Demographics

Table 3.1 (which can be found at the end of this chapter) summarizes the demographics of our sample. 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 75. Two participants did not have a formal educational qualification, seven completed high-school education, 30 had a college degree (e.g., B.A., B.Sc.), and 21 had a higher degree (e.g., M.A., M.Sc., Ph.D.). 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 computer security/privacy experts, so they did not necessarily represent mainstream users of communication tools.

3.3.2 Adoption Criteria of Communication Tools

We found nine main criteria influencing our participants’ decision to adopt a communication tool, namely (1) large userbases 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.

1. **Large userbases 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 explained, "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 userbases of current secure communication tools hinder adoption of these 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 than WhatsApp (see Section 3.3.8), they see the overhead of using two communication tools as not worth the better security offered by iMessage.

2. **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.

3. **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 3.3.7). Furthermore, 20 participants who perceive Telegram as more secure than WhatsApp (see Section 3.3.8) 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 end-to-end 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 chat 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). This is also caused by lack of utility (the secret mode does not support group conversations). We explore the end-user experience of Telegram in Chapter 5.

4. **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 3.3.8): 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 with regards to security.

5. **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.

6. **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).

7. **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).

8. **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.
9. **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. [63–65] 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).

### 3.3.3 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, in real life, many participants do not select a secure tool to do so. Instead, they use different practices and obfuscation techniques. In this section, we explain (1) how our participants perceive sensitive information, (2) which practices they use to send this information, and (3) the information’s level of sensitivity.

1. **Perceived sensitivity of 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.

2. **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 3.3.7 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 mentioned 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.

3. Sensitivity level. 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 under repressive regimes) can target a particular person and record their calls, as portrayed so memorably
3.3. Results

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 debated “we kill people based on meta-data” comment [140]. 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.

3.3.4 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”.

1. 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 messages or listen to voice calls. P5 mentioned that information exchanged via a communication tool should not be “re-routed to unintended recipients”.

2. Message integrity. No participant mentioned unprompted that a message should not be modified in transit (for several reasons discussed later in Section 3.3.5.2. 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.

3. “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 – some participants mentioned the provider’s server as a possible example of a secure place – where they cannot be compromised. Many participants used the term “hacking” in connection with this security property. Six participants (P15, P17, P32, P43, P49, and P56) 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 [141] and/or third-party anonymity [141] (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 highly important to our participants, referring to it as “reliable connection”. However, they regard it as a utility feature (see Section 3.3.2), not a security property.

### 3.3.5 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 3.3.5.1.
In Section 3.3.5.2, we explain how participants think the security properties of secure communication tools (discussed in Section 3.3.4) can be breached.

### 3.3.5.1 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.

1. **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.

2. **Application service providers.** 54 out of 60 participants think that all messages pass through the service provider that “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” (e.g., 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 some-
where, that the provider can access their data. Hence, “having my data anyway” means trying to protect it is pointless (P47).

3. 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.

3.3.5.2 Violating the Security of Communications

Below, we explain how participants believe the security properties of secure communication tools discussed in Section 3.3.4 – secrecy of message content, message integrity, and “no impersonation” – can be violated.

1. 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 3.3.5.1. P8 also reported that providers access log files
3.3. Results

to perform quality monitoring of the service and, 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 ciphertexts. 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 userbase, 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 later in Section 3.3.6.

2. Message integrity. As discussed in Section 3.3.4, 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 did not feel concerned 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 explained, “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 3.3.6.

3. **“No impersonation”**. All participants believe that as long as passwords are hard to guess or steal, authentication is achieved. Many participants also mentioned that passwords can be stolen by hacking, social engineering, or brute forcing.

According to many 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 a service, or having access to a company’s server where passwords are stored insecurely, (2) logging into the account on behalf of
the legitimate user, and then (3) reading messages from the victim’s chat history. 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. Of these, 25 believe as long as service providers store passwords encrypted on their servers, brute-forcing attacks cannot occur: “they [service providers] are immune to brute-forcing attacks because encryption is used to protect credentials” (P9). 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).

3.3.6 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 3.3.5. 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

---

1 We explore in detail user mental models of secure (in particular, end-to-end encrypted) communications in Chapter 6.
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 our participants’ mental models are somewhat “ego-centric”: they see themselves as the centre of their personal communication universe. 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).

**Encryption.** 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. We, hence, probed and asked what encryption is, why it is used, and how it works (including client-server/server-client and end-to-end 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: \texttt{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: \texttt{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 programming language, and only those who understand the language (e.g., computer scientists) 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 explanation.

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, according to them, designers who create encryption schemes know how to decrypt messages. P15 mentioned that “even the ultimate encryption can be broken, like the ENIGMA machine in WWII”.

Only P2, P4, and P5 distinguished between client-server/server-client encryption and end-to-end 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 end-to-end 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/server-client encryption with SSL, and described end-to-end 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 end-to-end 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, and 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.

All 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 a fingerprint – which is generated when a Secret Chat session is established – is either (1) the encryption key used by the sender and the recipient to secure messages in-transit or (2) the encrypted message itself.
3.3. Results

**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.

3.3.7 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 (calls and messages). 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 many communication tools (e.g., WhatsApp, Google Hangouts) offer both services.
Chapter 3. Why Do People Give Up on Secure Communication Tools?

**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 to be 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 [142].

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, such as “*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 a 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 screenshot of a message, not something attackers can do with a phone call. This finding suggests users have a rudimentary understanding of forward
3.3. Results

SMS is the most secure messaging service. We discussed above why users regard voice calls as more secure than messages. We here provide the rationale behind why SMS messages are perceived by participants 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 and, hence, they have the same level of security. Also, P17 and P24 mentioned that their Yahoo! email account has been hacked, which explains why Yahoo! Messenger is perceived as insecure – mainly because the Yahoo! email and Yahoo! Messenger are seen as one entity. We discuss this theme in more detail in Section 3.3.8.

Some participants (29 out of 60) believe that “professional” email services (e.g.,
Outlook which is P11’s university email) are more secure than “commercial” ones (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 3.3.6.

3.3.8 Security Ranking Criteria of Communication Tools

We here discuss the reasons for our participants’ rankings of the communication tools they have used, and 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 3.3.2, such as userbases, QoS, cost of use, registration method (telephone numbers vs. usernames), and 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).

1. Userbases. 20 participants believe that popular communication tools (e.g., Face-
book Messenger, WhatsApp) have large userbases 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.

2. 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.

3. 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 costs are high. 22 participants also said that tools with advertisements are insecure.

4. Registration method: 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.

5. 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.

6. Integration with SMS. Many participants believe that SMS is more secure than IM for several reasons previously discussed in Section 3.3.7. 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 sensitive information, such as banking details, via iMessage for this reason.

7. Attractive user interfaces. 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) user interface 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 Messenger and Ebuddy XMS as examples. This finding shows that a good user experience of one aspect of the tool increases trust in the competence and motivation of the developers.

8. Visible security. According to several participants, 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 on their phone. Hence, they prefer to have a stand-alone desktop application similar to a mobile phone application downloaded from, for example, the App Store. 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, thus, are perceived as more secure, despite this being technically incorrect [143, 144]. 30 participants also think that the probability of a mobile phone getting infected by a “virus” is lower than that of a PC because they have never experienced any issue with their phones, unlike PCs, and have never installed a mobile phone version of an anti-virus program.

9. 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.

10. Geopolitical context. The local laws and practices that a service provider is
3.3. Results

subject to influence perception. P12 believes Facebook Messenger is less secure than other tools because Facebook is US-based. She believes that US intelligence services, 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 [145].

11. Self-destructing messages. The Telegram Secret Chat mode offers self-destructing messages, also known as ephemeral messages, which are messages that get erased within minutes or seconds of consumption. This happens on both the sender and recipient’s devices. Messages can also get removed from the application’s servers. P15 and P43 believe Telegram’s Secret Chat mode deceives participants into thinking that messages are deleted from the recipient side, while they are stored on Telegram’s servers. They compare Telegram to Snapchat and believe both tools are insecure.

12. 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 (an Apple service) that can be exploited [146]. 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 [147].

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

1. 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
Chapter 3. Why Do People Give Up on Secure Communication Tools?

of security in privacy policies in response to developments.

2. **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.

3. **Past experiences.** P19 and P22 believe 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 both believe all tools are insecure.

4. **Security is not possible.** P8 believes “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 audits need to be confidential because the design of secure tools should not be published (see Section 3.3.5 on threat models).

### 3.3.9 EFF Secure Messaging Scorecard

We provided our participants with the EFF Secure Messaging Scorecard [51] (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 end-to-end 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.
3.4 Discussion

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 end-to-end encryption. Recent literature [60] suggests that users develop more trust in an encrypted communication system that makes ciphertexts visible. However, whether the ciphertext 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 3.3.5).

Can you verify contact’s identity? Recent studies [72, 73] 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? In cryptography, forward secrecy ensures that past communications will not be compromised even if a current session’s encryption key has been discovered. Further, current and future sessions will not be compromised because a past encryption key has been leaked. 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.

3.4 Discussion

Most user studies of secure communication tools – in particular, email encryption tools, have been laboratory-based user studies mainly following the same pattern (see Section 2.2 in Chapter 2): 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., generating/sharing/managing cryptographic keys, encrypting a message) with fictional communication partners (study coordinators) to accomplish a particular security goal (e.g., confidentiality or secrecy of message content) without errors. Success, or failure, is then measured, based on the tasks and goals imposed on participants, rather than those 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 did not recognize the tool’s Secret Chat mode). However, our results show that to be adopted, secure tools have to offer utility; i.e., the ability of users to reach all their communication partners using the same tool. Security may be part of users’ primary communication goals. However, given a choice between a usable and secure tool that does not offer utility and a usable but insecure tool that does, users will 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 3.3), 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, affective interaction, marketing) the creators of secure communication tools do not necessarily 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 userbase. WhatsApp’s implementation of end-to-end encryption for text messages, voice calls, and video communications is an example of this more pragmatic
3.4. Discussion

In [66], De Luca et al. found that information security and personal 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/privacy at all. Users are aware of some threats and are willing to make some effort to manage them (e.g., by chopping up credentials into segments and sending these via different tools). Some participants preferred using some cumbersome processes/methods to send sensitive information over using a secure communication tool, because they did not believe the tools available are actually secure. This impression was fed by several misconceptions (e.g., most participants incorrectly believed service providers can access and read end-to-end encrypted messages). Besides poor usability and lack of utility, such misperceptions hindered users’ adoption of encrypted tools.

There are some users who want to be secure and are “shopping” for tools that offer specific security properties. The EFF Secure Messaging Scorecard aims – now archived – 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 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 mechanisms, such as encryption (see Section 3.3).

The key takeaway 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 end-to-end 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 incorrectly 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 – including encryption schemes – have been developed based on the best available knowledge from security research. These mechanisms are also open to audits by computer security and privacy researchers and practitioners. Users need to trust these audits in the same way that they trust agencies that carry out safety and consumer protection testing. It is very important to correct users’ mental models of that obscurity increases security, and explain why documented design and open-source software mean that it is less likely that a government agency or service provider can decrypt encrypted communications (see Chapter 6).

Based on our study findings and feedback, the EFF has archived the scorecard and is redesigning a new one. 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., end-to-end encrypted) without needing to understand security mechanisms specifically, while also providing text to help readers acquire accurate mental models of confidentiality, integrity, and authentication (see our participatory design study in Chapter 7). The scorecard will also attempt to provide more non-security information that users desire: Does the tool have a large userbase? What devices/platforms is it available on? Can it be used over 3G and Wi-Fi? Does it offer audio or video chats? Is it free? While not necessarily related to secure and private communications, 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) succeeded 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 computer security and privacy community.
3.5 Summary and Implications

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

**Secure tools with improved utility.** We encourage the computer security and privacy 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 userbase for a new tool is difficult and unpredictable. Therefore, we encourage computer security and privacy researchers and practitioners to work with today’s existing popular tools.

Although the thesis argues that we should focus on securing tools that have a large user base, this might be hard to achieve in practice due to different efforts/projects led by both large tech companies and small start-ups.

**Understand the target population.** In the long run, if computer security and privacy engineers 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 and privacy community must develop a deeper understanding of what is important (and not important) to users. Security properties and threats should also be framed in terms/phrases that users can understand (see Chapter 7 on participatory design).

**Improve QoS.** Secure communication tools must feel professional. Security itself is difficult for users to evaluate directly; they often use proxy signals, such as QoS. 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.
3.6 Limitations

Our study has a number of limitations common to all qualitative research studies. First, the quality of qualitative research mainly depends on the interviewer’s individual skills. Therefore, to minimize bias, one researcher (the thesis author), who was trained to conduct interviews and ask questions in an open and neutral way, conducted all ten unstructured and 50 semi-structured interviews.

Second, some participants’ answers tended to be less detailed, especially during the last 20 minutes of the interview. However, the interviewer prompted participants to give full answers to all questions. Further, the interviewer gave participants a ten-minute break during the interview, to reduce interviewee fatigue and inattention [136].

Third, as with all qualitative studies, our work is limited by the size and diversity of our sample. To increase ecological validity, we interviewed participants until new themes stopped emerging (total: 50 semi-structured interviews). We also recruited a demographically-diverse sample of participants in order to increase the likelihood that relevant findings have been mentioned by at least one participant.

3.7 Contributions to Thesis

In this chapter, we designed and conducted a user study to answer the first research question this thesis addresses: What are the primary obstacles to the adoption of secure communication tools (see Section 1.2)? We identified three main classes of barriers to adoption, namely: poor usability, lack of utility, and incorrect user mental models of secure communications. We explore each class of barriers in the next three chapters. Our findings also show the need for a paradigm shift: our community should prioritize securing communication tools that have large userbases over improving the usability of different secure tools that have small userbases.
### Table 3.1: Unstructured and semi-structured interview participant demographics.

<table>
<thead>
<tr>
<th>Gender</th>
<th>Age</th>
<th>Race</th>
<th>Education</th>
<th>Employment</th>
</tr>
</thead>
<tbody>
<tr>
<td>P01</td>
<td>Female</td>
<td>21–30</td>
<td>White B.Sc.</td>
<td>Student</td>
</tr>
<tr>
<td>P02</td>
<td>Male</td>
<td>21–30</td>
<td>White M.Sc.</td>
<td>Student</td>
</tr>
<tr>
<td>P03</td>
<td>Female</td>
<td>21–30</td>
<td>White B.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P04</td>
<td>Male</td>
<td>21–30</td>
<td>Black B.Sc.</td>
<td>Student</td>
</tr>
<tr>
<td>P05</td>
<td>Male</td>
<td>21–30</td>
<td>White Ph.D.</td>
<td>Student</td>
</tr>
<tr>
<td>P06</td>
<td>Male</td>
<td>31–40</td>
<td>Asian B.A.</td>
<td>Employed</td>
</tr>
<tr>
<td>P07</td>
<td>Female</td>
<td>21–30</td>
<td>White B.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P08</td>
<td>Female</td>
<td>31–40</td>
<td>Asian B.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P09</td>
<td>Male</td>
<td>21–30</td>
<td>Black M.Sc.</td>
<td>Employed</td>
</tr>
<tr>
<td>P10</td>
<td>Male</td>
<td>70+</td>
<td>White Some college</td>
<td>Self-employed</td>
</tr>
<tr>
<td>P11</td>
<td>Female</td>
<td>21–30</td>
<td>White M.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P12</td>
<td>Female</td>
<td>21–30</td>
<td>White B.A.</td>
<td>Employed</td>
</tr>
<tr>
<td>P13</td>
<td>Female</td>
<td>21–30</td>
<td>Mixed race B.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P14</td>
<td>Female</td>
<td>21–30</td>
<td>Hispanic B.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P15</td>
<td>Male</td>
<td>31–40</td>
<td>Mixed race B.Sc.</td>
<td>Employed</td>
</tr>
<tr>
<td>P16</td>
<td>Female</td>
<td>21–30</td>
<td>Black Ph.D.</td>
<td>Student</td>
</tr>
<tr>
<td>P17</td>
<td>Female</td>
<td>21–30</td>
<td>White B.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P18</td>
<td>Female</td>
<td>31–40</td>
<td>Hispanic M.A.</td>
<td>Employed</td>
</tr>
<tr>
<td>P19</td>
<td>Female</td>
<td>21–30</td>
<td>Black B.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P20</td>
<td>Female</td>
<td>31–40</td>
<td>White B.A.</td>
<td>Self-employed</td>
</tr>
<tr>
<td>P21</td>
<td>Female</td>
<td>21–30</td>
<td>White M.Sc.</td>
<td>Student</td>
</tr>
<tr>
<td>P22</td>
<td>Male</td>
<td>18–20</td>
<td>Asian B.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P23</td>
<td>Male</td>
<td>21–30</td>
<td>White B.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P24</td>
<td>Female</td>
<td>31–40</td>
<td>White B.A.</td>
<td>Employed</td>
</tr>
<tr>
<td>P25</td>
<td>Male</td>
<td>21–30</td>
<td>Hispanic M.Sc.</td>
<td>Student</td>
</tr>
<tr>
<td>P26</td>
<td>Female</td>
<td>51–60</td>
<td>White VoC</td>
<td>Employed</td>
</tr>
<tr>
<td>P27</td>
<td>Female</td>
<td>51–60</td>
<td>White B.A.</td>
<td>Employed</td>
</tr>
<tr>
<td>P28</td>
<td>Male</td>
<td>21–30</td>
<td>Black Ph.D.</td>
<td>Student</td>
</tr>
<tr>
<td>P29</td>
<td>Male</td>
<td>18–20</td>
<td>White B.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P30</td>
<td>Male</td>
<td>21–30</td>
<td>White M.Sc.</td>
<td>Student</td>
</tr>
<tr>
<td>P31</td>
<td>Female</td>
<td>18–20</td>
<td>White B.Sc.</td>
<td>Student</td>
</tr>
<tr>
<td>P32</td>
<td>Male</td>
<td>31–40</td>
<td>White M.A.</td>
<td>Employed</td>
</tr>
<tr>
<td>P33</td>
<td>Female</td>
<td>70+</td>
<td>White Some college</td>
<td>Retired</td>
</tr>
<tr>
<td>P34</td>
<td>Male</td>
<td>18–20</td>
<td>Black B.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P35</td>
<td>Female</td>
<td>18–20</td>
<td>Asian Some college</td>
<td>Student</td>
</tr>
<tr>
<td>P36</td>
<td>Male</td>
<td>18–20</td>
<td>White Some college</td>
<td>Student</td>
</tr>
<tr>
<td>P37</td>
<td>Male</td>
<td>21–30</td>
<td>White M.Sc.</td>
<td>Student</td>
</tr>
<tr>
<td>P38</td>
<td>Female</td>
<td>31–40</td>
<td>Black M.Sc.</td>
<td>Student</td>
</tr>
<tr>
<td>P39</td>
<td>Female</td>
<td>31–40</td>
<td>White M.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P40</td>
<td>Male</td>
<td>21–30</td>
<td>White B.Sc.</td>
<td>Student</td>
</tr>
<tr>
<td>P41</td>
<td>Female</td>
<td>31–40</td>
<td>White B.A.</td>
<td>Employed</td>
</tr>
<tr>
<td>P42</td>
<td>Male</td>
<td>18–20</td>
<td>White Some college</td>
<td>Student</td>
</tr>
<tr>
<td>P43</td>
<td>Female</td>
<td>21–30</td>
<td>White B.A.</td>
<td>Employed</td>
</tr>
<tr>
<td>P44</td>
<td>Female</td>
<td>21–30</td>
<td>Black M.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P45</td>
<td>Prefer not to answer</td>
<td>21–30</td>
<td>Hispanic M.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P46</td>
<td>Female</td>
<td>21–30</td>
<td>Mixed race M.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P47</td>
<td>Female</td>
<td>41–50</td>
<td>White B.A.</td>
<td>Employed</td>
</tr>
<tr>
<td>P48</td>
<td>Female</td>
<td>21–30</td>
<td>Black B.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P49</td>
<td>Female</td>
<td>21–30</td>
<td>White B.Sc.</td>
<td>Student</td>
</tr>
<tr>
<td>P50</td>
<td>Female</td>
<td>21–30</td>
<td>White M.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P51</td>
<td>Female</td>
<td>51–60</td>
<td>Mixed race B.A.</td>
<td>Retired</td>
</tr>
<tr>
<td>P52</td>
<td>Male</td>
<td>18–20</td>
<td>White Some college</td>
<td>Student</td>
</tr>
<tr>
<td>P53</td>
<td>Male</td>
<td>31–40</td>
<td>White M.A.</td>
<td>Employed</td>
</tr>
<tr>
<td>P54</td>
<td>Female</td>
<td>21–30</td>
<td>White B.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P55</td>
<td>Male</td>
<td>31–40</td>
<td>Black M.A.</td>
<td>Employed</td>
</tr>
<tr>
<td>P56</td>
<td>Female</td>
<td>21–30</td>
<td>White B.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P57</td>
<td>Male</td>
<td>18–20</td>
<td>White Some college</td>
<td>Student</td>
</tr>
<tr>
<td>P58</td>
<td>Female</td>
<td>41–50</td>
<td>White B.A.</td>
<td>Employed</td>
</tr>
<tr>
<td>P59</td>
<td>Female</td>
<td>21–30</td>
<td>Black M.A.</td>
<td>Student</td>
</tr>
<tr>
<td>P60</td>
<td>Prefer not to answer</td>
<td>61–70</td>
<td>White VoC</td>
<td>Retired</td>
</tr>
</tbody>
</table>
Chapter 4

Dead on Arrival: Recovering from Fatal Flaws in Email Encryption Tools

In this chapter, we discuss the first class of obstacles to the widespread adoption of secure communication tools, which is poor usability. We present a novel approach to studying the adoption and use of encrypted email tools. We carry out a three-part user study – installation, home use, and debrief – to assess the user experience of two open-source email encryption tools: Mailvelope and Enigmail. We recruited two groups of participants (n=10) and asked each group to install, configure, and use either Mailvelope or Enigmail over a period of one week. Participants had access to help during installation (an installation guide and an experimenter with domain-specific knowledge). After installation, we asked participants to complete a primary task of a mock flash mob using encrypted email. We gave participants a week to complete the task. We find that participants struggled to set up (install and configure) the tools. Further, they would not have been able to complete installation without help from the experimenter. Even with help, it took participants about 40 minutes to install and configure Enigmail. Participants using Mailvelope failed to encrypt their initial emails due to usability problems. Participants also reported that both tools had software bugs. During the debrief, participants said that they were unlikely to continue using the tools after the study, mainly due to the tools’ poor usability.

The rest of this chapter is structured as follows:
Chapter 4. Recovering from Fatal Flaws in Email Encryption Tools

• Section 4.1 describes the research objectives of this study.

• Section 4.2 describes our focus group study design.

• Section 4.3 presents the findings of our study.

• Section 4.4 discusses the findings of our study and explains why the computer security and privacy community should look beyond ‘ease of use’ when evaluating the usability of email encryption tools.

• Section 4.5 describes the principal limitations of the study.

• Section 4.6 describes the contributions this chapter makes to the thesis.

The content of this chapter is an edited version of the following publication:


4.1 Introduction

In [5], Whitten and Tygar’s seminal paper – “Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0” – received the USENIX Security Test of Time Award. Since Whitten and Tygar’s user study of PGP 5.0 in 1999, there have been continuing efforts to develop and produce email encryption tools, to attempt to make mainstream users adopt and use these tools. Recent research [148] reports that users are increasingly learning about security threats from various sources, making users more willing to encrypt their email than ever before.

Most user studies of email encryption tools (see Section 2) have been laboratory-based user studies (lasting for an hour on average) to assess the usability (mainly, ease of use) of encrypted email tools. Unlike prior work, we carried out a novel user study over a period of one week, to evaluate the user experience of two open-source email encryption
tools: Mailvelope [35] and Enigmail [32]. We chose to study these two tools because we know that users prefer to use encryption tools which integrate with email applications they already use [60].

The main objective of our study was to observe and analyze how novices; i.e., first-time users of Mailvelope and Enigmail, use and interact with encrypted email tools. We specifically aimed to answer this question: 20 years after Whitten and Tygar’s Johnny study, how usable is to set up and use an email encryption client? Hence, we designed and conducted a group-based user study, where we observed participants (n=10) using Mailvelope or Enigmail across three stages of activity: an installation group session, home use over a week with assigned group communication tasks (primary task: organizing a mock flash mob), and a debrief group session. Participants had access to help during installation (an installation guide and an experimenter with domain-specific knowledge). Ten participants completed the study. They were divided into two groups of four and six participants using Enigmail and Mailvelope, respectively. We found that participants struggled to set up (install and configure) the tools. Additionally, they would not have been able to complete installation without help from the experimenter. Even with help, it took participants about 40 minutes to install and configure Enigmail. Participants using Mailvelope failed to encrypt their initial emails due to usability problems. Participants also reported that both tools had software bugs. During the debrief, participants said that they were unlikely to continue using the tools after the study, mainly due to the tools’ poor usability.

To sum up, our study has shown that poor usability still remains as a primary obstacle to adopting and using encrypted email tools. Participants needed the assistance of a knowledgeable experimenter to successfully complete the various stages of the study. This raises, for future work, questions about the role of an expert in the process of helping novices learn to use a complex piece of software, to overcome the barriers to adoption and effective use, where the expert may need to take on this duty.
4.2 Methodology

In this section, we describe the research questions this study addresses, recruitment process, study design, and details of our data analysis. The Research Ethics Board at UCL reviewed and approved our research study (project no.: 9423/001). We handled all data collected in accordance with the provisions of the UK Data Protection Act 1998 (registration no.: Z6364106/2016/07/11).

4.2.1 Research Questions

In this work, we address the following research questions:

- **RQ1**: What are the facilitators and obstacles behind the adoption of encrypted email tools?

- **RQ2**: What usability issues beyond ‘difficulty of use’ should the computer security and privacy community look out for when assessing the usability of secure communication tools?

4.2.2 Recruitment

We recruited participants through a research participant pool at UCL. It is a participant pool where members of the general public can register and sign-up for research studies. Prospective participants completed a pre-screening questionnaire (see Appendix A) to indicate occupation, age, gender, whether they had previously used an email client, and whether they had any experience with email encryption tools.

Overall, 52 people completed the pre-screening questionnaire. We formed two focus groups, with six participants each, in order to be resilient to unanticipated no-shows. Those with a background in computer science were excluded to favor non-technical users. Two of the invited Enigmail participants did not show up on the day of the lab-based setup session.

We paid participants a reward of £30 for taking part in our study.
4.2.3 Study Design

We aimed to compare characteristics of Mailvelope and Enigmail, to understand the facilitators and obstacles behind adoption of encrypted email tools. We chose Mailvelope and Enigmail as they are end-to-end encrypted, open-source, and available free of charge. While Enigmail is a stand-alone extension to the Thunderbird email client, Mailvelope is an integrated solution, as either a Chrome extension or a Firefox add-on.

We designed and conducted a three-part study with one group of participants installing and using Enigmail alongside Thunderbird, while the other group using Mailvelope. Participants used their own laptops during the study, as follows:

- **Lab-based setup.** We interviewed participants about their email-related habits, and asked them to install, configure, and begin using their assigned tool.

- **Home use of encrypted email.** We gave participants a task to complete outside of the lab setting, organizing a mock flash mob campaign via encrypted email over one week. Participants sent emails to each other to agree on the location and music for the mock event, and to confirm the location with the experimenter. They also sent emails to a new member of the group (another researcher).

- **Lab-based feedback session.** Participants discussed their experience of Enigmail or Mailvelope after organizing the flash mob campaign.

We asked participants to bring their own laptop to the study. We provided them with printed copies of the installation guidelines for either Thunderbird and Enigmail or Mailvelope. Crucially, the experimenter (Juan Ponce-Mauries) was available to assist participants – rather than presume to lead them – during the setup phase, and was contactable during the home-use phase. We asked participants to note when they completed specific tasks on another sheet: (1) installing Thunderbird (only for the Enigmail group), (2) installing the Enigmail extension for Thunderbird or the Mailvelope extension on Chrome or Firefox, (3) configuring the extension (generating a private and public key pair), (4) sharing public keys with other group members, and (5) sending an encrypted
email to the study coordinator.

At the lab-based debrief session, participants completed System Usability Scale (SUS) [149] forms for both Mailvelope and Enigmail. The SUS form consists of ten statements, where users indicate how strongly they agree with each statement on a five-point Likert scale.

4.2.4 Procedure

Upon arrival, we asked participants to read an information sheet and sign a consent form. We tasked the first group with installing Mozilla Thunderbird and Enigmail. We assigned the second group the browser extension Mailvelope that worked with Chrome or Firefox web browsers. Although we gave participants an explanation of the tasks to be completed, we did not brief them on the specific goal of the study until the end of the final session one week later, to minimize biases.

4.2.5 Role of the Experimenter

We initially conceived the role of the experimenter to be that of a session facilitator, asking participants about their experiences with the tools, and eliciting their mental models of how encryption worked. As Mailvelope and Enigmail are targeted towards mainstream users, we provided participants with official setup guidelines published by the developers of these tools.

At the design stage of the study, we did not envisage the role of the experimenter to be an instructor telling participants how to set up the tools. However, the pilot session we conducted before the main study sessions made us change this element of the study design. In the pilot study, we used a convenience sample consisting of colleagues who mostly had a computer science background. We asked them to perform the exact same tasks as our participants. The pilot session of the setup lab-session took in excess of 1.5 hours, where despite the sessions being full of discussion about the instructions, the pilot participants struggled with the installation process to such a degree that it was necessary for the experimenter, a domain-knowledge expert, to guide them through the process to
successful installation and use. As a result, we decided that the experimenter to not actively lead participants through the setup steps, but to respond to requests for help from participants if they arose during the session(s).

### 4.2.6 Data Analysis

We conducted, transcribed, and analyzed both focus groups. The transcripts were independently analyzed by two researchers (Juan Ponce-Mauries and thesis author) using Thematic Analysis [150].

### 4.3 Results

We first describe the demographics of our participants in Section 4.3.1. We then present the key emerging and recurring themes we observed across our interviews in Sections 4.3.2–4.3.3. We referred to participants as PX-E for those in the Enigmail group, and PX-M in the Mailvelope group. We additionally report how many participants mentioned each theme to give an indication of the frequency and distribution of themes (although the main purpose of qualitative research is to explore a phenomenon in depth, and not to generate quantitative results).

#### 4.3.1 Demographics

The Enigmail group had four participants, two females and two males. Their mean age was 32.7 ($SD = 20.2$, range: 23–45). The Mailvelope group consisted of four females and two males, with a mean age of 39.6 ($SD = 9.1$, range: 24–76).

#### 4.3.2 Task Completion and Times

The average task completion times are shown in Figure 4.1. The average completion time for all tasks was 48.1 minutes for the Enigmail group, and 40.4 minutes for the Mailvelope group. Task times are self-reported, so values may not be precisely accurate, but are indicative of the time it took for each group to complete the tasks assigned to
them. The majority of participants in both groups reached and completed the final task. However, it can be seen that even with (minimal) assistance from the knowledgeable experimenter, it can take novices in the region of half an hour to set up and test encrypted email. Average task times for Enigmail are shown below alongside notable participant quotes in Figure 4.2, and for Mailvelope in Figure 4.3.

All Enigmail participants completed the four mock campaign tasks successfully. In the Mailvelope group, one out of six participants was unable to complete the third and fourth setup task (e.g., importing a new public key from a new participant and sending encrypted email to this person). This participant, P4-M, downloaded the attachment correctly but imported an incomplete block of text as part of the public key. Participant P2-M was unable to complete task four due to a broken laptop.

**SUS.** A SUS score can range from 0 (poor) to 100 (excellent). The average score for Enigmail was 63.1 (range: 57.5–77.5, $SD = 9.7$), and for Mailvelope was 50.8 (range: 27.5–70, $SD = 19.4$). This result means that Enigmail achieved “Good Usability”, whereas Mailvelope achieved “OK Usability”. An unpaired t-test showed that these differences were not statistically significant ($p = 0.28$), possibly due to a small sample size.

### 4.3.3 Qualitative Results

We transcribed and analyzed the audio-recordings of the sessions. We identified the themes below.
4.3. Results

“It’s too much text!” (P3-E)

“I don’t like the format of Mozilla Thunderbird. It looks too... I don’t know, Hotmail is a bit better, and with Thunderbird, it looks like I don’t know, very retro...” (P2-E)

“Oh, that was easy...” (P1-E)

“... But when you got all of the boxes “Oh my god! Which one do I do – this one or this one?” And that’s where I start to struggle because I don’t understand the technical language. If it just says: “Do this. Press this.” but once it starts giving me choices, I’m like: I don’t understand the differences!” (P4-E)

“If I say to some of my friends or even my elderly parents: “Hey! That’s encrypted email!”, it’s just not going to happen and it’s not like I really understand it. It needs to be literally as easy as installing some of the other apps, you know, that you can just download and have encryption that way. For me, it has to get to that point really for general consumption...” (P4-E)

Figure 4.2: The user journey of setting up Enigmail. The graph shows timings for each step of the setup process with notable participant quotes.
“There was no way of knowing if we had done it or not. It would have been good if there’d been a bar across the top saying or showing how much of it was installed, or saying it was installed because I wasn’t absolutely sure if it was finished…” (P1-M)

“It was a bit complex, I had to ask many times, it was complicated…” (P2-M)

“It’s too complicated, it’s too much!” (P4-M)

“Finding the keys, importing them, that was pretty difficult!” (P5-M)

“Yeah, very simple, it was kind of cool to learn that it was that easy, to be able to encrypt an email… I didn’t realise that you could just add something to your Gmail… you know, an add-on and do it that easily…” (P2-M)

Figure 4.3: The user journey of setting up Mailvelope. The graph shows timings for each step of the setup process with notable participant quotes.

4.3.3.1 Sharing Sensitive Information

Participants generally considered personally identifying information to be sensitive (e.g., when shopping online or entering passport details for flights). They felt that disclosure of
this information could expose them to the risk of identity theft or leakage of, for instance, online banking details.

All participants expressed that they had needed to share sensitive information at some point. Diverse means were mentioned; two participants had shared sensitive information via regular email, a further two via the telephone, and three via messaging applications, such as WhatsApp or Facebook Messenger. Two participants stressed that they, as users, had to trust the service provider, or otherwise not use the service at all:

“I mean… you basically have to put your trust in it, otherwise you just don’t use the email or you don’t use the messenger service, you know?” (P5-M)

Participants spoke of unintended recipients who might access their emails. All Mailvelope participants agreed with P4-M’s sentiment: “Well, I think […] Gmail, it’s checked every time we use it and all of our data is known to them.” Participant P3-M argued that their emails would not be a target for malicious parties: “We are not… important enough for somebody to hack my personal email… we are not Hillary Clinton!”

4.3.3.2 Encryption

All participants had previously heard of “encryption”, but did not report having used a dedicated email encryption tool. Participant P4-E had; however, previously tried to install Mailvelope a few months prior to the study:

“I tried to install Mailvelope, yeah, but only got half-way through ’cause I really couldn’t understand how to do the rest of it…”

Participant P2-E noted having “seen people use PGP and stuff” without having used it personally, despite having “technical friends” who encrypted their emails. In response, P3-M explained the mechanism behind encryption as follows:

“It kind of converts the entire message into some kind of codes and then you
send to the recipient in the form of code and then something happens… I
don’t know what happens…”

There was a consensus amongst participants that encryption did something to the original message that prevented an unintended person from reading the message.

Participants also commented on recent news, airing concerns about anonymous browsing and government involvement. P1-E commented: “Recently the government was trying to block… something they were trying, they didn’t want the encryption because obviously they want access to your emails…” They further elaborated that using encryption might draw attention: “If all our communications are being monitored, wouldn’t having encryption make you a suspect of some suspicious activity instead?”

4.3.3.3 Installation and Configuration

Participants from both groups agreed that the installation of the extensions was straightforward (including Thunderbird for the Enigmail group). For P1-M, installing the Mailvelope extension was perhaps too seamless:

“There was no way of knowing if we had done it or not. It would have been good if there’d been a bar across the top saying or showing how much of it was installed, or saying it was installed because I wasn’t absolutely sure if it was finished…”

All participants agreed that configuration of the extensions was complicated. For Enigmail, the experimenter had to intervene because there was a bug in the setup wizard. When the setup wizard tried to download the GnuPG component required by Enigmail to do the cryptographic work, a progress bar was shown with the progress of this download. However, the download and installation did not actually start, and no error message or warning message was displayed.

The Mailvelope group complained that after installation, the steps required to configure the extension were unclear. They found locating the button to open the options menu
was frustrating since they did not know what to look for. Participant P2-M commented: “It was a bit complex, I had to ask many times, it was complicated...” Enigmail users similarly complained that the process was convoluted, difficult to follow, and that it was hard to completely understand all available options, and then decide which one to choose. P4-E elaborated:

“... When you get all of the boxes I’m like “Oh my god! Which one do I do – this one or this one?” And that’s where I start to struggle because I don’t understand the technical language.”

All participants completed the steps up until key exchange without incident. Those in the Mailvelope group were frustrated at being unable to share public keys. The key-generation setup wizard had an option to automatically upload a public key to Mailvelope’s key servers, but this process did not work – even when the option was selected, the keys were not uploaded. Participants instead had to copy and paste the key or download it as a file to manually share it with others.

Experimenter intervention was necessary to explain the manual process needed to effectively exchange keys. P4-M was evidently frustrated: “It’s too complicated, it’s too much!” All participants agreed that this step was the worst, as it was unclear what to do intuitively or from the official guide. P5-M: “Finding the keys, importing them, that was pretty difficult!” Most participants did not understand the need for two keys:

“I didn’t understand the need for keys, this is all new to me... I can use email, but I don’t know why we need a key... so I would have given up, I think!”
(P1-M)

4.3.3.4 Thunderbird and Enigmail

The Enigmail group generally did not like the encryption experience. When asked if any changes would make the tool better, the focus was on the setup process. P3-E saw too many steps in the installation and configuration process:
“I was thinking it should be built into Thunderbird, just using one piece of software, so just basically the install is like: “Where [do] you want to install it?” and then: “Do you need to set up keys?” or whatever.”

P4-E made comparisons to the use of other applications:

“It needs to be literally as easy as installing some of the other apps, you know, that you can just download and have encryption that way.”

When considering the design of the Thunderbird interface, P1-E commented that:

“I didn’t really like the interface of Thunderbird, I thought it was a little bit more clunky, umm, it had very old-school interface.”

Participant P4-E said that even though she liked the idea of encryption, the whole process of getting it to work was too complicated. She attributed it to her age, after hearing about encryption, she had genuine privacy concerns:

“Because it’s there I would use it, but it’s too complicated, maybe because I’m 45 and maybe it’s the younger generation of people who put their whole lives on the Internet, you know, and privacy, the idea of privacy is changing… and I… even though I haven’t got any sensitive information really, it’s just about protecting my own privacy. It’s just like getting letters in the post, you wouldn’t necessarily just leave your letters laying around for people to read…”

P4-E explained usability was necessary for adoption by all users:

“If I say to some of my friends or even my elderly parents: “Hey! That’s encrypted e-mail!” , it’s just not going to happen and it’s not like I really understand it. It needs to be literally as easy as installing some of the other
4.3. Results

Apps, you know, that you can just download and have encryption that way.
For me, it has to get to that point really for general consumption…”

Participants commented that once the applications had been configured, the interface in fact simplified the use of encrypted email as well as public key sharing. They all noticed the warning messages when an email was going to be sent unencrypted. They also said that sharing their public key was easy and convenient because they only had to click one button.

All those in the Enigmail group did, however, say that they would likely remove it from their laptops after the study. P3-E explained:

“I’ll reinstall it if I have specific reasons like someone sends me an encoded message or I need to send someone something, but it’s taking a lot of space.”

4.3.3.5 Mailvelope

Once through the process of exchanging keys, Mailvelope users felt that the rest was easy to do. P3-M and P2-M commented, respectively, that “I think it was fairly simple to use after that and yeah!… I can see myself using this with people that I email often…” and that “it was kind of cool to learn that it was that easy, to be able to encrypt an email… I didn’t realise that you could just add something to your Gmail… you know, an add-on and do it that easily…”

All participants felt confident using the system after a few days completing tasks, and wanted to share their comments. P1-M: “I didn’t know that just adding an extension you could do all that… encrypting and decrypting…” P6-M struggled to complete tasks for the first few days of home use, having forgotten the passphrase for their private key. They were upset about missing the tasks:

“So I tried all the password permutations, so I was so confused… I still wonder why it is… I used something easy to remember… After several days, I said “Oh my goodness!” I had to tell you I had forgotten…”
Once asked to repeat the process of generating new keys, they were excited to ex-
change the new public key, where “that was one thing that I managed to do and I feel quite proud about that!”

There were some comments as to how to improve Mailvelope’s interface and the pro-
cess of encrypting emails. Three participants reported that the button to activate encryp-
tion was not obvious, leaving them prone to sending unencrypted email (see Figure 4.4
for a screenshot depicting the encryption button). P3-M explained:

“Perhaps something more prominent than just that tiny button, because I did it a couple of times, I was writing the text until I realised.”

Figure 4.4: A screenshot of the user interface for Mailvelope displaying the encryption button on the right.

P6-M expressed a concern that the tool did not warn them when they tried to send their public key, and instead attached the private key:
4.4. Discussion

“It’s just not safe, I mean, they should definitely send a warning message saying “Do you really want to send your private key...?” or something. Yeah... I sent my private key, it should at least warn once. There are so many times when you do something and it’s like “Are you sure?” and for the private key it just sends...”

All those in the group agreed that despite interface issues, Mailvelope was easy to use once they were familiar with the process. Some members of the group mentioned that they would try to use the tool with friends and family. P4-M explained:

“I’ll keep it but to be honest, I doubt I’ll use it... I just don’t email sensitive information with people... that often...”

4.3.3.6 Interoperability: Network Effects

In the final session, when discussing their possible future use of the tools, participants (in both groups) raised concerns that their contacts would need to install these tools as well. While it is true that their contacts would need to install a PGP-based client, participants thought the client would need to be the exact same one that they had. They were surprised when we explained to them that any PGP-client would be able to exchange encrypted messages with another PGP-client. It was an interesting mental model that could have influenced the design of instant messaging tools that generally did not offer interoperability. We showed in the previous chapter that the adoption of such communication tools is largely influenced by network effects [1].

4.4 Discussion

Adoption barriers appeared across all three stages of our study and for both Mailvelope and Enigmail. Computer security and privacy researchers and practitioners may continue to study emerging encrypted email solutions to progressively identify isolated barriers to adoption. However, security software developers continue to rely on an intuitive sense
of what constitutes usability [151]. If we want any chance of promoting adoption of email encrypted tools, basic software quality and usability need to be delivered first and foremost. Furthermore, developers need to draw on usability and design expertise: if the tools are seen as “retro” and do not meet user expectations, we can hardly expect these tools to be adopted by mainstream users.

Both tools had software bugs; downloading the GnuPG component required by Enigmail and automatically uploading a public key to Mailvelope’s key servers did not work. Participants had to do both manually after being instructed by the experimenter. Mailvelope’s option to encrypt was not immediately obvious as previously shown by Schochlow et al. [152], where prevention of errors is a fundamental precursor to providing good user experience [153]. Effective user interaction with encryption tools still lies in following basic software design principles.

Participants in both groups were familiar with using email clients, both in the browser and as standalone applications. Both Mailvelope and Enigmail integrated with existing solutions. However, Mailvelope integrated with a browser, permitting users to continue to use existing email clients that they were familiar with. This shows that we should pave the way for email encryption to be integrated into existing popular platforms. We should also emphasize the importance of interoperable tools (as we discuss in the next chapter).

There is a shared assumption in the computer security and privacy community that people would use a secure communication tool (e.g., an email encryption tool) to share information they regard as sensitive. However, we found (in line with our findings in the previous chapter) that our participants would not use an encrypted email tool to share sensitive information. They reported other ways to share such information that they incorrectly believed to be more secure than encrypted email.

Finally, we make a methodological contribution in this chapter. Ideally, the experimenter has an observatory role in a study like this, but because of the shortcomings of both Mailvelope and Enigmail, the experimenter had to step out of this role and take on a more active approach of responding to participants’ questions. Without an informed expert present, many participants reported that they would not have continued trying to
use the tool(s) in reality. One flaw can be enough to dissuade potential users. However, with guidance, participants in both groups were able to complete the setup and encrypt their email. Our findings show that for computer security/privacy user studies, employing researchers who act strictly as experimenters and with domain knowledge has its own advantages. Having a knowledgeable expert close by study participants can be a natural way of learning how to use a new technology [154], where this study has also been an opportunity to observe how having a helper available to provide assistance can aid participants in overcoming obstacles which have a known – albeit complicated and demanding – solution.

4.5 Limitations

Our study has a number of limitations common to all qualitative research studies (see Section 3.6). An obvious limitation of this study was the small sample size of ten participants who took part in our focus groups. However, as this was an exploratory study involving focus groups, the “common rule of thumb” is that an average of six participants in each focus group is reasonable [155]. We also recruited a demographically-diverse sample of participants in order to increase the likelihood that relevant findings have been mentioned by at least one participant.

A major advantage of focus groups – their ability to encourage group-level discussion – is potentially one of their major limitations. Participants may behave differently in a focus group study. The privacy paradox, in which people’s stated privacy behaviour is not the same as their actual behaviour, is a well-known phenomenon [155]. However, in the context of a focus group, people may be more truthful about their privacy behaviour in front of others who may challenge them and ask for justification of their views.

Finally, in focus group studies, there may be a danger of dominant personalities steering a group’s discussion. To mitigate this, we allocated a certain amount of time to each interview question, ensuring discussion remained focused and was not hijacked by particular participants.
4.6 Contributions to Thesis

In this chapter, we designed and conducted a user study to answer the second research question this thesis addresses: What usability issues beyond ‘difficulty of use’ should the computer security and privacy community look out for when assessing the usability of secure communication tools (see Section 1.2)? We found that, in addition to difficulty of use and regularly-cited usability issues (see Section 2.2), Mailvelope and Enigmail – two encrypted email tools – had bad software quality. One software bug or flaw can easily dissuade potential users from adopting a secure tool. This finding supports the paradigm shift we encouraged our community to prioritize in the previous chapter – namely, securing communication tools with proved utility and good user experience instead of improving the usability of different secure tools that have small userbases – to, in part, avoid software quality issues. Finally, this chapter makes a methodological contribution to the thesis; employing researchers as knowledgeable experts in computer security/privacy user studies to assist study participants would help overcome many barriers which have a known – albeit complicated – solution.
In Chapter 4, we showed how poor usability is one of the three main classes of obstacles to the adoption of secure communication tools (in particular, email encryption tools). Participants struggled to setup (install and configure) two PGP email encryption tools: Mailvelope and Enigmail. They also would not have been able to complete set-up without the help of a knowledgeable experimenter. Even with help, it took participants about 40 minutes to setup both tools. Further, most participants did not know how to generate, share, and manage their cryptographic keys, as well as encrypt emails.

We also showed why the computer security and privacy community should prioritize securing communication tools that have a large userbase and have already been adopted by mainstream users, over improving the usability of different, especially newly-created, secure tools. We found that both Mailvelope and Enigmail, two recently-created end-to-end encrypted tools, suffered from bad software quality as well as many usability issues, including the classical issues cited as barriers to adopting PGP 5.0 by Whitten and Tygar in their seminal paper in 1999 [5].

In this chapter, we describe the second class of obstacles to the adoption of secure
communication tools, namely **lack of utility**. We show how users’ goal and ability to reach all their communication partners in a timely-manner when using a secure messenger override everything else, including both usability and security. We evaluate the end-user experience of Telegram, a usable instant messaging tool that was launched with security (mainly, end-to-end encryption) as a key selling point. Unlike Mailvelope and Enigmail, Telegram secures communications without any user interaction; Telegram communications are encrypted by default. Users are not required to manually generate/share/manage their keys or encrypt/digitally-sign their Telegram messages, alleviating many of the usability issues we uncovered in the previous chapter. Yet, we find that a communication tool that is usable, secure, and perceived as secure by many of its users (as we found in Chapter 3 and show in this chapter), like Telegram, can still suffer from low adoption due to its lack of utility.

This chapter is structured as follows:

- Section 5.1 describes the research objectives of this study.
- Section 5.2 gives a detailed overview of the Telegram instant messaging tool and its security features.
- Section 5.3 describes two parts of our study – a laboratory-based user study and usability inspection of the user interface of Telegram – we designed and conducted to evaluate the end-user experience of Telegram. The section also presents the findings of these two parts.
- Section 5.4 discusses the findings of this study and explains why lack of utility is a primary obstacle to adopting Telegram.
- Section 5.5 describes the principal limitations of the study.
- Section 5.6 describes the contributions this chapter makes to the thesis.

The content of this chapter is an edited version of the following publications:
5.1. Introduction

Recent events have seen developers offering communication tools with greater security. These events include revelations about mass surveillance and the potential for user tracking in communication tools (e.g., Facebook’s tentative plan to use WhatsApp user data [156]). In light of these events, the computer security and privacy community has advocated the widespread adoption of secure (especially end-to-end encrypted) communication tools to protect users’ personal privacy and resist surveillance. Several communication tools (e.g., iMessage, WhatsApp) have adopted end-to-end encryption. Other tools have been launched with security as a key selling point (e.g., Signal, Telegram). However, security-related features may differ in how much they involve the user. Further, differences in the visibility of security features could easily create problems and erode users’ trust in a secure communication tool [59, 60]. In this work, we evaluated the end-user
experience of the Telegram instant messaging tool [157]. We chose to study Telegram not only because it is advertised as secure and is perceived as such by many users, but also it is unique in offering two separate chat modes with different levels of security: (1) the non-end-to-end encrypted default chat mode and (2) the end-to-end encrypted Secret Chat mode. However, we hypothesize that although Telegram is usable and is perceived as secure by many people, users could use Telegram in ways that are not anticipated by its developers. Additionally, users might not be able to distinguish between the two chat modes of Telegram and make effective use of them.

To evaluate the user experience of Telegram and explore the factors influencing its adoption, we designed and conducted a three-part study: (1) a laboratory-based user study (n=22: 11 novices and 11 Telegram users or participants with prior experience of using Telegram); (2) a hybrid analytical approach combining cognitive walkthrough and heuristic evaluation, focusing on inspecting the user interface of Telegram (with no participants recruited); (3) a survey (n=300 respondents). The approach we followed in the first and second parts of the study has been applied before in the area of usable security, notably by Whitten and Tygar to evaluate PGP 5.0. Here, we conducted a laboratory-based user study that uses a set of tasks to elicit user perceptions of Telegram. The usability inspection complements this by allowing us to look at issues not touched upon by those tasks or not reported by our participants. However, unlike Whitten and Tygar who only recruited novices (first-time users of PGP), we recruited both novices and non-novices.

Prior work has focused on first-time users of a secure communication tool (i.e., novices) to identify the barriers to adopting the tool. However, prior user studies of secure communications have rarely involved non-novices, where these users can identify the factors that influence the adoption and usage of secure tools in practice. In this work, we recruited both novices and non-novices (current users and abandonees) for the first and third parts of the study. For the first part, we asked participants to bring their mobile

---

Signal and iMessage provide end-to-end encryption for both one-to-one communications and group communications within the same platform, unlike Telegram. However, we chose to study Telegram in this chapter because we found in Chapter 3 that participants who used, or had used in the past, Telegram exchanged communications they regarded as sensitive using the default chat, and not the Secret Chat mode – incorrectly believing they used Telegram securely. Hence, we were interested in further exploring how Telegram’s two chat modes influenced people’s usage and perceptions of Telegram.
devices to the laboratory. Novices installed Telegram to explore its features by way of a ‘sensitive payment information’ messaging scenario. Prior users of Telegram were similarly involved in the task, but as an opportunity to see how they had been using the tool and the role of Telegram’s various security features in these practices, such as the use of the Secret Chat mode. In both cases, we used scenario tasks to promote discussion as part of semi-structured interviews. We used the System Usability Scale (SUS) questionnaire to further explore the usability of the tool for novices and non-novices alike. We found that both groups associated high SUS scores with Telegram, even where we found non-novices used (or had used in the past) a few features – including security features. The high SUS scores indicate that Telegram is usable.

We also recruited novice and non-novice respondents for our survey (third part of the study). We asked respondents whether or not they had used Telegram. If they had not, we asked them to share their experience of their main instant messaging tool. For those who used (or had used in the past) Telegram, we asked them to explain why they decided to use Telegram, describe what they used (or had used) Telegram for, and compare their experience of Telegram with that of their main instant messaging tool, if Telegram was not their main tool. For abandonees (prior users), we asked them why they stopped using Telegram.

Comparing the initial impressions of novices with the experiences of non-novices illustrated that in practice there may be at most partial adoption of Telegram and its security features by regular users. Non-novices tended to abandon Telegram despite believing it was usable. They preferred to adopt a communication tool which was more popular with the people they wanted to remain in contact with (i.e., offered better utility). Similarly, participants would benchmark Telegram and its features against a favored communication tool (e.g., WhatsApp). For both novices and non-novices, when participants wanted to exchange sensitive information, they would use a mix of communication channels (such as calling a person’s phone or meeting in-person), rather than using a tool they perceived as secure, such as Telegram (and indeed other secure messaging tools).

Alarmingly, most non-novice participants developed the habit of using the less secure
default chat mode of Telegram, incorrectly believing they were using Telegram in a secure way. This is mainly due to Secret Chat’s lack of utility. Secret Chat does not support group conversations. Further, the communicating parties (sender and recipient) need to be online at the same time when they initiate a Secret Chat session. Hence, the sender cannot reach their communication partner in a timely-manner, hindering the adoption and use of Secret Chat mode.

Finally, although Telegram is usable (mainly, easy-to-learn and easy-to-use) and was perceived as such by our participants (as indicated by the high SUS scores), we found some design issues in Telegram’s user interface. For example, the inconsistent use of terminology (e.g., using the term “Encryption Key” to describe a verification fingerprint) was a source of issue to novices and non-novices alike. Drawing from these findings, we recommend that practitioners should follow the usability engineering principles (such as those advocated by Nielsen and Molich [58]) consistently, or they risk leading users into using tools in such a way that the security features of a communication tool become unclear.

5.2 Telegram

Telegram (or Telegram Messenger) is an instant messaging tool that was launched in 2013. Telegram client applications exist for both desktop (e.g., MacOS, Microsoft Windows) and mobile systems (e.g., Android, iPhone). Telegram supports the exchange of text messages, photos, videos, and files between individual users and groups of users. Users can also make voice calls using Telegram. In March 2018, Telegram announced that it had more than 200 million monthly active users, generating billions of messages daily [157].

Telegram accounts are tied to phone numbers, verified via an SMS message or a phone call. Users can create an alias (a public username) to limit exposure of their phone number. A passcode can be used to lock an account, and multiple devices can be linked to a single account. An optional “two-step verification” feature requires a password in order for a user to access an account from a new device (in addition to the verification code).
Users can delete their account manually. Otherwise, an account is automatically deleted after a period of inactivity.

Telegram has been launched with security as a key selling point. Telegram supports two chat modes: a default chat mode and a Secret Chat mode. Messages exchanged within the default chat mode are cloud-based and stored on Telegram’s servers, supporting synchronization of messages across a user’s connected devices; in this mode, messages are encrypted in transit using client-server/server-client encryption. In contrast, messages exchanged within the Secret Chat mode are end-to-end encrypted (where the ends refer to the sender and recipient’s devices) and can only be accessed from the originating device (i.e., are not cloud-based). When a Secret Chat session is initiated, participating devices exchange a long-term encryption key using Diffie-Hellman key exchange [56]. After an end-to-end encrypted session has been established, communicating devices use this key to exchange encrypted messages using a symmetric encryption protocol, called MTProto [158].

When a Secret Chat session has been established, both an image and a textual visualization are generated on the sender and recipient’s devices, visualizing their public-key fingerprints. Communicating parties would verify each other’s identities by comparing both representations through a trusted channel (e.g., in-person). If the representations match, the session is secure, and a man-in-the-middle attack has not occurred. Users can initiate different Secret Chat sessions with the same contact. Telegram claims that secret chats can be deleted at any time, and can, in principle, self-destruct; i.e., disappear from both the sender and recipient’s devices after a period of time, without storing a copy of exchanged secret chats on Telegram’s servers. Users have the option to set the “self-destruct timer” to the desired time limit. Secret chats cannot be forwarded to other contacts, and, according to Telegram, leave no traces on the servers (see figure below).

Telegram’s client-side code is open-source, whereas its server-side code is closed-source and proprietary. The EFF Secure Messaging Scorecard (now archived) provides information to non-expert users about the security features offered by various messaging tools [51]. The EFF Scorecard gives Telegram’s default chat mode a rating of four out of
seven points, and the Secret Chat mode seven out of seven points. However, recent audits have revealed that Telegram has many security issues that could compromise its integrity as a secure instant messaging tool [158]. Telegram uses its own “home-brewed” encryption protocol, MTProto, rather than well-studied, provably-secure encryption schemes that achieve strong definitions of security (and that are at least as efficient). Further, Telegram leaks metadata, which could allow an attacker to determine when a user is online and offline, when they use the tool, or where they are located [159].

Figure 5.1: Secret Chat mode.
5.3 Methodology

In this work, we evaluate the end-user experience of Telegram and its security features. We also explore the factors influencing the adoption and use of Telegram. We chose to study Telegram because it has been launched with security (mainly, end-to-end encryption) as a key selling point, and has recently gained significant popularity. Further, Telegram is a unique instant messaging tool; it supports two distinct chat modes: communications exchanged within the default chat mode are encrypted in transit, whereas communications exchanged within the Secret Chat mode are end-to-end encrypted. Hence, we investigate how users send information using Telegram and how they perceive its security. We found in Chapter 3 that most participants who reported using Telegram sent information they regarded as sensitive using the less secure default chat, rather than the Secret Chat mode. In this chapter, we investigate and expand on this finding.

User studies of secure communications (described in Chapter 2) have further motivated questions around the uptake of secure communication tools and their security-related features. Hence, we studied both novices and people with prior experience in using Telegram to compare and contrast their experiences. We designed and conducted a three-part study to explore the factors impacting adoption and effective use of Telegram. The findings of the first part of our study (laboratory-based user study) showed that the vast majority of participants, especially non-novices, were not making use of the Secret Chat mode. To investigate why our participants developed the habit of using the default chat mode, we inspected the user interface of Telegram (second part of our study) to understand whether or not the user interface was a potential source of confusion for users.

Finally, we conducted a survey of 300 respondents (non-users and former/current users) in 2019 – after three years from conducting the first and second parts of the study – to investigate whether or not people’s usage of Telegram has changed. The findings of our survey confirm the findings of the first and second parts of the study. Therefore, we do not describe the survey questionnaire and findings in this thesis. However, the survey study can be found in the journal publication above (see Section 5.1) and the survey questionnaire in Appendix C.
To this end, we address the following research questions:

- **RQ1**: What are the factors that influence the adoption and effective use of an instant messaging tool – like Telegram – that is usable, secure, and perceived as secure by most of its users?

- **RQ2**: Is the user interface of Telegram a source of confusion for its users? If yes, why?

### 5.3.1 User Study

In this section, we describe our laboratory-based user study, recruitment process, task-based scenario, complementary study questionnaires, post-study interview script, and data analysis. Our UCL’s Research Ethics Committee approved our study (project no.=3615/008). We handled all collected data in accordance with the provisions of the UK Data Protection Act 1998 (registration no.=Z6364106/2016/02/71). We conducted the study between August 2016 and September 2016. We present the findings of our user study after the methodology description.

#### 5.3.1.1 Method

**Recruitment.** We recruited our participants via UCL’s Psychology Subject Pool. We asked prospective participants to complete a short online pre-screening questionnaire, to provide basic demographic information (e.g., gender, age) and contact details (e.g., name, email address, phone number). We also provided prospective participants with a list of different communication tools, asking them to indicate the tools they currently used or had used in the past. We also asked them to name any other tools they used, or had used, but were not on the list. Telegram was on the list.

Overall, 210 individuals completed the pre-screening questionnaire. 27 participants reported they used or had used Telegram. We divided our pool of eligible participants into sub-groups based on their demographics, with the aim of achieving a balance of age
and gender in the following two groups: novices (first-time users of Telegram) and non-novices (current and prior users of Telegram). We selected 22 participants: 11 novices and 11 non-novices. We detail our participant demographics in Section 5.3.1.2.

**Task-based scenario.** We designed and conducted a face-to-face laboratory-based session consisting of both a task-based scenario using Telegram and a post-study interview. Each session lasted for approximately one hour. We explained to participants (upon arrival) the general objective of our study, which was the evaluation of the end-user experience of Telegram. We also outlined our participants’ rights as individuals taking part in our user study, supported by a printed information sheet and a printed consent form. We gave each participant a £10 Amazon voucher for their participation.

We asked novices to install Telegram on their own personal mobile phone, rather than using a phone which they would be unfamiliar with and could hinder using Telegram. However, we maintained back-up mobile phones in the event of technical problems: Nexus 6 running Android 6.0 and iPhone 6 running iOS 10.1.1. Four participants used these back-up phones; two were Android users and two iOS users. We gave novices the time they needed to explore Telegram and its features after installing it.

We then introduced participants to a researcher (me) with whom they would communicate during a structured scenario. In the scenario, the researcher acted as a trustworthy colleague, with whom they ran a fictional small business. We asked participants to send sensitive financial details to the researcher using Telegram in order to complete a mock purchase. Participants referred to a paper booklet containing the financial details: randomly-generated credit card number, card validation value (CVV), and card expiry date. We asked participants to treat these details in the same way they would treat their own sensitive information. Participants were free to choose what chat mode (default or Secret Chat) to send the financial details with no prompting from the researcher. We also encouraged them to think aloud throughout the activity.

After sending the financial details, participants were then asked to send a greeting to their ‘colleague,’ who was me in this case. I would then prompt them to start a Secret Chat.
session – in case they did not send the financial details using the Secret Chat mode. We asked participants to explain the security features or properties displayed to them upon switching to the Secret Chat mode (see Figure 5.3b). We also asked them to test the self-destruct timer.

**SUS.** We asked our participants (after completing the study tasks) to complete the SUS questionnaire, a tool commonly used to assess the usability of a system or a technology [149]. SUS is a ten-item questionnaire for capturing subjective assessments of usability. Each item or question has five possible responses on a Likert scale, ranging from “Strongly agree” to “Strongly disagree.” SUS is generally used after participants or study subjects use a system or a product, but before any debrief. Many prior user studies have considered SUS to be a good indicator of users’ perceived usability [160]. It has been used, for instance, to assess the usability of encrypted email tools, as we described in Chapter 4.

**Post-study interview.** We asked participants (after completing the SUS questionnaire) about their general impressions of Telegram. We also explored participants’ opinions of other communication tools they used or had used in the past, and how they compared to Telegram. This was also an opportunity to explore participants’ perceptions of secure and private communications, as well as information sensitivity 3. In the post-study interview, we visited notable events that occurred during the task-based scenario session (e.g., whether the use of one chat mode or the other was intentional or incidental). These events might have been influenced by participants’ real-life experiences and approaches to sharing their own sensitive information.

**Pilot study.** We conducted a pilot study to calibrate our user study design and protocol (e.g., duration, resources, response to technology failure). We used the common practice of convenience sampling [134]; selecting colleagues and friends (n=6: 3 novices and 3 non-novices).

**Data analysis.** We recorded all study sessions. We then asked a UCL-approved transcrip-

---

3 We explore users’ mental models and perceptions of secure – mainly, end-to-end encrypted – communications in detail in the following chapter.
tion service to transcribe the audio recordings. Two researchers (Kat Krol and I) analyzed and coded all transcripts using Thematic Analysis [150]. First, we independently coded five transcripts and created their codebooks. We then met to discuss the themes and the most suitable codes to capture them. I then unified the codebooks into one. Kat and I used the unified codebook to analyze and code the 22 transcripts in batches, meeting weekly to discuss the meaning of participant statements, by adding, removing, and merging codes. The results we present in Section 5.3.1.2 reflect the themes that Kat and I agreed on.

5.3.1.2 Results

First, we describe our participant demographics. Second, we report the SUS scores provided by our participants to assess the usability of Telegram. Third, we present the key themes that emerged across both the ‘think-aloud’ task scenario and the post-task interviews. We report how many participants mentioned each theme to give an indication of the frequency and distribution of key points. Discussion was participant-led, meaning that the frequency of a specific theme may be lower than the frequency of that theme in real life; a participant not mentioning a belief does not mean that they did not hold that belief. We use the following prefixes: ‘PN’ for novices and ‘PU’ for non-novices.

Participant demographics. Overall, 22 participants took part in our study: 12 female participants (six novices and six users) and 10 male participants (five novices and five users). Mean age was 31 (range: 19–75). Four completed high-school education, 14 had an undergraduate degree (e.g., B.A., B.Sc.), and four had a higher degree (e.g., M.A., M.Sc., Ph.D.). Our participants used several communication tools on three computing platforms: Android (14), iOS (7), and Microsoft Windows (1). Table 5.1 summarizes the demographics of our sample.

SUS. We asked participants to complete the SUS questionnaire, facilitating a quantitative comparison of perceived usability across participants, especially given that we interviewed both first-time users and prior/current users of Telegram. Table 5.2 shows the SUS scores for both participant groups: novices and non-novices.
Bangor et al. analyzed 2,324 SUS surveys from 206 usability tests over a ten-year period, and derived a set of acceptability ranges (‘not acceptable’, ‘marginal’, and ‘acceptable’) to generally describe the usability perceived by users [161]. Later, a letter-grade scale (A, B, C, D, and F) was used to interpret SUS scores. Bangor et al. also associated specific ranges of SUS scores with adjective descriptions (e.g., excellent, good, poor). In our study, Telegram’s SUS scores of 83.4 (novices) and 81.8 (users) indicate that Telegram has “excellent” usability (letter grade: B). The difference between the scores of the two groups of participants was not statistically significant (unpaired t-test, $t = 0.36$, $p = 0.72$).
5.3. Methodology

Adoption and abandonment of Telegram. We asked the prior users of Telegram to tell us the story of how they adopted the tool. For seven of them, the tool was suggested to them by one of their contacts. Eight participants said that they explicitly chose it for reasons related to security. For example, PU06 used Telegram when taking part in a protest: “People at the time downloaded Telegram to send messages to talk about situations at their sites.”

Three participants stated that they tried Telegram out of curiosity. Nine participants associated Telegram with low popularity and saw this as an obstacle to continued use. PU04 explained: “I personally would prefer to move to Telegram because I don’t like Facebook as a company, but... so few people use it that I’m still stuck using WhatsApp for most things.”

Out of 11 prior/current users of Telegram, seven stated that they used Telegram for casual conversations rather than sensitive content, and seven mentioned that they used the tool to keep in touch with some of their contacts who were using Telegram exclusively. Six users of Telegram mentioned that they stopped using the tool because it did not support voice calls, as opposed to WhatsApp and Viber.

Upon arrival to the laboratory, we asked prior users of Telegram if they still had Telegram installed on their phone. Six stated they had uninstalled it, whereas four said that they still had the tool on their phone due to having sufficient storage space to be able to keep it there.

Secret Chat. Eight out of 11 novices did not encounter the Secret Chat mode during the initial exploration, despite encouragement to explore Telegram and assurance that they could take as much time as they felt was necessary to do so. The other four novices believed tapping on a contact’s name, to begin messaging them, would enter the Secret Chat mode, not the default chat mode (as we also uncovered during the usability inspection described in Section 5.3.2).

Five participants (three novices and two users) associated Secret Chat with one-to-one chat; i.e., a private chat mode to message only one person rather than multiple users.
Telegram’s default mode supports group conversations, whereas Secret Chat does not. PN05 questioned whether “the recipient uses the Secret Chat mode” if the sender initiates a Secret Chat session, viewing the modes as options that senders and recipients could choose from independently. PU16 believed they had always been using the Secret Chat mode for group chats, despite that the mode does not support group communications.

Starting a Secret Chat session with a contact prompts a list of the mode’s security features, specifically: “use end-to-end encryption,” “leave no trace on our servers,” “have a self-destruct timer,” and “do not allow forwarding” (see Figure 5.3b). Below, we review participants’ perceptions of these features. We also discuss participants’ views on verification fingerprints.

1) Using end-to-end encryption. Out of 22 participants, 20 (11 novices and nine non-novices) told us that they had heard of the term “encryption.” Two participants (PU16 and PU17) stated they did not know what encryption meant.

When asked about encryption, six participants (three novices and three non-novices) provided explanations relating to security and safety. These included “an extra barrier of security”, “more time is needed to know the content of the message”, and “making chats safe from hacking until they get deleted from the servers.”

Regarding the barrier analogy, some participants variously referred to encryption as “a security blanket around the message”, “a password to unlock the message”, “hiding the message in a box”, “a message protected by a series of programs”, “covering the IP address of devices”, “a message cannot be intercepted by other people”, and “a thread or tunnel is used to exchange messages through.” The capacity to see what is in a message was also alluded to by a number of participants, such as “writing a message in a way only the sender and recipients can understand”, “sending a message in a different format”, “using all sorts of numbers to jumble up the message”, “looking like gobbledygook to people outside”, “seeing a bunch of signs that do not make sense when reading an encrypted message”, and “turning the language into something else for reading the other device.”
Overall, 17 participants (nine novices and eight non-novices) offered explanations for what the ‘ends’ were in end-to-end encrypted communications, including: sender and recipient; sender and recipient’s phones; sender and Telegram’s server; the start and end of a message body.

In terms of the role of encryption in protecting messages, participants variously mentioned that a person who did not have the phone number could not read the message, that a special piece of software (not Telegram) was necessary to decrypt a message, and that encryption was ineffective against people sitting next to the sender/recipient. We found that 20 participants believed “some entities” could access and read end-to-end encrypted messages. These entities included government agencies, Telegram’s service providers (sometimes referred to as “staff”), competing companies (e.g. Apple, Google), and tech-savvy people (sometimes referred to as “hackers” by our participants).

We explore user mental models of end-to-end encrypted communication tools in detail in the next chapter.

2) Leaving no trace on servers. Out of 22 participants, one novice (PN07) linked “no traces” to protecting the meta-data of communications, stating that Telegram claimed to protect meta-data including users’ online/offline status, their location, the identities of the communicating parties, and how many messages had been exchanged. The 21 remaining participants believed that leaving no traces on servers meant that exchanged messages would not be stored on Telegram’s servers, confusing it with the functionality of the self-destruct timer, which we discuss next.

3) Having a self-destruct timer. Telegram claims that messages sent via Secret Chat can (in principle) self-destruct, that is, disappear from both the sender and recipient’s devices after a period of time with no copy of exchanged messages persisting on Telegram’s servers. 12 participants (seven novices and five non-novices) said that Secret Chat’s self-destruct timer was useful for sending sensitive information, but not for daily conversations (where ‘daily’ was regularly equated to the conversation being trivial). Similarly, the capacity to keep a log of exchanged messages (the ‘chat history’) was seen as important. Several participants believed that message expiry was defeated by the capacity to take a
picture of their phone’s screen (including timed messages). All prior users of Telegram explicitly mentioned that they had not set up the timer for sending a message. Some participants (three novices and seven non-novices) also doubted how effective the feature was because, as PN05 put it, “the practical thing is that nothing in electronic media is ever destroyed.”

The understanding of what the self-destruct timer did varied across participants: some thought that all their previous messages would be destroyed once a timer had been set up, whereas others were unsure if the messages would also be deleted from the recipient’s phone (as likened to Facebook Messenger). Similarly, there was confusion as to whether both the sender and recipient would have to forcibly or bilaterally set up the timer to the same amount of time, and whether the timer was applicable to group conversations. PN11 believed the default chat mode should have a self-destruct timer, instead of the timer being exclusive to Secret Chat, judging sensitivity on a message-by-message basis: “First of all, if it’s encrypted for all messages, which would be safer and more useful and then if the timer is made available on a regular chat and if you need to use it, you use it; otherwise you don’t.

4) No forwarding. 17 out of 22 participants (six novices and 11 non-novices) considered the “no forwarding” feature as not useful because messages could still be copied and pasted, and taking screenshots was possible (where Telegram v3.16.1 detected the taking of screenshots, but did not prevent it).

5) Verification fingerprints. When the user taps on a contact’s name within the Secret Chat mode, a screen entitled “Encryption Key” is presented, as shown in Figure 5.6. Public-key fingerprints are used for verifying the identities of communicating parties. All 22 participants were unsure of the usefulness of fingerprints, where all 11 users of Telegram had not used this feature despite their experience with the tool. They variously speculated that the image was the encrypted message sent to the recipient, the key used to encrypt/decrypt, or a sign that messages sent via the Secret Chat mode were end-to-end encrypted.
Comparison of chat modes. When we asked participants to send fabricated payment card numbers to their mock colleague (as per the task scenario described in Section 5.3.1), seven novices sent it via Secret Chat, and four used the default chat mode. In the group of Telegram non-novices, two participants used the Secret Chat mode while nine used the default chat mode.

We asked participants to tell us if they saw any differences between the two chat modes in Telegram. Overall, 17 participants said that the Secret Chat mode was more secure than the default chat mode, and nine pointed at the four features that the Secret Chat mode advertised to its users. 12 participants speculated that the default chat mode offered no encryption of messages, whereas two participants expressed hope – rather than pointing to particular listed features – that the default chat had some form of encryption. Furthermore, three participants stated that the default chat mode had some encryption, but that it was weaker than that of the Secret Chat mode. 11 participants stated that only the timer was the distinguishing feature that made the Secret Chat more secure. Five participants stressed that the default chat mode was equivalent to other communication tools, such as WhatsApp.

Eight users of Telegram stated that they had never used Secret Chat, and five stressed that they did not feel they communicated information that was sensitive enough to warrant using it. Seven participants also mentioned that Secret Chat was not useful because it did not support group conversations.

Sharing of sensitive information. After the scenario tasks, we asked participants if they had ever used a communication tool to share their own payment card numbers – or any other information that they regarded as sensitive – with others in real life. Most participants had experience with sharing payment card numbers with others, where participants preferred in-person sharing. 11 out of 22 participants stated that they had shared sensitive information over the phone. Eight of them argued that phone calls were more secure than text messages, and three perceived calls as being more secure than email messages. Otherwise, three participants reported splitting up information into segments and then sending the segments using different communication methods to the same recipient, or using the
same method to several different recipients (e.g., family members).

**Secure communications.** The discussions around the two chat modes and encryption often led to more general questions of what “secure communications” meant to our participants. Out of 22 participants, 13 equated security with confidentiality. For PU2, “security” meant “the fact you can send something to someone without somebody else, even if they know you.” Specifically, three participants took security to mean making sure the right person was receiving their messages.

**Comparison with other communication tools.** Overall, 21 participants made some comparison between Telegram and other messaging tools during the session. 16 participants (eight novices and eight non-novices) stated that it was similar to WhatsApp, where 10 of these found the user interfaces to be very similar. PN09 wondered if Telegram and WhatsApp were developed by the same company, whereas PU06 stated: “I basically think Telegram is a fake version of WhatsApp. I don’t know, everything is similar. With some… other functions that are not relevant to me.” 15 participants (nine novices and six non-novices) believed that Telegram had more options than WhatsApp. Four participants described Telegram as faster, and three of them mentioned photo downloads being smoother. In terms of security, 12 participants (eight novices and four non-novices) felt that Telegram was more secure than WhatsApp.

**Security and privacy settings.** Telegram has several security and privacy settings; some are analogous to features found in other popular messaging tools, such as WhatsApp and Facebook Messenger. These settings include the ability to block contacts, a visible “last seen” status for contacts, and active sessions. Here, we explore participants’ perceptions of three security-specific functions: passcode, two-step verification, and account deletion.

All but one participant (PN09) believed that a passcode was used to lock their Telegram account, whereas PN09 associated passcodes with specific chat sessions. Eight participants, four in each group, felt that a passcode would provide “extra security;” however, two novices and three users saw the feature as lacking usefulness because the participant could not know who the sender was, and what the content of the messages received was.
Forgetting a passcode was seen as a risk, resulting in the loss of prior messages and a need to reinstall Telegram. Eight novices implied that they would set a passcode, whereas nine users of Telegram had not done so, seeing the phone lock of their handset as sufficient (i.e., Apple’s Touch ID or passcode, Android’s pattern/PIN lock).

Telegram has an optional two-step verification feature to further verify users when logging into their accounts from a new device (in addition to the verification code). However, only two novices and one non-novice understood the two-step verification feature after reading the description of the feature on the screen. 17 participants (eight novices and nine non-novices) equated this feature with two-factor authentication, seeing it analogous to having an additional password for online banking and email accounts. Based on this belief, participants said that setting two passwords was “a hassle” (PU18), and “having one password [was] enough” (PU20). PU21 believed that the feature was used to reset a password, which may be attributed to them not having used the feature before. None of the 11 prior/current users of Telegram had used this security feature before.

Telegram allows users to delete their accounts, and accounts are automatically deleted after a period of inactivity. Although five novices and one user perceived the feature as useful, many participants (six novices and ten users) would prefer to receive a notification that their account would be deleted. Several participants believed that uninstalling a tool would also remove their account; five participants expressed a wish to keep a copy of their chat history.

5.3.2 Usability Inspection

5.3.2.1 Method

Usability inspection has seen increasing use since the 1990s as a way to evaluate the user interface of a computer system [162]. Usability inspection is aimed at finding usability problems in the user interface design and evaluating the overall usability of an entire system. Unlike empirical user studies, a user interface is inspected by developers and evaluators without engaging users (i.e., without recruiting participants to assess the us-
Evaluating a design with no users are present can identify problems that may not necessarily be revealed by an evaluation with users [162–165]. Although it is important to bring users into the design process, evaluating a design without users can also provide benefits [163].

There are several usability inspection methods. In this work, we use a hybrid approach combining cognitive walkthrough and heuristic evaluation. Both methods are actively used in human-computer interaction (HCI) research [166]. We also examined the usability of Telegram using the seven foundational principles of Privacy by Design, as defined by Cavoukian [167].

**Cognitive Walkthrough.** Cognitive walkthrough is a usability inspection method that focuses on evaluating a user interface design for its exploratory learning, a key aspect of usability testing [168] based on a cognitive model of learning and use [57, 169, 170]. First-time users of a system may prefer to learn how to use it by exploring it, rather than investing time in comprehensive formal training or reading long tutorials [171,172]. Cognitive walkthrough identifies problems that users could have as they approach an interface for the first time. It also identifies mismatches between how users and designers conceptualize a task, as well as how designers make assumptions about users’ knowledge of a specific task (which could, for example, impact the labelling of buttons and icons).

Cognitive walkthrough is task-specific, studying one or more user tasks. The process comprises a preparatory phase and an analysis phase. In the preparatory phase, evaluators decide and agree on the input to the cognitive walkthrough process: (1) a detailed description of the user interface, (2) the user interface’s likely user population and context of use, (3) a task scenario, and (4) a sequence of actions that users need to accurately perform to successfully complete the designated task. In the analysis phase, evaluators examine each of the actions needed to accomplish the task. The cognitive walkthrough process follows a structured series of questions, derived from the theory of exploratory learning, to evaluate each step (or action) in the workflow. A detailed overview of the cognitive walkthrough process can be found in [170].
5.3. Methodology

Heuristic Evaluation. In 1990, Nielsen and Molich introduced a new method for evaluating a user interface, called heuristic evaluation [58, 162]. Heuristic evaluation involves having usability evaluators judge dialogue elements in an interface against established usability principles (“heuristics”). The use of a complete and detailed list of usability heuristics as a checklist is considered to add formalism. Jeffries et al. found that heuristic evaluation uncovered more issues than any other evaluation methods, whereas empirical user studies revealed more severe, recurring, and global problems that are more likely to negatively affect the user experience of a system [173].

The ten heuristics are as follows:

1. Visibility of system status: The system should always convey its status to its users. Appropriate feedback translates to better decision-making.

2. Match between system and the real world: The system should speak the users’ language.

3. User control and freedom: The system should enable users to easily undo unwanted actions.

4. Consistency and standards: The system should maintain a consistent vocabulary.

5. Error prevention: The system should prevent users from making unconscious errors.

6. Recognition rather than recall: The system should minimize users’ memory workload by promoting recognition over recall in the user interface design.

7. Flexibility and efficiency of use: The system should allow fast interaction.

8. Aesthetic and minimalist design: The system’s user interface design should not contain irrelevant or unneeded information.

9. Help users recognize, diagnose, and recover from errors: Error messages should clearly explain what the problem is, and then suggest a workable solution.

10. Help and documentation: Necessary information should be easy to search and find.
Hybrid Approach. To avoid biases inherent in either of the usability inspection methods, we used a hybrid approach combining two of the most actively used and researched methods: cognitive walkthrough and heuristic evaluation. Combining both task scenarios and heuristics was recommended by Nielsen [174] and Sears [175]. The hybrid approach is as follows:

1. Provide a detailed description of the user interface.
2. Define the users and their goals.
3. Define the tasks the users would attempt (e.g., sending a message).
4. Break each task into a sequence of sub-tasks or actions (e.g., hitting the “Send” button).
5. Walk through each task workflow step-by-step through the lens of the users (e.g., what they would look for, what paths they would take, what terms they would use).
6. For each action, look for and identify usability problems based on the ten heuristics described above.
7. Specify where the usability problem is in the user interface, how severe it is, and possible design fixes.

Two researchers (my colleague Kat Krol and I) used the hybrid approach and inspected the user interface of Telegram. The researchers did so independently before discussing the findings. A third researcher (my colleague Simon Parkin) read the evaluation reports, identifying usability issues in each report and then aggregating all the uncovered issues in a larger set.

Privacy by Design. In addition to using the hybrid approach to assess the user interface of Telegram, we used the seven foundational principles of Privacy by Design, as defined by Cavoukian [167]. The principles advocate that systems should be designed with the preservation of privacy as a requirement, and that settings that ensure security and privacy should be the default.
The seven principles are as follows:

1. Proactive not reactive; preventative not remedial: The system should prevent privacy-invasive events before happening.

2. Privacy as the default setting: Privacy should be built into the system by default.

3. Privacy embedded into design: Privacy should be an integral part of the system, and not an add-on.

4. Full functionality – positive-sum, not zero-sum: System designers should not support the pretence of false dichotomies, such as believing there is an inherent trade-off between usability and security.

5. End-to-end security – full lifecycle protection: The system should support strong security measures, from start to finish.

6. Visibility and transparency – keep it open: The system’s component parts and functions should always be open to both users and providers.

7. Respect for user privacy – keep it user-centric: The system should offer user-friendly and privacy-by-default options.

5.3.2.2 Results

We used a hybrid approach combining cognitive walkthrough and heuristic evaluation to assess the usability of Telegram based on a set of tasks. In any messaging tool, users perform two core tasks: sending and receiving messages [41]. In a secure messaging tool, users may need to perform additional security tasks, such as manually encrypting/decrypting or digitally-signing messages. However, Telegram secures messages without any user interaction. Hence, our focus is on evaluating the two core tasks of sending and receiving messages, as well as the security- and privacy-related settings offered

---

4 Telegram messages exchanged within the default chat mode are by default client-server/server-client encrypted, whereas those exchanged within the Secret Chat mode are by default end-to-end encrypted.
by Telegram. We evaluated Telegram v3.16.1 on iPhone 6 (iOS 10.1.1) and Nexus 6 (Android 6.0.1). We did not find any meaningful differences for the tasks studied between the two devices.

As shown in Figure 5.2, the user is presented with three ways of sending a message: “New Group,” “New Secret Chat,” and “New Channel.” However, tapping on a contact’s name in the list underneath (here: Kat) directs the user to the default chat mode (the less secure mode), without giving them the option to choose between the default chat mode and the Secret Chat mode. Further, the default chat mode is not listed as one of the three ways of sending a message, but is activated once the user taps on the contact’s name. This violates Nielsen’s heuristic of visibility of system status, which stresses the system should always keep the user informed about what is happening.

![Figure 5.2: Options to send a message in Telegram.](image)
5.3. Methodology

When starting a Secret Chat session with a contact (here: Kat), Telegram provides a list of the security features offered by this mode (see Figure 5.3b on page 150). The four bullet points state that Secret Chats “use end-to-end encryption,” “leave no trace on our servers,” “have a self-destruct timer,” and “do not allow forwarding.” The terms used in these bullet points assume users’ familiarity with technical terminology. Additionally, there is no direct link to further explanation next to each point. This violates Nielsen’s heuristic of match between system and the real world, which states that the system should speak the user’s language, with words, phrases, and concepts familiar to the user, rather than system-oriented terms [166] – as seen in Section 5.3.1.2, where participants differed in how they perceived and articulated security terminology.

The security properties of the default chat mode are also not clear (see Figure 5.3a). Once the user starts exchanging messages, the visible difference between using the default chat mode and the Secret Chat mode is minimal. Further, as shown in Figure 5.4a and Figure 5.4b, there is only a small padlock symbol to the left of the contact’s name in a Secret Chat session. This also violates Nielsen’s heuristic of visibility of system status, as described above.

To start a Secret Chat session with someone, both communicating parties (i.e., sender and recipient) need to be online for the two participating devices to exchange keys (see Figure 5.5). However, this may push the user to send messages within the less secure default chat mode if their contact is not online. The Secret Chat mode also does not support group communications, which could further undermine the mode’s usefulness (especially, its utility).

When the user taps on the contact’s name within the Secret Chat mode, a screen entitled “Encryption Key” is presented (see Figure 5.6). Displayed is a square image containing smaller squares of different shades of blue. There are also four lines of characters and numbers below the square image. The explanation found underneath states that both the image and the alphanumeric lines were derived from the encryption key for the Secret Chat with ‘Kat.’ In this case, if the representations on both the sender and recipient’s (here: Kat’s) devices are the same, “end-to-end encryption is guaranteed.”
Chapter 5. The Security Blanket of the Chat World

(a) Default chat mode.  
(b) Secret Chat mode.

Figure 5.3: The security properties of the default chat mode are not described (unlike the Secret Chat mode).

Telegram uses the term “Encryption Key” to describe fingerprint verification. This could lead users to incorrectly think that the fingerprint is the encryption key used to encrypt Telegram messages. When a Secret Chat session is initiated, an image and a textual representation are generated on both the sender and recipient’s devices, visualizing their public-key fingerprints. The two communicating parties can verify each other’s identity by comparing both representations through a trusted channel (e.g., in-person). If the representations match, then the session is secure, and no man-in-the-middle attack has occurred.

Finally, under the “Security and Privacy” settings, the user can set up a passcode (4-digit pin) to lock their Telegram application. However, we found that when Telegram is locked, the user can receive notifications about messages without the sender’s name
Figure 5.4: Sending a message in Telegram’s default chat mode (left) and Secret Chat mode (right). The only difference is the small padlock to the left of the contact’s name (here: Kat).

and text. Another usability issue related to locking the application is that the user can either “auto-lock” the application after a specified period of inactivity or manually lock the application from the screen, which is not explained to the user at the time of enabling the lock (see Figure 5.7b and Figure 5.7a).

We also examined Telegram using the seven foundational principles of Privacy by Design. We found Telegram violated six out of the seven principles of Privacy by Design. The second principle (privacy as the default) states that privacy should be built into the system by default, whereas in Telegram the user is guided towards the less secure, less private default chat mode. This feature also violates the sixth principle (visibility and transparency) due to the minimal feedback the user gets when they start chatting in the
If the user decides to choose the *Secret Chat* mode, they will not enjoy full functionality due to the mode’s lack of utility; the other party has to be online when initiating a *Secret Chat* session, and group conversations are not possible, violating the third (*privacy embedded into design*) and fourth (*full functionality*) principles. Telegram also violates the fifth principle (*end-to-end security*); it does not provide full-lifecycle protection because the default chat mode is not end-to-end encrypted.

Finally, Telegram is in violation of the seventh principle (*keeping it user-centric*) due to technical jargon and inconsistent use of terminology, as we explained above.
5.4 Discussion

The study of both novices and non-novices is invaluable; the SUS scores indicate that both groups perceived Telegram as a highly usable communication tool. Nevertheless, we found many non-novices had stopped using Telegram because – in most cases – it lacks utility: it has a small userbase and the Secret Chat mode does not support group communications. In this sense, communication is a naturally social practice, where peer influence governs the adoption and use of communication tools [63, 66].

Visible security can increase trust in a security system (e.g. [59, 60]); our results indicate that making some security properties visible, while at the same time leaving others as invisible could easily create confusion for users. Many participants believed

---

**Figure 5.6:** A verification fingerprint.
that both the default chat and the Secret Chat modes offer the same security properties, except for the self-destruct timer which was regarded as the most visible feature of the Secret Chat mode (and as such the only indicator of the security level of that mode). Having two chat modes with different levels of security and, at the same time, making the less secure mode the default could lead users to confusion and error. Hence, we encourage designers and developers of secure communication tools to follow the design principles proposed by Nielsen and Molich [58] as well as those proposed by Cavoukian [167].
5.5 Limitations

The design of the task-based scenario (in the first part of the study) did not involve a real risk for participants, where we asked them to run a fictional small business and send financial details that were randomly-generated using Telegram, to complete a mock purchase. We believe an element of personal risk in the task might have motivated participants to give consideration to more secure behaviours and maybe use the Secret Chat, instead of the default chat, mode [176]. Here, the study tasks were considered more as an opportunity for participants (especially novices) to learn about Telegram and promote further discussion of its security features.

Further, our findings show that participants described technical terms/concepts (e.g., end-to-end encryption) in different and interesting ways. We had to take care not to introduce further technical jargon into the conversation with participants before they had the chance to frame concepts in their own words. In the next chapter, we explore user mental models and understanding of end-to-end encryption in detail.

5.6 Contributions to Thesis

In this chapter, we designed and conducted a three-part study – (1) a laboratory-based user study (n=22: 11 novices and 11 Telegram users or participants with prior experience of using Telegram); (2) a hybrid analytical approach combining cognitive walkthrough and heuristic evaluation, focusing on inspecting the user interface of Telegram (with no participants recruited); (3) a survey (n=300 respondents) – to answer the third research question this thesis addresses: How does lack of utility negatively influence the use of a usable and secure communication tool (see Section 1.2)? We showed how users’ goal and ability to reach all their communication partners in a timely-manner when using a secure messenger override everything else, including both usability and security. Alarmingly, most non-novice participants developed the habit of using the less secure default chat mode of Telegram, incorrectly believing they were using Telegram in a secure way. This is mainly due to Secret Chat’s lack of utility. Secret Chat does not support group conversations. Further, the communicating parties (sender and recipient) need to be on-
line at the same time when they initiate a *Secret Chat* session. Hence, the sender cannot reach their communication partner in a timely-manner, hindering the adoption and use of *Secret Chat* mode.
Chapter 6

Adoption Is Necessary, But Not Sufficient: Exploring User Mental Models of End-to-End Encrypted Communication Tools

In previous chapters, we showed how poor usability and lack of utility are primary obstacles to the adoption of secure communication tools. In this chapter, we describe the third class of obstacles to the adoption of secure communications: incorrect mental models and misperceptions. We design and conduct a quantitative survey (n=125 respondents) to examine the role user mental models and perceptions play in the adoption and use of secure (especially, end-to-end encrypted) tools. We assess users’ general mental models and understanding of a hypothetical end-to-end encrypted communication tool, named Soteria. We find the vast majority of survey respondents had adopted usable end-to-end encrypted communication tools (mainly, WhatsApp) in the real world, but lacked confidence and accuracy in their mental models of end-to-end encryption. Two key misconceptions include: (1) three-quarters of respondents incorrectly believed that their end-to-end encrypted communications could be easily accessed by unauthorized entities (e.g., governments, creators of tools); (2) one-half of respondents incorrectly felt that SMS and landline phone calls were more secure than, or at least as secure as, end-to-end encrypted
communications. These findings suggest that most users do not know what it means for a usable and secure messenger that is widely-adopted and offers the utility users look for, such as WhatsApp\(^1\), to be end-to-end encrypted. Hence, we argue that the primary user-related challenge for end-to-end encrypted communication tools is not only fostering adoption, but also emphasizing appropriate use – by helping users who have already adopted an end-to-end encrypted tool avoid sending information, especially information they regard as sensitive, over less secure channels that they incorrectly perceive as more secure than their encrypted tool.

The rest of this chapter is structured as follows:

• Section 6.1 describes the research objectives of this study.

• Section 6.2 describes our survey design and instrument.

• Section 6.3 presents the findings of our survey.

• Section 6.4 discusses the findings of our survey and shows why emphasizing appropriate use, and not fostering adoption, of end-to-end encrypted communication tools is the key user-related challenge for secure communications.

• Section 6.5 summarizes the chapter.

• Section 6.6 describes the principal limitations of the study.

• Section 6.7 describes the contributions this chapter makes to the thesis.

The content of this chapter is an edited version of the following publication:


Appendix D contains supplementary (in particular, the survey questionnaire) for this chapter.

---

\(^1\) WhatsApp is not necessarily a secure – in this case, end-to-end encrypted – tool. However, it was chosen as an example.
6.1 Introduction

Secure communication tools empower people to resist surveillance. Encrypted email was one of the first forms of secure communications. It was followed by Off-the-Record (OTR) messaging [42], which then spawned a variety of secure instant messaging tools (e.g., Signal). Such tools offer various security properties, such as confidentiality (secrecy of communication), integrity (accuracy and completeness of communication), and user authentication. Secure communication tools are critical for activists, journalists, and others who seek to avoid corporate or government surveillance.

In Chapter 3, we showed that users’ incorrect mental models – e.g., most participants believed secure communications were futile – are a key obstacle to the adoption of secure communication tools. We qualitatively explored users’ familiarity with secure communication tools and gaps in their mental models. In this chapter, we quantitatively validate and expand on these findings. We do so by studying both users and non-users via a quantitative survey through which we assess people’s mental models and perceptions of end-to-end encrypted communication tools and their security properties. We specifically focus on one type of secure communications, end-to-end encrypted communications, abstracted away from detailed predispositions of any specific tool created by any particular brand in the real world.

To this end, we surveyed 125 respondents about a hypothetical end-to-end encrypted communication tool, named Soteria\(^2\). The description of our hypothetical tool was based on a systematic review of the descriptions of 20 real communication tools that are end-to-end encrypted or are advertised as such (e.g., Signal, Telegram, WhatsApp); we chose this method in order to minimize bias from brand-based perceptions of specific tools. Using this hypothetical tool as a foundation, we explored people’s understanding of end-to-end encryption and the security properties of end-to-end encrypted communication tools.

We found that the majority of our survey respondents (90%) used at least one end-to-end encrypted communication tool, most frequently WhatsApp. Yet, only 12% felt

\(\footnote{We named our hypothetical communication tool “Soteria” after the Greek goddess of safety and salvation, deliverance, and preservation from harm.}\)
they could confidently explain end-to-end encryption – only 20% of those provided an accurate explanation. Most surprisingly, only one-quarter of our respondents believed that no one could compromise the security of communications in our hypothetical tool. This is concerning because a belief that end-to-end encrypted tools are already insecure could mislead users about the danger of proposed measures that would build in insecurity (e.g., backdoors). In other words, this belief suggests that users may not feel threatened by proposals of backdoors because they already believe that different unauthorized entities could access their end-to-end encrypted communications.

Further, one-half of respondents incorrectly felt that SMS and landline phone calls would be more secure than, or as secure as, end-to-end encrypted communications. Such misunderstandings could lead users to unknowingly select insecure communication tools in situations where they most require privacy. In some cases (e.g., activists communicating under threat of imprisonment or death), such mistakes could be life-threatening.

Overall, our findings suggest that end-to-end encrypted communication tools are widely-adopted but not accurately understood. Thus, the key struggle for end-to-end encrypted tools is not only fostering adoption, but also emphasizing appropriate use – by helping users of end-to-end encrypted tools send sensitive information using only these secure tools.

### 6.2 Methodology

In this section, we describe the research questions we address in our study, recruitment process, survey methodology, and details of our data analysis. We designed and conducted an online survey of 125 respondents in the UK in April 2018. Our UCL’s Research Ethics committee reviewed and approved our study (project no.= 12567/001). We handled all collected data in accordance with the UK Data Protection Act 1998 (registration no.= Z6364106/2018/01/06).
6.2.1 Research Questions

In this study, we answer the following research questions:

- **RQ1**: What are users’ general mental models of end-to-end encryption?
- **RQ2**: How do users perceive the security properties of end-to-end encrypted communication tools?

6.2.2 Recruitment

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

6.2.3 Survey Method

We developed our survey questionnaire through an iterative process, as we describe below.

6.2.3.1 Survey Structure

We asked respondents to answer questions about a hypothetical end-to-end encrypted communication tool. We chose to use a hypothetical tool to avoid bias from respondents’ preconceived notions of specific tools or tool providers (in the real world). We introduced respondents to this tool using the following description: “Imagine you are considering using a new tool named Soteria to communicate with your family members, friends, work colleagues, and others. When you install Soteria, the following message is displayed: ‘Soteria communications (messages, phone calls, and video calls) are end-to-
We constructed the Soteria message (i.e., the italicized text above) by conducting a cognitive walkthrough of the user interface of 20 different communication tools included on the EFF Secure Messaging Scorecard. Cognitive walkthrough is a usability inspection method actively used in human-computer interaction to identify and evaluate design components [57]. Using cognitive walkthrough, we inspected the user interface of the following tools: AIM, BlackBerry Messenger, Facebook Messenger, FaceTime, Google Hangouts, Hushmail, iMessage, Kik Messenger, QQ, Signal, Skype, Snapchat, Telegram, Threema, Viber, WeChat, Weibo, WhatsApp, Wickr, and Yahoo! Messenger. We chose these tools because some of them are (or at least used to be) popular and/or are advertised as “secure,” “private,” or “end-to-end encrypted.” In our case, we sought to identify how information about message security and privacy was conveyed to users in the real world. For example, WhatsApp advertises itself as end-to-end encrypted by displaying a message when the user begins chatting with their contacts. The displayed message explains that communications exchanged using WhatsApp “are secured using end-to-end encryption.” Hence, we worded the Soteria display message to closely match wording used by the majority of tools (e.g., WhatsApp, Telegram) to advertise, or provide feedback to users, about the security of their communications.

We asked respondents to answer a list of questions about Soteria based on one of the scenarios below (which we randomly assigned to each respondent) to determine whether respondents’ answers would vary based on the described context of use:

- Chatting (not necessarily gossiping) and making plans with family members, friends, or work colleagues.
- Sharing account credentials (e.g., usernames, passwords, PINs) with family members, friends, or colleagues. Examples of accounts include personal email account, personal banking account, or personal payment account (e.g., PayPal, Venmo).
- Discussing salary with work supervisor.

---

3 See Section 3.1 for an overview of the EFF Scorecard.
4 See Section 5.3 for a detailed description of cognitive walkthrough.
• Discussing politics.

• Buying/selling illegal substances (e.g., drugs).

• Whistleblowing – a whistleblower is an employee who reports their employer’s misconduct (e.g., an illegal or unethical activity).

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

Our survey aims to assess the following constructs:

**General mental models of end-to-end encryption.** First, we aimed to investigate respondents’ mental models (conceptual understanding) of end-to-end encryption (see RQ1 in Section 6.2.1). To do so, we asked whether respondents had heard of the term “end-to-end encryption,” and if so, whether they felt confident explaining what the term meant. We then asked them to explain what it meant for communications to be “end-to-end encrypted” and what the ends in “end-to-end encryption” referred to.

To assess the mental models of communication tools that are end-to-end encrypted, we asked respondents whether different types of communication (e.g., landline phone calls, mobile phone calls, SMS, email) are as secure as Soteria text messages. Further, we investigated whether or not respondents’ familiarity with end-to-end encrypted communication tools affected the robustness of their mental models. Thus, we asked respondents to list the communication tools they regularly used, as well as those they believed they had the same security guarantees as our hypothetical tool, Soteria.

**Security properties of end-to-end encrypted communications.** Second, we aimed to explore our respondents’ understanding of the security properties offered by end-to-end encrypted communication tools with regards to confidentiality, integrity, and authentication (see RQ2 in Section 6.2.1). Hence, we asked respondents about the entities, if any, who could read their Soteria messages, listen to their Soteria phone calls, modify the content of their Soteria communications, and/or impersonate them (i.e., communicate with others using their Soteria account). We provided respondents with examples of different
entities (e.g., people who work at Soteria, people with a technical background, people who are up to no good, corporations other than the company that develops Soteria, Internet service providers (ISPs), governments). We also asked respondents how they would verify the identity of a communication partner in Soteria.

We refer the reader to Section 2.1 for a technical definition of end-to-end encrypted communications.

**Demographics.** Finally, we included a number of demographic questions about gender, age, race, educational level, and employment status. We aimed to assess whether or not age or education would affect respondents’ answers to our survey questions. We also asked respondents to rate the overall difficulty of the survey.

The survey questions can be found in Appendix D.

### 6.2.3.2 Cognitive Interviews

After developing an initial questionnaire of our survey, we conducted cognitive interviews – a method used to pre-test questionnaires to glean insights into how survey respondents might interpret and answer questions [177] – with 15 demographically-diverse participants (see Table 6.1). The interviewer (I) asked participants to share their thoughts as they answered each survey question. After answering each question, participants were asked the following questions: “Was this question difficult to answer?;” “Was there an answer choice missing?;” “How did answering this question make you feel?” We used the findings to iteratively revise and rewrite our survey questions, to minimize bias and maximize validity.

### 6.2.3.3 Expert Reviews

After the tenth cognitive interview was complete, we asked five human-computer interaction researchers with survey expertise to review our survey questionnaire and evaluate question wording, ordering, and bias. We also asked UCL’s Research Ethics consultant to review the survey. Expert reviewing is a method that complements cognitive interviews
6.2. Methodology

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

Table 6.1: Cognitive interview participant demographics.

in identifying questions that require clarification, as well as in uncovering problems with question ordering or potential biases [177]. Following these expert reviews, we updated some questions and then conducted the remaining five cognitive interviews to ensure no more problems emerged.

6.2.4 Data Analysis

Two researchers (Miranda Wei and I) independently coded qualitative responses to all open-answer questions using Thematic Analysis [150], a common method used to analyze qualitative data sets. Coding was not mutually exclusive; one response could express multiple themes. After coding all responses and creating the final codebook, we tested for the inter-coder agreement (or inter-rater reliability). The average Cohen’s kappa coefficient (κ) for all themes in our data was 0.87. A κ value above 0.75 is considered excellent agreement [138, 139].

Finally, we report responses to closed-answer questions descriptively, except for demographic comparisons (in which we use binomial logistic regression models to evaluate demographic effects, if any).
6.3 Results

We present the results from our 125 UK-based respondents.

6.3.1 Demographics

Table 6.2 summarizes the demographics of our sample (n=125). 40% of respondents identified as male, 58% female, and 2% non-binary. Our sample skewed young; 28% were between 18 and 24 years old, 27% between 25 and 34, 25% between 35 and 44, 8% between 45 and 54, and 12% 55 and above. About one-half of respondents identified as White, one-quarter Black, one-tenth Asian, and 7% mixed-race. 34% of respondents had a college/undergraduate degree and 20% had a graduate/postgraduate degree. 19% reported having high-school education, 12% vocational training, and 11% some post-secondary education (no degree). Young respondents used a wide range of communication tools, as opposed to older respondents who frequently used only one or two tools.

Despite advertising our study broadly and with no mention of security or end-to-end encryption, 90% of our respondents currently used, or had used in the past, an end-to-end encrypted communication tool. The vast majority (87%) of these respondents used, or had used, WhatsApp, which is very popular outside of the United States due largely to its minimal use of cellular data relative to other communication tools. Notably, 89% of respondents used, or had used, at least one end-to-end encrypted tool that is frequently advertised as such (e.g., Signal, Telegram\(^5\), WhatsApp, Wickr). Furthermore, 55.5% of respondents used, or had used, at least one end-to-end encrypted tool that is not frequently advertised as encrypted (e.g., FaceTime, iMessage). Table 6.3 details the tools respondents used, or had used.

6.3.2 General Mental Models of End-to-End Encryption

Although a majority of respondents used/had used a communication tool that is advertised as end-to-end encrypted, only 12% felt confident explaining the term “end-to-end

\(^5\) Telegram does not feature end-to-end encryption by default, but it does advertise end-to-end encryption (see Chapter 5).
6.3. Results

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

Table 6.2: Demographics of survey respondents.

encryption.” Of the 12%, only 3% gave a correct explanation of the term. Further, 50% had heard of the term but did not feel confident explaining it, and 38% had not heard of it at all.

Despite a lack of confidence reported by the majority of respondents (88%) in their knowledge of end-to-end encryption, when we asked whether they would want to use our hypothetical tool (and why), 86% of respondents mentioned that Soteria would be a beneficial tool to use because it offers end-to-end encryption. In particular 22% of respondents explained that end-to-end encryption was a benefit because no third-parties could access Soteria communications, and 20% explained that only the sender and the recipient could access Soteria communications; the remaining 44% provided no further explanation. Furthermore, respondents mentioned that end-to-end encryption made Soteria secure (28%), private (19%), protected (19%), safe (16%), and reliable (1%). Finally, 10% wrote that Soteria could not be “hacked.” A minority of respondents also identified
Chapter 6. Adoption Is Necessary, But Not Sufficient

<table>
<thead>
<tr>
<th>Tool</th>
<th>Currently</th>
<th>Previously</th>
<th>Heard of</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adium</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>ChatSecure</td>
<td>0</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Facebook Messenger</td>
<td>90</td>
<td>22</td>
<td>5</td>
</tr>
<tr>
<td>FaceTime</td>
<td>47</td>
<td>17</td>
<td>43</td>
</tr>
<tr>
<td>iMessage</td>
<td>32</td>
<td>12</td>
<td>25</td>
</tr>
<tr>
<td>Jitsi</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Pidgin</td>
<td>0</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>Signal</td>
<td>5</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Surespot</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Telegram</td>
<td>3</td>
<td>6</td>
<td>20</td>
</tr>
<tr>
<td>Threema</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Viber</td>
<td>1</td>
<td>17</td>
<td>27</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>98</td>
<td>11</td>
<td>17</td>
</tr>
<tr>
<td>Wickr</td>
<td>1</td>
<td>0</td>
<td>9</td>
</tr>
</tbody>
</table>

**Tools that do not support E2E encryption**

<table>
<thead>
<tr>
<th>Tool</th>
<th>Currently</th>
<th>Previously</th>
<th>Heard of</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blackberry Messenger</td>
<td>2</td>
<td>21</td>
<td>58</td>
</tr>
<tr>
<td>Blackberry Protect</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Confide</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>eBuddyXMS</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Google Hangouts</td>
<td>6</td>
<td>12</td>
<td>46</td>
</tr>
<tr>
<td>Instagram DM</td>
<td>29</td>
<td>6</td>
<td>32</td>
</tr>
<tr>
<td>Kik Messenger</td>
<td>2</td>
<td>14</td>
<td>35</td>
</tr>
<tr>
<td>LinkedIn Mail</td>
<td>15</td>
<td>3</td>
<td>32</td>
</tr>
<tr>
<td>Ostel</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>QQ</td>
<td>0</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>Skype</td>
<td>40</td>
<td>47</td>
<td>21</td>
</tr>
<tr>
<td>Snapchat</td>
<td>38</td>
<td>14</td>
<td>47</td>
</tr>
<tr>
<td>Twitter DM</td>
<td>19</td>
<td>16</td>
<td>40</td>
</tr>
<tr>
<td>Yahoo! Messenger</td>
<td>4</td>
<td>23</td>
<td>65</td>
</tr>
<tr>
<td>Other</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 6.3: Respondents’ familiarity with different communication tools, specifically whether they use each tool currently, used it previously (i.e., “used it before, but stopped using it”), or had heard of it (i.e., “had heard of it, but had not used it”). Some tools that support end-to-end encryption offer this mode by default, while others require users to open a special window (e.g., Facebook Messenger’s Secret Conversations).

some of the potential drawbacks of end-to-end encryption: 11% mentioned that the sender and the recipient both needed to use Soteria in order to communicate and 9% were worried that Soteria could be used for evading police or intelligence services in conducting cybercrime, cyber harassment, or terrorism.

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

We then asked respondents to define the “ends” in “end-to-end encryption.” Half of the respondents defined the ends as the sender and the recipient, 15% defined the ends as the communicating devices, and 15% as the two installed instances of Soteria on the sender and recipient’s devices. Interestingly, 15% reported that the ends refer to the start and end of an exchanged Soteria message. Three-quarters of the respondents reported they were not confident they provided the correct answer to this question. We also note that respondents answered all questions in the context of one-to-one communications; there was no mention of group communications.

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

Finally, we also explored whether respondents believed that different types of communication sent using Soteria had equivalent security guarantees. About three-quarters of respondents correctly believed that all types of Soteria communication (text messages, images, file attachments, phone calls, and video calls) would offer the same security guarantees. Additionally, about one-half of respondents incorrectly believed that SMS messages, landline phone calls, mobile phone calls (using cellular data), and email messages were more secure, or at least as secure as, Soteria communications (see Figure 6.1).

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

We asked respondents about the entities that could compromise the confidentiality, integrity, and authentication of communications sent or received with Soteria. Figure 6.2 summarizes their responses. Only one-quarter of respondents believed no one could gain any kind of access (e.g., no one could read, listen, modify, or impersonate) their Soteria communications. A larger proportion (nearly half) thought that someone could gain at least one type of access (e.g., someone could read, but not listen, modify, or impersonate).

Roughly one-third of respondents believed that someone with a technical background or a computer science degree could compromise the confidentiality and integrity of Soteria communications, as well as impersonate users. When asked why, 60% of respondents explained that technical people have the necessary knowledge and skills to learn how an encryption protocol works and, thus, could “reverse-engineer” the protocol to recover the
Furthermore, one-third of respondents believed that Soteria’s security could be compromised by their country’s government (in this case, the UK). Although we did not have a follow-up question to probe, we can speculate that respondents believed this would be possible because governments and intelligence services have the necessary resources and technical expertise to break an encryption protocol. Another reason could be that some respondents were aware of the ability of governments to pressure companies to insert backdoors into secure software and hardware to allow law enforcement agencies to bypass authentication and access data surreptitiously.

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

6.4 Discussion

Our results suggest that a high-level description of a secure communication tool as “end-to-end encrypted” is too vague, and insufficiently informs users of that tool’s security properties. Inappropriate mental models of security derived, at least partially, from such descriptions could lead users to send important and sensitive information over less secure channels that users incorrectly perceive as more secure than an end-to-end encrypted communication tool. In Chapter 3, we found that people use methods they perceive as most secure to communicate sensitive information. Yet, half of our respondents in this study incorrectly perceived communication channels like SMS and landline phone calls to be more secure than, or at least as secure as, end-to-end encrypted communications. These results suggest that even if respondents have installed end-to-end encrypted tools, they may not realize they should be using them at the most security-critical moments.
Therefore, it is critical to communicate the security properties of end-to-end encrypted communication tools. While warning messages have been thoroughly explored in the literature (see Section 2.6), little work has investigated how to design descriptions of pro-security properties. In one of the few examples of work in this space, Ruoti et al. argue that making the ciphertext visible to users after encryption takes place increases user trust in the system [59, 60]. In a similar vein, developers of end-to-end encrypted tools may seek to provide explicit examples or diagrams, illustrating security properties, by, for example, showing how an SMS message could be intercepted, compared to an end-to-end encrypted communication that could not. Furthermore, our findings concur with our findings in Chapter 3, showing that the size of a userbase is crucial for encouraging adoption of a communication tool. Hence, new descriptions might consider communicating, briefly, the size of a tool’s userbase in the tool description to encourage adoption and use.

Further, educational interventions which are included within a particular end-to-end
6.5 Summary and Implications

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

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

Feelings of self-efficacy – which may arise from confidence in the security or privacy a user has gained from tool adoption – have been shown to improve continued use and the ability to protect oneself in other situations [178, 179]. We hypothesize that a sense that third parties can access communications that are supposed to be private may erode such self-efficacy. Thus, while we should be careful to avoid engaging in “privacy theater” [180] – increasing users’ expectations of privacy beyond reality – if users do not feel private or secure when using end-to-end encrypted tools, or do not feel as secure or
as private when using other tools, this may reduce their sense of online well-being and sustained engagement in privacy behaviors [181].

Finally, our community has developed an understanding of user mental models of a variety of privacy-enhancing technologies, including end-to-end encrypted communication tools (e.g., most notably PGP) [5] and Tor [182]. While we have explored each technology independently, we have yet to consider the interplay between users’ models of these different technologies. Doing so may be a fruitful direction for future work. Additionally, user mental models of privacy-enhancing technologies have typically been explored in the Global North, especially in English-speaking countries. However, the mental models of people living in highly-censored countries, including some in the Global South, have not been studied. It is critical to study the Global South to enable the development of a more complete and cohesive set of interventions for ensuring privacy and protection against censorship.

6.6 Limitations

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

Furthermore, traditional survey biases might have occurred. Some questions could have introduced a social-desirability bias, in which some respondents felt social pressure to give the “desirable” response. Whenever possible, we carefully worded these questions.
For example, we phrased a question asking whether respondents sent/had sent emails using encryption, to emphasize that there are different reasons people decide whether or not to encrypt their email.

Finally, we asked demographic questions at the end of the survey to minimize sensitivity and bias [183].

6.7 Contributions to Thesis

In this chapter, we designed and conducted a user study to answer the fourth and fifth research questions this thesis addresses: Do users understand the security properties offered by secure (in particular, end-to-end encrypted) communication tools? Should the computer security and privacy community focus on fostering adoption, without emphasizing appropriate use, of secure communication tools (see Section 1.2)? We found that the vast majority of survey respondents had adopted usable end-to-end encrypted communication tools (mainly, WhatsApp) in the real world, but lacked confidence and accuracy in their mental models of end-to-end encryption. This suggests that most users do not know what it means for a usable and secure messenger that is widely-adopted and offers the utility users look for, such as WhatsApp, to be end-to-end encrypted. Hence, we argue that the primary user-related challenge for end-to-end encrypted communication tools is not only fostering adoption, but also emphasizing appropriate use.
Chapter 7

Users Do Not Bite: A Participatory Design Study of End-to-End Encrypted Communication Tools

In the previous chapter, we explored user mental models of end-to-end encrypted communication tools. We found that users have a wide range of misconceptions about end-to-end encryption. This suggests the key user-related challenge for secure communications is not anymore spurring adoption, but emphasizing appropriate – by effectively communicating the security properties of end-to-end encrypted communications.

To do so, we seek in this chapter to improve the design of ‘end-to-end encryption’ descriptions. We perform a participatory design user study (n=10) to solicit new description designs from participants. Drawing from the findings of the study, we extract a set of design guidelines to help developers of communication tools design more informative descriptions of ‘end-to-end encryption.’

The rest of this chapter is structured as follows:

• Section 7.1 describes the research objectives of this study.

• Section 7.2 describes our participatory design user study.
• Section 7.3 presents and discusses the findings of our study.

• Section 7.4 describes the principal limitations of the study.

• Section 7.5 describes the contributions this chapter makes to the thesis.

The work described in this chapter is under submission for publication. The thesis author is the sole author of this work.

7.1 Introduction

In previous chapters, we found that, in addition to poor usability, lack of utility and incorrect user mental models of secure communications are primary obstacles to adoption. Users will not adopt a communication tool that is both usable and secure, but lacks utility (due to, e.g., the tool’s small userbase or lack of interoperability). Further, most users do not know what it means for a usable and secure tool that is widely-adopted and offers utility (e.g., WhatsApp) to be end-to-end encrypted. Incorrect mental models of encryption lead people to use less secure channels that they incorrectly perceive as more secure than end-to-end encrypted tools.

Thus, we argue the key user-related challenge for secure communications is no longer fostering adoption, but emphasizing appropriate use – by helping people who already use secure tools avoid sending sensitive information over less secure channels. By employing participatory design in this chapter, we take a user-centered approach to designing effective descriptions that explain the security properties of end-to-end encrypted communications.

To this end, we performed a participatory design user study to improve the design of ‘end-to-end encryption’ descriptions. We recruited 10 demographically-diverse participants and asked them to critique the existing ‘end-to-end encryption’ descriptions, or security messages, of Telegram and WhatsApp, and to explain why these descriptions are vague. We then asked them to design new descriptions to convey the actual benefits and limitations of end-to-end encrypted communications.
We found that the vast majority of participants were specifically interested in the purpose (or security properties) of end-to-end encryption, and not how encryption worked, unlike prior work that has focused on making encryption “easier” for non-security experts—mainstream users—to understand. Further, participants suggested short and direct statements to explain what the purpose of encryption was, without the need for using the term “end-to-end encryption.”

### 7.2 Methodology

In this section, we describe the research questions we address in our study, recruitment process, participatory design study, and details of our data analysis. We designed and conducted a design study of 10 participants in the UK in May 2018. Each session lasted for thirty minutes. Our UCL’s Research Ethics committee reviewed and approved our study (project no.= 12567/001). We handled all collected data in accordance with the UK Data Protection Act 1998 (registration no.= Z6364106/2018/01/06).

#### 7.2.1 Research Questions

In this study, we answer the following research question:

- **RQ:** How can a user-centered approach to designing better descriptions of end-to-end encryption improve the end-user experience of encrypted communication tools?

#### 7.2.2 Recruitment

To recruit our participants, we posted flyers and distributed leaflets in London (UK). We asked interested participants to complete an online screening questionnaire, which about 70 completed. We aimed to recruit a demographically-diverse sample of participants. Hence, we included a number of demographic questions about gender, age, race, educational level, and employment status (see Appendix A for the pre-screening questionnaire).
We conducted a total of 10 design studies. We describe our participant demographics in Section 7.3.

### 7.2.3 Participatory Design Study

After exploring user mental models of end-to-end encrypted communications in Chapter 6, we aimed to investigate why ‘end-to-end encryption’ descriptions do not communicate the actual benefits and limitations of encrypted communications. We also sought to improve the design of these descriptions. Hence, we performed a participatory design study to solicit new designs from our participants.

**Critiquing existing descriptions.** We asked participants to critique existing descriptions. We sought to get feedback on two descriptions from participants. Hence, we asked each participant to critique the ‘end-to-end encryption’ descriptions of Telegram and WhatsApp (see Figure 7.1a and Figure 7.1b). To minimize bias, descriptions were assigned to each participant randomly. We chose these two descriptions because Telegram has been launched with security as a key selling point, and WhatsApp is widely-adopted and has recently added end-to-end encryption to its communications.

We showed participants one description at a time. We then asked them to describe what they felt about the description, how useful they felt the description was, what about the description that would make them decide to use or not use an encrypted tool, and what else they would like the description to tell them or elaborate on. We gave participants green and red markers to highlight what they liked and disliked about the description. We then showed participants the second description and followed-up by asking the same questions we asked about the first description they saw. We also asked participants to compare the second description to the first one, and then explain whether they would be more or less likely to use an encrypted tool if they saw this description or the prior one.

**Soliciting new description designs.** Finally, we performed a participatory design study to solicit new description designs from our participants. We asked participants to describe end-to-end encryption as if they were explaining it to someone new to this mechanism. We
7.2. Methodology

prompted our participants as follows: “We would like you to design a new description that clearly explains the benefits and limitations of end-to-end encrypted communication tools. While designing, think about what would make you use an encrypted communication tool, what information you would want to know, what information you would want to omit, and how you would want the description to look.” We gave participants a large pad of paper and a 24-colour pack of markers to describe their descriptions, giving them the option to draw.

We also asked participants to share their thoughts on the term: “end-to-end encryption,” and suggest a new term and/or metaphor, if any.

Figure 7.1: ‘End-to-end encryption’ descriptions in Telegram and WhatsApp.

(a) Telegram description.  
(b) WhatsApp description.
Chapter 7. Users Do Not Bite

7.2.4 Data Analysis

To develop depth in our exploratory research, we conducted multiple rounds of interviews, punctuated with periods of analysis and tentative conclusions [184]. In total, we (thesis author) conducted, transcribed, and analyzed all 10 design studies. We present the findings we identified in the next section.

7.3 Results and Discussion

We present and discuss the results from our 10 participants.

Demographics. Table 7.1 summarizes the demographics of our sample (n=10 participants). We interviewed five male and five female participants. Participants’ ages ranged from 18 to 54. Five identified as white, three as black, and two as Asian. Four reported having a college (or an undergraduate) degree, and three a graduate (or postgraduate) degree. Three reported having secondary (or high-school) education. Four were either high-school or university students, five employed, and one unemployed.

Finally, we note that P1 and P5 identified as computer security and privacy experts. Hence, they did not necessarily represent mainstream users.

Complexity and clarity. Eight participants reported finding the sentence “messages to this chat and calls are now secured with end-to-end encryption” in WhatsApp confusing. P7 said: “I believe this sentence is very confusing because I am not a technical person. I do not know what the ends refer to.” Similarly, P9 mentioned that the sentence was

<table>
<thead>
<tr>
<th>Gender</th>
<th>Age</th>
<th>Race</th>
<th>Education</th>
<th>Employment</th>
</tr>
</thead>
<tbody>
<tr>
<td>P01</td>
<td>Male</td>
<td>25–34</td>
<td>White</td>
<td>B.Sc. Student</td>
</tr>
<tr>
<td>P02</td>
<td>Male</td>
<td>25–34</td>
<td>Black</td>
<td>M.Sc. Employed</td>
</tr>
<tr>
<td>P03</td>
<td>Male</td>
<td>45–54</td>
<td>White</td>
<td>B.Sc. Unemployed</td>
</tr>
<tr>
<td>P04</td>
<td>Female</td>
<td>18–24</td>
<td>Black</td>
<td>High-school Student</td>
</tr>
<tr>
<td>P05</td>
<td>Male</td>
<td>25–34</td>
<td>White</td>
<td>B.A. Employed</td>
</tr>
<tr>
<td>P06</td>
<td>Female</td>
<td>35–44</td>
<td>Asian</td>
<td>M.Sc. Employed</td>
</tr>
<tr>
<td>P07</td>
<td>Male</td>
<td>18–24</td>
<td>White</td>
<td>B.A. Employed</td>
</tr>
<tr>
<td>P08</td>
<td>Female</td>
<td>25–34</td>
<td>Black</td>
<td>High-school Student</td>
</tr>
<tr>
<td>P09</td>
<td>Female</td>
<td>18–24</td>
<td>Asian</td>
<td>M.Sc. Employed</td>
</tr>
<tr>
<td>P10</td>
<td>Female</td>
<td>25–34</td>
<td>White</td>
<td>High-school Student</td>
</tr>
</tbody>
</table>

Table 7.1: Participant demographics.
short, did not explain why and how messages and calls were secured, and did not explain what end-to-encryption meant. Further, six participants mentioned disliking sentences that were vague, and three mentioned preferring messages that were clear and detailed. These three participants were interested in descriptions that specifically described what end-to-end encryption was or what its purpose was. P5 explained that descriptions should be “simple and direct explanations.”

On the other hand, two participants (P1 and P5) were confident explaining what the term meant and, hence, found both descriptions clear.

**Type of chats/communications.** Seven participants mentioned that although the WhatsApp description mentioned that messages and calls were end-to-end encrypted, it did not explain what type of messages (e.g., text messages, photos, voice notes) was encrypted. Further, eight participants mentioned that the Telegram description – “Secret Chats use end-to-end encryption” – did not explain “at all (P9)” the type of Telegram chats that were encrypted, making the Telegram description vaguer than the WhatsApp one.

**Secure, private, or safe?.** Seven participants mentioned that end-to-end encryption made Telegram/WhatsApp secure (x5), private (x1), or safe (x1). Three participants also mentioned that the use of the word “secured” in the WhatsApp description is not necessary because “different people could interpret ‘secured’ differently” (P7). On the other hand, one participant (P10) preferred descriptions that mentioned “security or secure,” P10 explained their preference for the word “secure” as follows: “In non-end-to-end encryption descriptions, the word ‘secure’ is not mentioned. However, in encryption descriptions, adding security would convince me to use an encrypted messenger because I would assume end-to-end encryption adds an extra layer of security.”

Seven participants suggested using the word “protect.” Two participants suggested using both “secure” and “protect.” Surprisingly, all but one participant decided to not use the term “end-to-end encryption” in their new designs, explaining that the term “is technical and does not explain the purpose of encrypting chats.” (P2)

**“End-to-end encryption”.** When asked what it meant that Telegram and WhatsApp
communications are end-to-end encrypted, two participants mentioned that no one could access the communications, and six explicitly mentioned that only the sender and the recipient could access the information exchanged. Only two gave the most precise answer that only the communicating devices can access end-to-end encrypted communications.

We then asked participants to define the “ends” in “end-to-end encryption.” Six participants defined the ends as the sender and the recipient, one as the communicating devices, and one as the two installed instances of Telegram/WhatsApp on the sender and recipient’s devices. Interestingly, two reported that the ends referred to the start and end of an exchanged message. We also note that participants answered all questions in the context of one-to-one communications; there was no mention of group communications. When prompted to think of end-to-end encryption in the context of group communications, only two participants were able to give a precise explanation.

Metaphors. Surprisingly, nine out of ten participants mentioned that the use of the term “end-to-end encryption” was not necessary. They argued that encryption is a mechanism or a “way (P5)” to achieve confidentiality or secrecy of content. Participants were interested in what encryption achieved, and not in whether or not a communication tool offered encryption. Unlike prior work [5,80] that has explored and engineered new terms or metaphors to explain what encryption or public-key cryptography is, participants preferred the use of direct sentences that explained what the purpose of, and not what, encryption was. The following six sentences were suggested by our participants to explain the purpose (or the security properties) of end-to-end encrypted communication tools:

1. Only the sender and recipient(s) can read [tool] text messages (x8).
2. Only the sender and recipient(s) can listen to [tool] voice notes (x5).
3. Only the sender and recipient(s) can view [tool] photos (x7).
4. Only the sender and recipient(s) can listen to [tool] phone calls (x4).
5. Only the sender can edit or modify [tool] messages (x2).
6. No one can impersonate the sender or the recipient(s) (x4).
Three participants mentioned using these direct statements to explain the purpose of encryption was sufficient – without the need to worry about engineering new metaphors for “end-to-end encryption” for both one-to-one communications and group communications.

**Backdoors.** Three participants mentioned the need to include that end-to-end encryption would be effective if “no backdoors (P1, P4)” or “no vulnerabilities (P4)” existed.

**Userbases and interoperability.** Five participants preferred that messaging tools should mention how large their userbases were. Three participants mentioned that tools should mention whether or not they were interoperable and worked across different platforms.

Finally, participants used bullet points to describe the purpose of end-to-end encrypted communications. The use of a specific color was not strongly favored by participants.

Drawing from the findings of our small-scale participatory design study, we encourage developers of secure – especially, end-to-end encrypted – communication tools to avoid using the term “end-to-end encryption” and, instead, explain what the purpose of encrypted communications is. Unlike prior work that has focused on making encryption easier for mainstream users to understand (see the work conducted by [3] and [80] in 2004 and 2018, respectively), mainly through engineering new metaphors to explain, for example, what public and private keys were (analogous to explaining how a car works), our participants were interested in what encryption achieved, and not what encryption was or how it worked. Indeed, in [80], Demjaha et al. conducted a survey to test whether or not exposing users to different metaphors of “end-to-end encryption” would “improve users’ understanding of the functionality provided by end-to-end encrypted messaging apps,” let alone the actual protection provided by these apps. They found that none of the metaphors tested in the survey improved respondents’ understanding of encryption.

Further, we argue that using direct and short sentences to explain the security properties of end-to-end encrypted communications would be effective, to help users form accurate mental models of encryption, as opposed to the models we uncovered in Chapters 3
and 6. Finally, we encourage developers to avoid using the words “secure,” “private,” or “safe” when describing encryption, and mention what type of communications (e.g., messages, calls) is encrypted.

7.4 Limitations

Our study has a number of limitations common to all qualitative research studies (see Section 3.6). The most obvious limitation is the small sample size of 10 participants. However, we recruited a demographically-diverse sample of participants in order to increase the likelihood that relevant findings have been mentioned by at least one participant.

To enable the development of a more complete and cohesive set of ‘end-to-end encryption’ description designs, we aim to develop the designs/guidelines suggested by the work described in this chapter. We will then evaluate the efficacy of these designs via controlled experiments with different user groups, especially those at-risk: refugees, immigrants, and sex workers (see Section 9.2.2 for future work).

7.5 Contributions to Thesis

In this chapter, we designed and conducted a user study to answer the sixth research question this thesis addresses: How can a user-centered approach to designing better descriptions of end-to-end encryption improve the end-user experience of encrypted communication tools (see Section 1.2)? We employed participatory design and proposed a set of data-driven guidelines to design more informative descriptions.
Chapter 8

A Validation Study: Evaluating the End-User Experience of Private Browsing Mode

In previous chapters, we took a user-centered approach to evaluating the end-user experience, and improving the design, of encrypted communication tools. In this chapter, we design and conduct a validation study to show how a user-centered approach can be taken to evaluating and improving the end-user experience of another privacy-enhancing technology: private browsing mode.

Nowadays, all major web browsers have a private browsing mode. However, the mode’s benefits and limitations are not particularly understood. Through the use of survey studies, prior work has found that most users are either unaware of private browsing or do not use it. Further, those who do use private browsing generally have misconceptions about what protection it provides.

However, prior work has not investigated why users misunderstand the benefits and limitations of private browsing. In this work, we do so by designing and conducting a three-part study: (1) an analytic approach combining cognitive walkthrough and heuristic evaluation to inspect the user interface of private mode in different web browsers; (2) a qualitative, interview-based study to explore users’ mental models of private browsing...
Chapter 8. Evaluating the End-User Experience of Private Browsing Mode

and its security goals; (3) a participatory design study to investigate why existing browser disclosures, the in-browser explanations of private browsing mode, do not communicate the security goals of private browsing to users. Participants critiqued the browser disclosures of three web browsers: Brave, Firefox, and Google Chrome, and then designed new ones. We recruited 25 demographically-diverse participants for the second and third parts of the study.

We find the user interface of private mode in different browsers violated well-established design guidelines and heuristics. Further, most participants had incorrect mental models of private browsing, influencing their understanding and usage of private mode. We also find existing browser disclosures did not explain the primary security goal of private mode. Drawing from the results of our study, we extract a set of recommendations to improve the design of disclosures.

The rest of this chapter is structured as follows:

- Section 8.1 describes the research objectives of this study.
- Section 8.2 describes our three-part study design.
- Section 8.3 presents the findings of our study.
- Section 8.4 discusses the findings of our study and proposes a set of data-driven guidelines to improve the design of browser disclosures related to private mode.
- Section 8.5 describes the principal limitations of the study.
- Section 8.6 describes the contributions this chapter makes to the thesis.

The content of this chapter is an edited version of the following publication:

Appendix B contains supplementary material (in particular, the pre-screening questionnaire we designed and used to recruit our study participants) for this chapter.

8.1 Introduction

Prior work has extensively explored users’ online privacy concerns when using the Internet [10–17]. For example, a survey of 1,002 US respondents (conducted by the Pew Research Center in 2013) found that respondents were concerned about their personal information being available online [14]. Respondents also felt strongly about controlling who had access to their behavioural data and communications, including family members, partners, friends, employers, advertisers, and government agencies. In 2015, Angulo and Ortlieb conducted a user study to investigate users’ concerns with regards to “online privacy-related panic” incidents [16]. They identified 18 different incidents that would make participants panic or distress. Online tracking, reputation loss, and financial harm were the most frequently reported incidents by participants.

Prior work has also found that users are willing to take measures to protect their online privacy. In the same Pew Research Center survey [14], a clear majority (86%) of respondents reported they had taken steps to remove or hide their “digital footprints,” including clearing their browsing history and cookies. Further, Kang et al. conducted a user study to investigate how users would react to security and privacy risks [18]; 77% of non-technical participants reported taking several measures to protect their “digital traces,” including the use of private browsing mode.

As we can see, users have serious concerns about their online privacy, and try to employ different strategies or use different privacy-enhancing tools to protect it. In this work, we focus on evaluating the end-user experience of one of these tools: private browsing mode. Private browsing is a privacy-enhancing technology that allows a user to browse the Internet without saving information about the websites they visited in private mode on their local device. As of today, all major web browsers have a private browsing mode.

1 In this thesis, we use the terms “private browsing mode,” “private browsing,” and “private mode” interchangeably.
We refer the reader to Section 2.3 for the technical definition of private browsing mode.

Previous user studies have quantitatively – mainly through survey studies – investigated whether users are aware of private browsing, what they use it for, and whether they understand what protection it provides [19–24]. However, these studies have not investigated why most users misunderstand the benefits and limitations of private browsing mode. Further, many of the recruited participants in these studies were unaware of or had not used private mode. In this work, we address these research gaps by designing and conducting a three-part study, where we recruited 25 demographically-diverse participants (both users and non-users of private mode) for the second and third parts of the study.

First, we use an analytic approach combining cognitive walkthrough and heuristic evaluation to inspect the user interface of private mode in different web browsers. Second, we conduct a qualitative, interview-based study to explore user mental models of private browsing and its security goals. Third, we perform a participatory design study to investigate whether existing browser disclosures, the full-page explanations browsers present when users open a new private tab or window in private mode, communicate the security goals of private browsing to users. We ask participants to critique the disclosures of Brave, Chrome, and Firefox, and then design new ones.

We summarize our key findings below:

- We identify usability issues in the user interface of private mode in different browsers. We find some of these issues hampered the adoption of private mode (e.g., minimal feedback, use of technical jargon, lengthy disclosures).

- We find participants had inappropriate mental models of private mode. Further, almost all participants did not understand the security goal of private browsing. For example, some participants sent emails unencrypted in private mode, incorrectly believing private mode achieved confidentiality.

- We find most participants who used private mode performed their private browsing activities while being authenticated to their personal online account (mainly their
Google account), incorrectly believing their browsing or search history would get deleted from Google’s records after exiting private mode.

- We find none of the three studied browser disclosures communicated the security goal of private mode. Our participants also pointed out that disclosures did not explain where information related to a private browsing session would get deleted from, and when.

Drawing from these findings, we extract a set of guidelines to improve the design of disclosures. We also propose a new disclosure design.

## 8.2 Methodology

We conducted a three-part study: (1) a hybrid analytic approach combining cognitive walkthrough and heuristic evaluation; (2) a qualitative, interview-based user study; (3) a participatory design study. Our study was reviewed and approved by our organization’s ethics committee.

For the second and third parts of our study, we first conducted five unstructured (open-ended) face-to-face interviews, lasting for 60 minutes on average each (see Table 8.1). The emerging themes from these five interviews helped us design the study script we used to conduct our main interviews: 25 semi-structured face-to-face interviews lasting for 90 minutes on average each (see Table 8.3 in Section 8.3.1). Below, we describe our study script (see Section 8.2.4 and Section 8.2.5).

<table>
<thead>
<tr>
<th>Gender</th>
<th>Age</th>
<th>Race</th>
<th>Education</th>
<th>Employment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>18–24</td>
<td>Asian</td>
<td>Some college</td>
<td>Student</td>
</tr>
<tr>
<td>Male</td>
<td>35–44</td>
<td>Hispanic</td>
<td>B.Sc.</td>
<td>Employed</td>
</tr>
<tr>
<td>Female</td>
<td>25–34</td>
<td>White</td>
<td>M.Sc.</td>
<td>Student</td>
</tr>
<tr>
<td>Male</td>
<td>18–24</td>
<td>White</td>
<td>B.Sc.</td>
<td>Student</td>
</tr>
<tr>
<td>Female</td>
<td>55–64</td>
<td>Black</td>
<td>B.A.</td>
<td>Retired</td>
</tr>
</tbody>
</table>

Table 8.1: Unstructured interview participant demographics.

### 8.2.1 Research Questions

In this thesis, we answer the following research questions:
• **RQ1:** Does private mode in different web browsers suffer from poor usability that hampers the widespread adoption and use of private browsing?

• **RQ2:** How do users perceive the term “private browsing?”

• **RQ3:** What are users’ mental models of private browsing (as a privacy-enhancing technology) and its security goals?

• **RQ4:** How do users perceive those who use private browsing? Do users perceive the routine use of private browsing as “paranoid” or “unnecessary?”

• **RQ5:** How do users’ mental models and perceptions influence their usage of private browsing?

• **RQ6:** Why do existing browser disclosures (related to private browsing) misinform users of the benefits and limitations of private browsing?

• **RQ7:** How can the design of disclosures be improved?

### 8.2.2 Recruitment

In this work, our focus – similar to our user studies of secure communications in previous chapters – is to understand how mainstream users perceive private browsing and its security goals. This understanding is crucial to design browser disclosures that sufficiently inform the general public of the benefits and limitations of private browsing. We do not investigate how a specific at-risk user group – such as activists, journalists, or whistle-blowers – perceive and use private browsing. However, we have documented our study protocol step-by-step, meaning that it can be replicated with different user groups in varying contexts.

To recruit our participants (for the second and third parts of the study), we posted flyers and distributed leaflets in London (UK). We asked interested participants to complete an online screening questionnaire, which about 500 completed. We aimed to recruit a demographically-diverse sample of participants. Hence, we included a number of demographic questions about gender, age, race, educational level, and employment status.
We also assessed participants’ technical knowledge; we considered participants as technical if two out of three of the following were true [73]: (1) participants had an education in, and/or worked in, the field of computer science, computer engineering, or IT; (2) they were familiar with or an expert in at least one programming language (e.g., C++); (3) people usually asked them for computer-related advice. Further, we provided participants with a list of different web browsers, and then asked which browsers they used, what they used each browser for (in case they used multiple browsers), which browser they used the most, and how many hours they spent daily on their desktop and mobile phone browsing.

Additionally, we asked participants to list the digital security requirements they had at school or work, how often they received cybersecurity training, and whether they felt at risk due to their school work or job duties. In [62], Gaw et al. found that people perceived the “universal, routine use of encryption as paranoid.” In this work, we aimed to explore whether our participants perceived the everyday use of private mode as paranoid and unnecessary. The pre-screening questionnaire can be found in Appendix B.

We first conducted and analyzed five unstructured interviews (to help us design the study script, which we explain in detail in Section 8.2.4 and Section 8.2.5), followed by 25 semi-structured interviews (our study’s main interviews).

### 8.2.3 Part 1: Usability Inspection

Usability inspection is aimed at finding usability problems in the user interface design. Unlike empirical user studies (see Part 2 and Part 3 below), a user interface is inspected by evaluators without engaging users (i.e., without recruiting participants to assess the usability of a system). Although it is important to bring users into the design process, evaluating a design without users can also provide benefits [163].

To answer RQ1 (see Section 8.2.1), we used a hybrid approach combining cognitive walkthrough and heuristic evaluation to inspect the user interface of private mode in five different web browsers: Brave, Chrome, Internet Explorer, Firefox, and Safari. We refer the reader to Chapter 5 for a detailed overview of the hybrid approach – the same approach

2 [https://tinyurl.com/chi2020-2](https://tinyurl.com/chi2020-2)
Chapter 8. Evaluating the End-User Experience of Private Browsing Mode

we used to evaluate the user interface of Telegram. We:

1. provided a detailed description of the user interface.

2. defined the users and their goals.

3. defined the tasks the users would attempt (e.g., accessing a web page in private mode).

4. divided each task into a sequence of sub-tasks or actions (e.g., selecting the “New Private Window” option).

5. walked through each task workflow step-by-step through the lens of the users (e.g., what they would look for).

6. looked for and identified usability problems (for each action) based on the ten heuristics described in [58].

7. specified where the usability problem was in the user interface, how severe it was, and possible design fixes.

8.2.4 Part 2: Interview-Based Study

After inspecting the user interface of private mode, we aimed to answer RQ2—RQ5 (see Section 8.2.1), by qualitatively investigating participants’ mental models of private browsing and its security goals, as well as exploring how participants perceived those who (regularly or occasionally) used private browsing. We also aimed to understand how participants’ mental models and perceptions influenced their understanding and usage of private mode. Hence, we explored the following themes:

Mental models of “private browsing.” We asked participants whether they had heard of the term “private browsing,” and, if so, whether they felt confident explaining what it meant. We then asked them to explain what it meant to browse privately. We provided participants with a large pad of paper and a 24-color pack of markers, giving them the
option to draw their mental models of private browsing. We also asked participants to describe the benefits and drawbacks of browsing privately.

By asking these questions, we aimed to investigate participants’ conceptual understanding of the term “private browsing,” and how this understanding influenced their mental models and usage of private mode (as a privacy-enhancing technology), as we describe next in detail.

*Mental models of private mode (as a privacy tool).* After exploring participants’ general mental models of the term “private browsing,” we asked participants whether they had browsed in private mode and, if so, whether they felt confident explaining what it meant to open a private tab or window. We then asked them to explain the difference, if any, between default (non-private) mode and private mode.

We also aimed to understand how participants perceived the security goals of private mode. Hence, we asked participants about the entities that could learn about their private browsing activities (e.g., visited websites in private mode), and how. We wanted to explore whether participants understood the primary goal of private mode: protecting against a local attacker who controls a user’s machine after the user exits private mode.

*Perceptions of users of private mode.* We then asked participants to explain how they perceived the use of private mode. We aimed to investigate whether participants perceived users of private mode as paranoid.

*Expectations.* We asked participants to describe what they would expect from private mode. We also investigated whether participants’ familiarity with private mode affected the robustness of their mental models. Therefore, we asked participants to list the web browsers that they used (as well as those they did not necessarily use) and that they considered having a private mode that met their expectations.

*Private browsing usage.* Finally, we aimed to explore how participants’ mental models influenced their usage of private mode. Hence, we asked participants who used, or had used in the past, private mode to share their private browsing habits. We asked them what
they used private mode for, how often they used it, and where they used it. We also asked them to explain what they liked and disliked about private mode.

8.2.5 Part 3: Participatory Design Study

After exploring our participants’ mental models and usage of private mode, we aimed to investigate why browser disclosures (related to private browsing) did not communicate the actual benefits and limitations of private browsing. We also sought to improve the design of existing browser disclosures. Hence, we performed a participatory design study to solicit new disclosure designs from our participants.

Assessing participants’ knowledge of private mode (before tutorial). To answer RQ6 and RQ7 (see Section 8.2.1), we asked participants to take a short quiz to further test their knowledge of private mode. We asked them to answer seven questions about a private mode that worked properly:

- Private mode hides my browsing activities from [browser vendor].
- If I visited a website in private mode, the website would not be able to determine whether I was browsing in private or public mode.
- After I exited private mode, a family member would not be able to learn about my activities in private mode.
- Before I start browsing in private mode, a family member will not be able to learn about the websites I plan to visit in private mode.
- Private mode encrypts information I send and receive while browsing in private mode.
- Private mode hides my browsing activities from my school or employer.
- Private mode hides my identity from websites I visit.

We also asked participants whether they were familiar with the following items that appeared on almost all existing browser disclosures, and whether they felt confident ex-
plaining what each item meant: browsing history file, cookies, search items, bookmarks, downloads, and temporary files.

*Giving a tutorial.* We then gave participants a 15-minute tutorial, explaining the primary security goal of private browsing, the difference between default (non-private) mode and private mode, and why private browsing did not protect against website fingerprinting and, hence, website tracking and ad targeting. Further, we explained the different items/files that most browsers claimed to delete when a user exited private mode. We also explained the different privacy features that had been recently added by some web browsers (e.g., Brave’s Private Tabs with Tor). Finally, we explained the difference between a private tab, a private window, and a private session.

*Assessing participants' knowledge of private mode (after tutorial).* To evaluate whether participants’ knowledge of private browsing had improved after the tutorial, we asked participants to take the same quiz we gave them previously. However, we shuffled the questions to minimize bias.

*Critiquing existing disclosures.* We then asked each participant to critique the browser disclosures of three browsers: Brave, Chrome, and Firefox (see Figures 8.1, 8.2, and 8.3). To minimize bias, disclosures were assigned to each participant randomly. We chose these three disclosures because Chrome and Firefox were the most frequently-used browsers by participants, whereas Brave was launched with privacy as a key selling point.

We conducted a within-subject study; we showed participants one disclosure at a time. We then asked them to describe what they felt about the disclosure, how useful they felt the explanation was, what about the explanation would make them decide to use private mode, and what else they would like the disclosure to tell them. We gave participants green and red markers to highlight what they liked and disliked about the disclosure. We then showed participants the second disclosure and followed-up by asking the same questions we asked about the first disclosure they saw. We also asked participants to compare the second disclosure to the first one, and then explain whether they would be more or less likely to use private mode if they saw this disclosure or the prior one. We then showed participants the third disclosure and asked them the same questions we previously asked.
Figure 8.1: Brave browser disclosure.

Soliciting new disclosure designs. We then performed a participatory design study to solicit new disclosure designs from our participants. We asked participants to describe private browsing as if they were explaining it to someone new to this privacy-enhancing
8.2. Methodology

Figure 8.3: Firefox browser disclosure.

technology. We prompted our participants as follows: “We would like you to design a browser disclosure that clearly explains the benefits and limitations of private browsing. While designing, think about what would make you use private mode, what information you would want to know, what information you would want to omit, and how you would want the disclosure to look.” We gave participants a large pad of paper and a 24-color pack of markers to design their disclosures, giving them the option to draw.

Finally, we asked participants to share their thoughts on the following names: “Private Browsing,” “InPrivate Browsing,” and “Incognito Browsing,” and suggest a new name, if any.

8.2.6 Pilot Study

Quiz piloting. After developing our quiz (see Section 8.2.5), we conducted cognitive interviews with five participants to test our quiz (see Table 8.2). Cognitive interviewing is a method used to test questionnaires to glean insights into how participants might interpret
questions [134]. After answering each quiz question, participants were asked to share their thoughts and answer the following: “Was this question difficult to understand or answer?;” “How did answering the question make you feel?” We then used the findings to revise our quiz, and evaluate question wording and bias.

Main study piloting. To pre-test the second and third parts of our study (pre-screening questionnaire, study script, and quiz), we conducted a small-scale pilot study of five semi-structured interviews (using convenience sampling [134]). Additionally, we asked ten computer security and privacy researchers and experts to review the study. We used the findings to identify potential problems (e.g., time, cost, adverse events) in advance prior to conducting the full-scale study.

Drawing from the findings of our pilot study, we made the following changes:

• We decided to give participants a ten-minute break between the second and third parts of the study, to reduce interviewee fatigue and inattention [136].

• As part of the participatory design study, we asked participants to take a quiz (before our tutorial) to assess their knowledge of private mode. Based on the pilot study findings, we decided to give participants the same quiz after the tutorial, to assess whether or not participants’ knowledge had improved before they started analyzing and critiquing browser disclosures.

• We first aimed to ask participants to critique the browser disclosures of five web browsers: Brave, Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, and Safari (as part of the participatory design study). However, due to interviewee fatigue (as per our pilot study findings), we decided to analyze the disclosures of three browsers – Brave, Chrome, and Firefox – based on how popular the browser is and how it advertises itself (e.g., as fast, safe, or private).
8.3. Results

<table>
<thead>
<tr>
<th>Gender</th>
<th>Age</th>
<th>Race</th>
<th>Education</th>
<th>Employment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>18–24</td>
<td>Black</td>
<td>B.Sc.</td>
<td>Student</td>
</tr>
<tr>
<td>Male</td>
<td>35–44</td>
<td>Asian</td>
<td>M.Sc.</td>
<td>Employed</td>
</tr>
<tr>
<td>Female</td>
<td>18–24</td>
<td>White</td>
<td>B.Sc.</td>
<td>Student</td>
</tr>
<tr>
<td>Male</td>
<td>55–64</td>
<td>White</td>
<td>Some college</td>
<td>Retired</td>
</tr>
<tr>
<td>Female</td>
<td>45–54</td>
<td>Hispanic</td>
<td>Some college</td>
<td>Employed</td>
</tr>
</tbody>
</table>

Table 8.2: Cognitive interview participant demographics.

8.2.7 Data Analysis

Usability inspection (Part 1). Two expert HCI researchers inspected the user interface of private mode in Brave, Chrome, Internet Explorer, Firefox, and Safari. We did so independently before discussing the findings and aggregating all the uncovered issues in a larger set.

Interview-based and participatory design studies (Part 2 and Part 3). We conducted, transcribed, and analyzed all five unstructured and 25 semi-structured interviews (the study’s main interviews). We observed data saturation [136, 184, 185] between the 20th and the 25th semi-structured interview; i.e., no new codes emerged in interviews 20–25, and, hence, we stopped recruiting participants. Data saturation is commonly taken to indicate, on the basis of the data that has been collected and analyzed, further data collection and analysis are unnecessary.

Two researchers independently coded all interview transcripts and image data using Grounded Theory [136, 184, 185]. The researchers created two codebooks: one for the interview transcripts and one for the image data. After creating the final codebooks, we tested for the inter-rater reliability. The average Cohen’s kappa coefficient ($\kappa$) for all codes in the interview transcripts and image data was 0.77 and 0.89, respectively. A $\kappa$ value above 0.75 is considered excellent agreement [138, 139].

8.3 Results

In this section, we present the results of our study.
Chapter 8. Evaluating the End-User Experience of Private Browsing Mode

Table 8.3: Semi-structured interview participant demographics.

<table>
<thead>
<tr>
<th>Gender</th>
<th>Age</th>
<th>Race</th>
<th>Education</th>
<th>Employment</th>
</tr>
</thead>
<tbody>
<tr>
<td>P01</td>
<td>Male</td>
<td>25–34</td>
<td>White</td>
<td>Ph.D.</td>
</tr>
<tr>
<td>P02</td>
<td>Male</td>
<td>45–54</td>
<td>Mixed race</td>
<td>B.A.</td>
</tr>
<tr>
<td>P03</td>
<td>Male</td>
<td>45–54</td>
<td>White</td>
<td>Ph.D.</td>
</tr>
<tr>
<td>P04</td>
<td>Female</td>
<td>18–24</td>
<td>Black</td>
<td>High-school</td>
</tr>
<tr>
<td>P05</td>
<td>Female</td>
<td>25–34</td>
<td>White</td>
<td>B.A.</td>
</tr>
<tr>
<td>P06</td>
<td>Male</td>
<td>35–44</td>
<td>White</td>
<td>M.Sc.</td>
</tr>
<tr>
<td>P07</td>
<td>Female</td>
<td>18–24</td>
<td>White</td>
<td>B.A.</td>
</tr>
<tr>
<td>P08</td>
<td>Female</td>
<td>25–34</td>
<td>Asian</td>
<td>High-school</td>
</tr>
<tr>
<td>P09</td>
<td>Male</td>
<td>18–24</td>
<td>Asian</td>
<td>M.Sc.</td>
</tr>
<tr>
<td>P10</td>
<td>Male</td>
<td>25–34</td>
<td>White</td>
<td>Some college</td>
</tr>
<tr>
<td>P11</td>
<td>Female</td>
<td>25–34</td>
<td>White</td>
<td>M.Sc.</td>
</tr>
<tr>
<td>P12</td>
<td>Female</td>
<td>45–54</td>
<td>White</td>
<td>Some college</td>
</tr>
<tr>
<td>P13</td>
<td>Male</td>
<td>25–34</td>
<td>Mixed race</td>
<td>B.A.</td>
</tr>
<tr>
<td>P14</td>
<td>Male</td>
<td>18–24</td>
<td>Hispanic</td>
<td>B.A.</td>
</tr>
<tr>
<td>P15</td>
<td>Female</td>
<td>25–34</td>
<td>Asian</td>
<td>B.Sc.</td>
</tr>
<tr>
<td>P16</td>
<td>Female</td>
<td>45–54</td>
<td>Black</td>
<td>VOC</td>
</tr>
<tr>
<td>P17</td>
<td>Female</td>
<td>18–24</td>
<td>White</td>
<td>Ph.D.</td>
</tr>
<tr>
<td>P18</td>
<td>Non-binary</td>
<td>35–44</td>
<td>White</td>
<td>M.Sc.</td>
</tr>
<tr>
<td>P19</td>
<td>Female</td>
<td>35–44</td>
<td>Black</td>
<td>B.Sc.</td>
</tr>
<tr>
<td>P20</td>
<td>Male</td>
<td>18–24</td>
<td>White</td>
<td>Some college</td>
</tr>
<tr>
<td>P21</td>
<td>Male</td>
<td>25–34</td>
<td>White</td>
<td>VOC</td>
</tr>
<tr>
<td>P22</td>
<td>Male</td>
<td>18–24</td>
<td>Asian</td>
<td>Ph.D.</td>
</tr>
<tr>
<td>P23</td>
<td>Female</td>
<td>25–34</td>
<td>White</td>
<td>M.Sc.</td>
</tr>
<tr>
<td>P24</td>
<td>Female</td>
<td>25–34</td>
<td>Black</td>
<td>B.Sc.</td>
</tr>
<tr>
<td>P25</td>
<td>Female</td>
<td>65–74</td>
<td>Hispanic</td>
<td>Some college</td>
</tr>
</tbody>
</table>

8.3.1 Demographics

Table 8.3 summarizes the demographics of our sample (n=25). We interviewed 11 male, 13 female, and one non-binary participants. Participants’ ages ranged from 18 to 75. 13 identified as white, four as black, four as Asian, two as Hispanic, and two as mixed-race. Eight reported having a college (or an undergraduate) degree, and nine a graduate (or postgraduate) degree. Two reported having secondary education, and four some post-secondary education (i.e., some college education without a degree). Two participants mentioned having vocational training (VOC). Nine participants were either high-school or university students, 12 employed, two unemployed, and one retired. One participant preferred not to indicate their employment status. According to the definition we used to assess our participants’ technical knowledge (see Section 8.2.2), 17 qualified as technical.

Our participants used a wide range of web browsers (both on desktop/laptop and mobile phone). Chrome was the most used browser by participants, followed by Safari, Firefox, Internet Explorer, and Brave, respectively. Three participants (P01; P03; P25) used the Tor browser.
Participants daily spent between five and 17 hours browsing the Internet for both work-related and work-unrelated purposes. Desktop/laptop browsing overtook smartphone surfing, with the exception of three participants (P02; P12; P16). Further, most participants (22 out of 25) used multiple browsers. For example, 21 reported they used one browser for social activities and one for work-related activities.

19 participants reported they used (or had used in the past) private mode. Three (P12; P16; P24) were aware of private mode, but had not browsed in it. Three (P02; P11; P23) did not know private mode existed.

Finally, we note P01, P03, P18, and P25 identified as computer security and privacy experts. Hence, they did not necessarily represent mainstream users.

### 8.3.2 Part 1: Usability Inspection

We used an analytic approach combining cognitive walkthrough and heuristic evaluation to inspect the user interface of private mode in five different web browsers (desktop versions). Our findings are as follows:

**Public mode as the default mode.** In all browsers (including the ones we inspected), the default mode is the public one. To browse in private mode, users need to select (from a hidden drop-down list) “New Incognito window” in Brave and Chrome, or “New private window” in Internet Explorer, Firefox, and Safari. We hypothesize (and find in Section 8.3.3) most users are unaware of the hidden list, which explains why most users do not know about private mode. This violates Nielsen’s heuristics of *visibility of system status* [166] and *aesthetic and minimalist design* [166].

**Multiple windows and tabs.** Users cannot open a private tab in a public window, and vice-versa; that is, users can only open public (private) tabs in public (private) windows – which we regard as good design. Further, users can only re-open the most recently-closed public tabs, and not private ones.

Although users can open multiple public and private windows, feedback is minimal.
For example, in Safari, when users enter private mode, there is no appropriate feedback – through the user interface – that communicates to users that they are currently browsing in private mode. There is only a short line of text (using a small font size) at the top of the page that says: “Private Browsing Enabled.” In Brave and Firefox, the background changes from white to purple. Both browsers do not explain why purple was chosen by browser designers to distinguish between public and private modes.

*Use of jargon.* Both Brave and Chrome refer to private mode as “Incognito window,” and Internet Explorer, Firefox, and Safari as “private window.” This violates Nielsen’s heuristic of *match between the system and the real world* [166], making the assumption that users’ understanding and interpretation of words or terms would be the same as browser designers and developers. We also hypothesize that users would build their own mental models of private mode when encountering these terms, which could strongly impact how users would perceive and use the mode in real life. We explore user mental models of private mode in the following section (Part 2).

*Wordy disclosures.* When users enter private mode, a browser disclosure is shown to them. The disclosure is meant to explain the benefits and limitations of private browsing. However, the disclosures of all inspected browsers (except that of Firefox) are lengthy and full of jargon, violating Nielsen’s heuristic of *match between the system and the real world* [166]. Further, browser disclosures do not explain the primary security goal of private mode. In Firefox, the disclosure is relatively short, but, also, does not explain the security goal of private mode.

Further, in all five browsers, users are presented with these disclosures only once (when they open a private window or tab), violating Nielsen’s heuristics of *recognition rather than recall* [166] and *help and documentation* [166].

In Section 8.3.4, we present the results from our participants who critiqued three existing browser disclosures and suggested several design options for improvement.

*Private browsing and Tor.* Brave has recently added Tor to its private windows. Brave users can now open a “New window,” “New Incognito window,” or “New private window
8.3. Results

with Tor.” Both Incognito windows and private windows with Tor have the same purple background and lengthy disclosures, which could lead users to browse in one instead of the other, violating Nielsen’s heuristic of visibility of system status [166]. Further, the browser disclosures of both windows do not clearly explain how private mode and Tor are two different privacy tools.

8.3.3 Part 2: Interview-Based Study

The main purpose of qualitative research is to explore a phenomenon in depth, and not to investigate whether or not findings are statistically significant or due to chance [134]. Although we report how many participants mentioned each finding as an indication of prevalence, our findings are not quantitative. Further, a participant failing to mention a particular finding does not imply they disagreed with that finding; they might have failed to mention it due to, for example, recall bias [134]. Thus, as with all qualitative data, our findings are not necessarily generalizable beyond our sample. However, they suggest several future research avenues, and can be later supplemented by quantitative data.

In this section and the next section, we present the results of the second and third parts of the study (n=25).

Mental models of “private browsing.” We aimed to investigate our participants’ conceptual understanding of the term “private browsing.” 18 out of 25 (a clear majority) had heard of the term, and 17 felt confident explaining what the term meant3. 16 out of 17 were users of (or had used in the past) private mode. One participant (P11) was a non-user.

We then asked all participants to explain what “private browsing” meant to them. Five out of 25 associated the term with private browsing mode, mentioning the following: “the window that has a man with a coat and a pair of eye glasses” (x4); “going undercover or incognito” (P04). All five participants were referring to the “Incognito window” in Google Chrome. Further, five participants thought of the term in connection with

---

3 It is worth to mention that only three out of those 17 participants associated the term “private browsing” with private mode. We speculate that this was because the three participants used – regularly or occasionally – private mode.
network-encrypted communications or secure browser connections (i.e., webpages running HTTPS), three with end-to-end encrypted communications, three with anonymous communications (using Tor or VPN), and three with user authentication (both one-factor and two-factor authentication). One participant (P17) associated “private browsing” with both network encryption and authentication. Additionally, P15 described the term as the ability to browse the Internet “without getting infected with a virus.”

Further, eight participants mentioned the terms “privacy” and “online privacy” to explain what “private browsing” meant to them: P01–P05, P07, and P12–P14 defined the term as having control over how users’ online information was handled and shared. P09, P20, P22, and P24 referred to the term as the ability to manage and “regulate” one’s social space.

*Mental models and usage of private mode (as a privacy tool).* After exploring our participants’ conceptual understanding of the term “private browsing,” we aimed to investigate how this understanding influenced participants’ mental models and usage of private mode (as a privacy tool). We identified three types of users of private mode: regular users, occasional users, and former users. We explain each type as follows:

1. *Regular users:* Two participants (P01 and P17) were regular users of private mode. They performed all their browsing activities in private mode. They described themselves as “paranoid” and “cautious.” P01 mentioned that the routine use of private mode made them feel “safer” and “more comfortable.” Further, P01 used Safari’s private mode to protect against shoulder-surfing. They explained that Safari did not have a visual user interface element that indicated a user was currently browsing privately. However, when probed, P01 (as well as P17) did not know that staying in private mode for a long period of time could easily enable fingerprinting and, hence, website tracking (a threat that both participants thought they were protected against by regularly browsing in private mode).

2. *Occasional users:* Out of 25, 15 participants used private mode occasionally depending on their browsing activities and the websites they visited. They did not necessarily use the mode to visit “embarrassing websites.” Many used private mode for online shopping (e.g., purchasing a surprise gift for a family member or a friend), logging into
an online service using a different account, and/or debugging software.

3. Former users: Two participants (P13 and P19) reported they had used private mode before, but they stopped using it for the following reasons:

- **Lack of usability.** P13 and P19 mentioned that entries added to the history file would get deleted if they exited private mode, negatively impacting user experience. P13 also mentioned that private mode was “useless” because users could delete information about websites visited in default mode by manually clearing their browsing history file (a view shared by P12 and P16).

- **Lack of utility.** P13 stopped using private mode because they thought that web browsers did not allow extensions to run in private mode (although users could manually enable extensions in private mode in most browsers). This finding was also shared by five other participants.

- **Misconceptions about private mode.** P13 perceived those who used private mode as people who “had something to hide” or “were up to no good,” influencing P13’s decision to stop using private mode; P13 did not want to be perceived by others as a “cybercriminal.” Some participants shared this perception, as we discuss later in this section.

17 out of 25 participants reported they mainly used private mode in public spaces using shared devices, mainly coffee shops, libraries, and airports. They performed browsing activities they regarded as sensitive in private mode. For example,

“I usually use Incognito in . . . you know . . . in Google when I work at [coffee shop] because I connect to the Internet using insecure or public Wi-Fi. My laptop consistently warns me. So, I use Incognito to encrypt my data and hide it from people around me . . . Better to be safe!” (P05)

“I usually use the public or . . . shared workstations in my school’s library. You don’t need to login because there is one account shared by all students. I open a private tab or
window to download files that I want to be removed after I close the browser . . . By the way, I also use a private window to send an encrypted email.” (P17)

Surprisingly, P17 was a regular user of Safari that locally deleted files downloaded in its private mode. However, P17 did not notice he was using Firefox on the library’s computer, which did not delete private browsing downloads.

“I make a bank transfer or access my personal accounts – you know, like Facebook – when I use one of the computers that all passengers can use . . . I am talking about the computers you find in an airport lounge . . . I open a private window.” (P07)

“I use Incognito to search for new jobs. Hmm, I do not want my boss or company to know . . .” (P18)

“If I do not have Tor installed, I will use Incognito.” (P09)

We also found six participants who tended to use private mode to visit malicious webpages. For example,

“I sometimes encounter a message that warns me from accessing a bad webpage. I usually ignore the warning and open the page in a private window . . . Feels safer!” (P14)

Alarmingly, we found all participants who used or had used private mode (x19) browsed privately while being authenticated to their Google or YouTube account, incorrectly believing their search history would get deleted from Google or YouTube’s records after exiting private mode.

Additionally, we found that some participants (11 out of 25) perceived those who used private mode as people who “cared about their online privacy,” “had something to hide” (e.g., journalists, activists, dissidents), or “were up to no good” (e.g., cybercriminals, terrorists). These inappropriate mental models and misperceptions partially explain why most users overestimate the protection private mode offers.

To summarize the findings above, many participants found utility in private mode (e.g., online shopping, debugging software). However, our participants’ conceptual un-
8.3. Results

derstanding of the term “private browsing” negatively influenced their usage of private
mode in real life. Many incorrectly believed that private mode could be used to send en-
crypted email, achieve online anonymity, or simply access a phishing webpage because it
“felt safer” to do so.

Security goals of private mode. We aimed to further investigate how participants per-
ceived the security goals of private mode. Thus, we asked participants about the entities
that could learn about their private browsing activities, and how.

All, but three participants (P03; P18; P25) who identified as security/privacy experts,
did not understand what private mode could and could not achieve (i.e., did not recognize
the primary security goal of private browsing). Many participants (19 out of 25) believed
that a family member, a friend, or a work colleague would not be able to learn about the
websites they visited in private mode “whatsoever” (P01). Ten mentioned that this would
only be possible if the entity was “technically-sophisticated.” Only P03, P18, and P25 (as
mentioned above) correctly explained that private mode protected against a local attacker
after exiting private mode.

Several participants (12 out of 25) believed that a browser vendor (e.g., Google)
could not learn their private browsing activities, citing the following statement that ap-
peared on most browser disclosures: “[Browser vendor] won’t save your information . . . ”
Further, seven believed that private mode would hide their browsing activities from the
employer, six from the ISP, and six from intelligence services and governments.

As we can see, most participants did not understand the main security goal of pri-
vate mode, partially explaining why several participants perceived those who used private
mode as paranoid or up to no good.

Expectations. We then asked participants what they expected from private mode.
Again, 19 expected that anyone who had access to their machine would find no evi-
dence of the websites visited privately. Additionally, ten expected that a private mode
that worked properly would not link their browsing activities in private mode to those in
public mode. 13 also expected that a private mode would protect them from all types of
website tracking and ad targeting. Interestingly, five expected a website visited in private mode would not be able to determine whether the user was currently browsing privately or not.

Although some browsers, such as Brave, have added privacy features to reduce online tracking, no browser meets all participants’ expectations. However, we argue that participants’ expectations were high because they overestimated the benefits of private mode.

8.3.4 Part 3: Participatory Design Study

We aimed to investigate why existing browser disclosures did not communicate the actual benefits and limitations of private browsing. To further test participants’ knowledge of private mode, we asked participants to take a short quiz (see Section 8.2). Participants performed poorly with an average score of 3.21/7.00. Most participants (21 out of 25) overestimated the benefits of private mode.

We also asked participants to explain the following items that appeared on most browser disclosures: history file, cookies, and temporary files. We found that although all participants correctly described a browsing history file, most participants (21 out of 25) either had not heard of a cookie or a temporary file, or did not feel confident explaining what these items meant (in the context of private browsing). These findings suggest that most participants did not understand the functionality of private browsing, a finding recently echoed by [23]. However, we argue (see Section 8.4) that users do not need to understand the functionality of private browsing in order to use private mode correctly.

We then gave our participants a 15-minute tutorial, and asked them to take the same quiz again. Participants’ quiz performance significantly improved (mean= 6.31/7.00), which was an indication that participants could use the knowledge they newly acquired to critique existing disclosures and then design new ones. Hence, we asked participants to critique the disclosures of Brave, Firefox, and Chrome.

*Private mode.* Most participants (20 out of 25) criticized Firefox for describing its
private mode as a “private window.” Further, 17 participants pointed out that although both Brave and Chrome named their private mode “Incognito,” they still used the phrase “browse privately” in their browser disclosures (in the first sentence), which participants described as “misleading” (P02; P06—P09; P12; P19—P21; P24).

Moreover, 19 participants were confused about when information (e.g., cookies, search items) about websites visited in private mode would get deleted: after “closing a private tab?” (P03), “closing all tabs?” (P09), “closing a [private] window?” (P11), “closing a session?” (P04; P11; P13; P21), or “shutting down a browser?” (P09; P14; P17; P20; P21; P22; P24). Also, five participants questioned whether or not one private session could be shared across multiple windows or tabs.

We also asked participants to suggest a new name for private mode, if any. All participants came up with random names: “non-private,” “everything but private,” “insecure,” “random mode,” and “useless.” Although all participants agreed that the term “private browsing” was misleading, there was no clear winner among the names they suggested.

Primary security goal. Most participants (21 out of 25) pointed out that none of the three disclosures explained the primary security goal of private browsing. Seven participants pointed out that although the Chrome disclosure said that “[a user’s] private browsing activity will be hidden from users sharing the same device,” it did not explain that a user of the device could easily monitor other users’ activities by infecting the device with a malware.

Several participants (17 out of 25) also mentioned that browser disclosures should have mentioned all types of attackers that could violate the security goal of private browsing. They reported that all critiqued disclosures mentioned a subset of all possible attackers (i.e., not the complete set).

Private browsing functionality. 16 out of 25 criticized the use of the following statement by all three disclosures: “[vendor] will save/won’t save the following information.” Participants explained that the statement implied the vendor would not save information on its servers after exiting private mode. Yet, the true meaning of the statement is that the
vendor will only delete private browsing-related information from the user’s local device, and not necessarily from the vendor’s servers.

Further, 22 out of 25 suggested that the technical explanation of private browsing functionality (e.g., whether cookies would be stored or deleted) should have been hid or deferred until the primary security goal was explained in detail, which none of the disclosures critiqued did. Participants mentioned that browser disclosures should have explained (in bullet points) what protection private mode actually offered (protecting against a local adversary). Yet, disclosures described how this protection was achieved (e.g., by deleting cookies), without explaining what protection the mode offered.

**Tracking protection.** 12 out 25 participants mentioned that existing browser disclosures should have made it clear that protecting against website tracking was not a security goal of private mode. Five participants argued that Brave had been working on reducing online tracking as a browser feature, and not as a private mode feature.

Further, four participants argued most browser vendors did not have the incentive to implement a private browsing mode that delivered the level of privacy expected by consumers, mainly because most web browsers (e.g., Chrome, Internet Explorer) were owned by companies (e.g., Google, Microsoft) that relied on targeting users with advertisements to generate revenue. Hence, participants explained that disclosures should not have used the term “tracking protection” – without explaining what the term meant – to advertise the use of private mode.

**Chrome performed better.** Many participants (18 out of 25) perceived the Chrome browser disclosure as relatively more informative than the disclosures of Brave and Firefox, as it used a list of bullet points to describe both private browsing functionality and attackers. In contrast, nine participants reported that the Brave and Firefox disclosures gave them the false sense that private mode aimed to protect against website tracking and ad targeting, increasing their expectations of the protection offered by private mode beyond reality. Also, eight participants mentioned they would use the private mode of Brave and Firefox to perform sensitive browsing activities (before they were given our tutorial); they said they were influenced by the strong statement in the Brave disclosure:
“Private tabs . . . always *vanish* when the browser is closed,” and the use of the shield icon by Firefox. Participants explained that the statement and the shield were misleading, and did not communicate the actual benefits of private mode.

Finally, we asked our participants to propose new disclosure designs to better communicate the actual protection of private mode. We discuss the findings in the next section.

### 8.4 Discussion

Our findings show the high-level description of private mode as a “private browsing tab” or a “private browsing window” is not only vague, but also misleading. Users’ mental models and perceptions of the term “private browsing” influence the understanding and usage of private mode in real life. Incorrect or inappropriate mental models – partially derived from this term – could lead users to overestimate the benefits of private mode. For example, some participants used private mode to visit webpages not running HTTPS with a valid TLS certificate, incorrectly believing private mode encrypted Internet traffic. Further, several participants associated private mode with end-to-end encrypted messaging tools, Tor, or VPN.

Additionally, only three participants – who identified as security and privacy experts – correctly and accurately explained the primary security goal of private mode. The vast majority of participants incorrectly believed private mode protected against *any* local attacker, without considering the scenario of a motivated local attacker who could infect a shared machine with a spyware and monitor users’ private browsing activities.

Therefore, it is critical to effectively communicate the actual protection private mode offers. Although users might learn about private mode from peers or online articles, effective browser disclosures remain the vendor’s most reliable channel to communicate information to users. Hence, drawing from the findings of our study and the browser disclosure designs our participants proposed, we distill the following recommendations to improve the design of disclosures:

**Explain the primary security goal.** As most participants pointed out, none of the
browser disclosures they critiqued explained the primary security goal of private mode. Although the Chrome disclosure (version 76.0.3809.100) had the following statement: “Other people who use this device won’t see your activity,” it did not explain that a malicious user of “this device” could monitor the private browsing activities of other users of the same device through a spyware or a key-logger. Thus, disclosures must explain that private mode only protects against an entity that takes control of the user’s machine after the user exits private mode.

**Explain when information will get deleted.** Several participants pointed out that the browser disclosures of both Chrome and Firefox did not explain when information (e.g., browsing history, cookies) about the websites visited in private mode would get deleted. Further, some participants mentioned that although the Brave disclosure (version 0.56.15) had the following statement: “[Information (e.g., cookies)] always vanish when the browser is closed,” it did not clearly communicate the actual functionality of private browsing: information related to a specific private browsing session gets deleted after the user terminates that session. Thus, browser designers should better communicate when information related to a private browsing session will get deleted (e.g., “when closing a private tab, window, or session.” (P02), “when closing the browser” (P09)).

**Explain where information will get deleted from.** All three disclosures our participants critiqued had the following statement: “Brave; Chrome; Firefox will not save the following information: browsing history, cookies, …” Several participants argued that this statement was misleading because it implied information related to a private browsing session would not be stored by the browser vendor. Browser designers should consider rewriting the statement to capture the correct intended meaning: information about websites visited in private mode will not be locally stored on the user’s device.

**Explain the threat model.** Private browsing does not hide activities performed in private mode from motivated local attackers, web attackers, employers, ISPs, browser vendors, and governments. All three critiqued browser disclosures mentioned only a subset of these attackers. Further, several participants mentioned that disclosures needed to clearly describe the entities it protected, and did not protect, against before explaining the detailed
functionality of private mode, as we explain next.

**Hide or defer the explanation of functionality.** All three disclosures mentioned different types of files (e.g., browsing history file, cookies, temporary files) that would get deleted after exiting private mode. However, the vast majority of participants did not feel confident explaining what these files meant. Further, several participants preferred that disclosures hid (x13) the explanation of the functionality of private mode or deferred (x9) it until its threat model was described; none of the disclosures our participants critiqued did so.

**Notify users when authenticated.** We found all participants used private mode while being authenticated to online services, incorrectly thinking their search history would get deleted after exiting the mode. Several participants noted they would like to have a mechanism that would detect when they had started browsing in private mode while being logged into a service.

**Avoid using uncertain or misleading words.** The Chrome disclosure had the following statement: “Your activity might still be visible to [the websites you visit, your employer, etc.]” According to many participants, the use of the word “might” could lead users to incorrectly believe that private mode could protect against, for example, website tracking.

Further, the Brave disclosure stated the following: “Private tabs . . . always vanish when the browser is closed.” However, it did not explain from where the information would get deleted, or rather would vanish, from. The use of the word “vanish” led several participants to incorrectly think that information would completely get removed not only from local devices, but also from web servers.

**Explain the utility of private mode.** Many participants did not necessarily use private mode to visit “embarrassing websites.” They used the mode to login into an online service using another personal account (e.g., logging into Facebook using two different accounts), debug and test software, or purchase a surprise gift for a family member or a friend. Some participants suggested that browser disclosures should promote the utility of private mode: what private mode could be useful for.
Use bullet points and bold fonts. In line with prior work (see Section 2.4), most participants used bullet points in their disclosure designs to explain the utility of private mode. Our participants also used bold fonts to emphasize important points (mainly, the main goal of private mode).

Rethink the name “private browsing”. As our results show, the term “private browsing” is misleading. Many participants were “shocked” and felt “vulnerable” upon learning the actual benefits and limitations of private mode. Several participants suggested different names for private mode. However, there was no clear winner among the names suggested. We hypothesize that explaining what protection private mode offers would be sufficient, without the need to mention the name “private browsing” or engineer a metaphor for it.

Finally, we encourage browser designers to validate the design guidelines we extracted from the findings of our study. For future work, we are going to design and test different disclosure prototypes using the Experience Sampling Method (ESM). One possible prototype would be to explain the primary security goal of private mode first, followed by a list of bullet points debunking the myths (or misconceptions) that users have about private mode. Firefox has recently added a link to a list of misconceptions about private mode to its disclosure (see Figure 8.4). However, users who click on the link will be directed to a long page explaining some of the misperceptions users have. We hypothesize users do not have the time to read the long page and understand what private mode achieves (and does not achieve). Also, the Firefox disclosure does not explain the main security goal of private mode.

8.5 Limitations

Our study has a number of limitations common to all qualitative research studies. First, the quality of qualitative research mainly depends on the interviewer’s individual skills. Therefore, to minimize bias, one researcher (thesis author), who was trained to conduct interviews and ask questions in an open and neutral way, conducted all interviews.
Second, some participants’ answers tended to be less detailed. However, the interviewer prompted participants to give full answers. Further, the interviewer gave participants a ten-minute break between the second and third parts of the study, to reduce interviewee fatigue [136].

Third, our qualitative work is limited by the size and diversity of our sample. Following recommendations from prior work to interview between 12 and 25 participants [186], we interviewed 25 participants until new codes stopped emerging.

8.6 Contributions to Thesis

In this chapter, we designed and conducted a user study to answer the seventh research question this thesis addresses: Can a user-centered approach to understanding users’ mental models and usage of a privacy-enhancing technology – other than secure communications – improve the end-user experience and design of that technology? If so, how (see Section 1.2)? Our primary contributions are as follows:

• We performed the first usability inspection of private mode in different web browsers using an analytic approach combining cognitive walkthrough and heuris-
tic evaluation.

- We conducted the first qualitative user study to explore why most users misunderstand the benefits and limitations of private browsing. We did so by conducting an interview-based study with both users and non-users of private mode. We explored users’ mental models of private browsing and its security goals, and how these models influence users’ understanding and usage of private mode.

- We performed the first participatory design study to improve the design of browser disclosures related to private browsing mode. Prior work [20,23,24] has suggested that existing browser disclosures should be redesigned to better convey the actual benefits and limitations of private mode. In this paper, we did so by allowing our participants to take part in designing these disclosures; participants critiqued the browser disclosures of Brave, Firefox, and Google Chrome, explained why these disclosures were misleading, and then designed new ones.

- We extracted a set of design recommendations that we encourage browser designers to validate (by implementing and testing), in order to design more effective browser disclosures.
Chapter 9

Conclusion

9.1 Summary of Thesis

In the era of mass surveillance, computer security and privacy experts have always advocated the widespread adoption and use of PETs. However, it remains unclear if users understand what protection these technologies offer. Unlike prior work, we took a user-centered approach to evaluating the end-user experience, and improving the design, of two PETs: secure (mainly encrypted) communications and private browsing.

Prior studies of secure communications have shown poor usability primarily hampers the adoption of secure communication tools. However, we found – by conducting five qualitative (n=102) and two quantitative (n=425) user studies – that, in addition to poor usability, lack of utility and incorrect user mental models of how secure communications work are primary obstacles to adoption.

Users will not adopt a communication tool that is both usable and secure, but lacks utility (due to, e.g., the tool’s small userbase, low quality of service, lack of interoperability). Further, most users do not know what it means for a usable and secure tool that is widely-adopted and offers utility (e.g., WhatsApp) to be end-to-end encrypted. Incorrect mental models of encryption lead people to use less secure channels that they incorrectly perceive as more secure than end-to-end encrypted tools.
Thus, we argue in this thesis the key user-related challenge for secure communications is no longer fostering adoption, but emphasizing appropriate use. This does not mean that fostering adoption is not as important as highlighting correct use, but we argue that the usable security and privacy community has been focusing on spurring adoption of encrypted communications for the past twenty years [5], operating under the assumption that once an encrypted tool has been widely adopted, adoptees will use or continue using that tool appropriately. Our findings show that this is not necessarily true due to users’ incorrect mental models of how encrypted communications work, or what security properties or protection encrypted communications provide. Therefore, we need to focus on highlighting appropriate use by helping people who already use secure tools avoid sending information, especially information they regard as sensitive, over less secure channels. By employing participatory design, we took a user-centered approach to designing effective descriptions that explain the security properties of end-to-end encrypted communications.

Additionally, we took a user-centered approach (as part of a validation study) to evaluating and improving the end-user experience of another PET: private browsing mode. We conducted the first qualitative user study (n=25) to explore the factors that influence users’ adoption and usage of private mode in different modern web browsers, as well as investigate users’ mental models of private mode. We also employed participatory design and proposed guidelines to help create informative browser disclosures that explain the security properties of private mode.

The primary contributions of this thesis are as follows:

1. We designed and conducted the largest and broadest qualitative user study to date (see Chapter 3). We found, unlike prior work, poor or lack of usability is not the only barrier to adopting secure communication tools. Lack of utility and incorrect users’ mental models of secure communications are key barriers to adoption.

2. We found when people rank communication tools based on how secure they are, they base their rankings on how large the tool’s userbase is, QoS, social factors, and other criteria, rather than assessing the security properties different secure tools offer.
3. Most people cannot establish the link between a security mechanism (e.g., encryption) and the security properties offered by that mechanism (e.g., confidentiality, integrity, authentication). The computer security and privacy community has been usually operating under the assumption that if an encrypted communication tool reaches critical mass, people will use that tool appropriately. Hence, many efforts have been made – thus far – to address the usability issues of classical secure messaging systems (most notably, PGP [5]), in an attempt to make these systems widely-adopted. However, to date, these systems suffer from low adoption, and most people do not know what security properties they actually offer (see Chapter 4).

4. We found that adoption is necessary, but not sufficient. We found that a communication tool – like WhatsApp – that is usable, widely-adopted, and end-to-end encrypted may not be used by most people to send information they regard as sensitive, incorrectly believing that other methods of communication (e.g., SMS) are more secure than end-to-end encrypted communication tools. This finding highlights the need to focus on both fostering adoption and emphasizing appropriate use (see Chapter 6).

5. We showed why engineering metaphors – especially, without involving users in the design of these metaphors – might not be the ideal way to convey the security properties of end-to-end encrypted communications. Unlike prior work that has focused on making encryption easier for mainstream users to understand (see [3] and [80]), mainly through engineering new metaphors to explain how encryption works, we found that most non-expert users are interested in what encryption achieves, and not what encryption is or how it works in the context of secure communications. Therefore, we showed how participatory design could be used to design effective descriptions to explain the security properties of encryption (see Chapter 7).

6. The findings of and the insights gleaned from this thesis were used by the EFF to rethink their approach of how to provide information to non-expert users about the security properties different communication tools actually offer. The scorecard was initially an attempt to provide a “consumer guide” to encourage mainstream users
to adopt and use secure communication tools. We evaluated the effectiveness of the scorecard in this thesis and found that the current version of the scorecard was not effective, which led the EFF to archive the scorecard and think of different ways to design a new one.

7. We designed and conducted the first qualitative user study to explore the adoption and usage of private browsing mode (see Chapter 8). We identified usability issues in the user interface of private mode in different browsers. We also found that most people have inappropriate mental models of private mode and do not understand the security goal of private browsing. Additionally, we found none of the three studied browser disclosures communicated the main security goal of private mode. Drawing from these findings, we extract a set of guidelines to improve the design of disclosures related to private mode. We also propose a new disclosure design. Some of the ideas described in this thesis were used by Brave to improve their disclosure design.

8. Finally, we explained the design of all user studies described in this thesis in detail. We also provided the pre-screening questionnaires and surveys in the appendix, allowing researchers to replicate our studies with different user groups in different contexts in the future.

9.2 Future Work

9.2.1 Designing User-Centered Secure Communication Tools Supporting Group Chat

People around the world use insecure group communication tools. These tools, such as Facebook Messenger, Google Hangouts, Skype, GroupMe, Telegram, and so forth, are very popular for group chatting, but they often do not include security features, or hide those features beneath a complex user interface. Even when tools include secure communication features, existing research as well as the research described in this thesis show that users tend not to understand these features, do not turn them on when they are
optional, and do not know how to use these features to protect themselves against attacks.

Despite the current lack of secure group communications (from the tools themselves or from user practices), people around the world, especially vulnerable populations, need secure multi-party communication systems. Group communications can cover a wide range of topics that may be the focus of censorship, such as religion, politics, and sexuality.

To this end, to design and build communication tools that effectively protect users, we need to understand how these users perceive secure communications, and what influences their decision to adopt (or not adopt) secure tools. While the usable security community has made some progress in this area with regard to one-to-one communications (as we demonstrate in this thesis), there is relatively little work that explores user needs, practices, and mental models of secure communications in the context of group chat.

The use of group communications via instant messaging tools has been previously studied in individual efforts targeting different tools and the cultures that use them; e.g., WeChat (China) [187], KakaoTalk (Korea) [188], and WhatsApp (UK) [189]. These endeavours, however, touched only briefly on group communication needs and practices, did not explore the security/privacy needs of their respondents in this domain, and did not attempt to examine these issues in a single, cross-cultural study allowing for direct comparison between one user group and another. Subsequently, the community lacks a clear picture of what security/privacy needs have gone unmet for group communication users.

For future work, we seek to generate foundational knowledge for the user-centered design of communication tools that support secure group chat. We plan to design and conduct a cross-cultural study to identify the salient features people want in secure group chat and characterize perceptions of its security and privacy. Specifically, we aim to:

1. Compare user perceptions of secure group chat with the actual security offered by existing group chat protocols.
2. Identify what threats users want to protect against when participating in group chat, and how users perceive existing tools help them cope with those threats.

3. Explore when users need confidentiality (secrecy of content) versus when they need anonymity.

4. Investigate how the perceived security of group chat influences user behaviour with respect to the frequency of usage of a particular communication tool, range of topics discussed, sensitivity of information sent, and so forth.

5. Identify adoption/usability factors: why, when, and how people use secure group chat.

We are also interested in how culture influences user needs and perceptions on these topics. Hence, we will conduct a study of countries from the Global South, and then compare our findings with a simultaneous study of countries in the Global North. By comparing countries in the Global South to each other, and to the Global North, we will be able to identify issues and perspectives that are unique to a particular country, those that are shared across the Global South, and those that are shared even more broadly. Identifying these cultural differences will enable us to call attention to particular needs that are currently unmet by developers.

The insights gleaned from this work will add to the body of knowledge of secure communications (taking into account user needs, practices, and mental models), as well as help developers build tools that can support user needs and practices, especially those living in repressive regimes. Ultimately, our contributions/outcomes will be three-fold. We will (1) compile a list of recommendations that will guide the development of secure, widely-adopted tools that support secure group chat, while better communicating the security properties they offer to users, (2) translate our findings into use cases, design patterns, and guidelines that developers can use, (3) disseminate our results to developers in a variety of forums to ensure that the development of secure group chat software is in alignment with the needs and practices of users.

The survey questionnaire for this work can be found in Appendix E.
9.2. Future Work

9.2.2 Developing Culturally-Appropriate Educational Materials

Secure communication tools have relatively low adoption rates across the world. Further, while the use of secure communication tools is especially important for users in regions with restricted Internet freedom, such tools can provide an important access and security from potentially threatening bodies (e.g., the government). Additionally, educational materials promoting such tools and even the technologies themselves may need to be adapted cross-culturally in order to aid adoption and appropriate use, especially as most secure communication tools are not developed in the context of Internet-restricted countries, nor in the cultural context of, for example, the Global South.

In order to increase the adoption of secure communication tools both in countries with restricted Internet freedom and across the Global South, we propose a two-phase project that will (1) develop a cross-cultural understanding of barriers to secure communication tool adoption in order to (2) develop culturally-appropriate educational materials via in-situ participatory design studies with community collaborators to educate users about the benefits of secure communications, and address misperceptions and misunderstandings, in order to increase adoption of secure communication tools and Internet freedom more broadly. Co-designed, culturally-aware and research-based educational tools have had a profound impact (e.g., thousands of users) on adoption of other “social good” devices, such as condoms [190]; yet, to our knowledge, no similar work (except for our small-scale participatory design study described in Chapter 7) – especially focused on secure communications and involving in-situ studies in multiple countries – has been conducted in privacy and security.

To this end, we aim to:

1. Release professional-quality, research-backed educational materials that can make a (statistically) significant and measurable impact on the adoption of secure tools in three broad regions: countries with varying levels of Internet freedom in the Global South; countries with differing political and privacy climates within Europe; the USA.
2. Even more broadly, set a good example for researchers and engineers of developing educational and training materials through culturally-aware co-design.

3. Make actionable, research-driven recommendations for future technical development of secure communication tools.

4. Through a combination of (1) and (2), help users – especially the most vulnerable users – enjoy the many positive benefits of a connected world with the opportunity for free expression (which is known to have significant psychological and economic benefits). Why should these opportunities be restricted to technically-savvy users in technology-advantaged communities?

5. Finally, make a significant contribution to the body of knowledge on user preferences for security and privacy-preserving tools at a cross-cultural level; emphasizing not only usability challenges but also tensions between perceptions of the intended users of such tools and self-perceptions. Such work can not only assist the research community, but strengthen policy arguments (e.g., for the FTC) to ensure future freedom of development and adoption for such tools.

This future work will (1) benefit every-day people who would like to use some form of encrypted chat to communicate. For example, in countries where freedom of speech is guaranteed, people may need encryption to discuss mental health issues. Alternatively, people living within repressive regimes need, for example, to discuss politics secretly. The purpose of this project is to study users’ perceptions of encrypted communication tools, and raise concerns about government surveillance in both the Global North and the Global South; (2) help developers who are interested in building encrypted communication tools. We plan to conduct constructive research by providing clear and concrete recommendations that will help developers address unmet needs among diverse communities, as well as improve the user experience of existing tools. Current solutions are built by organizations, and, hence, they are not user-driven. We plan to conduct user-centered research, with the aim to fill a gap in both knowledge and research of usable and secure communications.
9.2. Future Work

We also plan to develop culturally-appropriate educational materials for other security mechanisms and privacy tools, such as verification fingerprints, private browsing, and anonymity tools.
Bibliography


[27] Juan Ramón Ponce Mauriés, Kat Krol, Simon Parkin, Ruba Abu-Salma, and M. Angela Sasse. Dead on Arrival: Recovering from Fatal Flaws in Email En-


[113] Pedro Giovanni Leon, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu. What Do Online Behavioral Advertising Disclo-


<table>
<thead>
<tr>
<th>Citation</th>
<th>Author(s)</th>
<th>Title</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>165</td>
<td>Clayton Lewis and John Rieman</td>
<td><em>Task-Centered User Interface Design: A Practical Introduction</em></td>
<td>1993</td>
</tr>
<tr>
<td>166</td>
<td>Tasha Hollingsed and David G. Novick</td>
<td>Usability Inspection Methods after 15 Years of Research and Practice</td>
<td>In <em>Proc. Conference on Design of Communication</em>, 2007</td>
</tr>
<tr>
<td>167</td>
<td>Ann Cavoukian</td>
<td>Privacy by Design</td>
<td><em>IEEE Technology and Society Magazine</em>, 2012</td>
</tr>
<tr>
<td>171</td>
<td>John M. Carroll and Mary Beth Rosson</td>
<td><em>Paradox of the Active User</em></td>
<td>The MIT Press, 1987</td>
</tr>
</tbody>
</table>


Appendix A

Pre-Screening Questionnaire (Secure Communications)
Q1 Please indicate which of the following ranges your age falls within.

- Under 18 (1)
- 18 – 20 (2)
- 21 – 30 (3)
- 31 – 40 (4)
- 41 – 50 (5)
- 51 – 60 (6)
- 61 – 70 (7)
- 70+ (8)
- Prefer not to answer (9)

Q2 Please indicate your gender.

- Male (1)
- Female (2)
- Non-binary (3)
- Other: (4) ___________________________________________________________
- Prefer not to answer (5)
Q3  What is your highest level of education? If you are currently enrolled, please specify the highest level/degree completed.

- Some high-school education  (1)
- High-school education or equivalent  (2)
- Vocational training (e.g., NVQ, HNC, NHD)  (3)
- Associate’s degree (e.g., AS, AB)  (4)
- Some college/undergraduate education; no degree  (5)
- College/undergraduate degree (e.g., BSc, BA)  (6)
- Graduate/postgraduate degree (e.g., MSc, MA, MBA, PhD)  (7)
- Other:  (8) ________________________________________________

End of Block: A

Start of Block: B

Q4 If you have pursued (or are currently pursuing) a college degree (e.g., B.A., B.Sc.), what is your area of study?

__________________________________________________________

Q5 If you have pursued (or are currently pursuing) a graduate degree (e.g., M.A., M.Sc., Ph.D.), what is your area of study?

__________________________________________________________

End of Block: B

Start of Block: C
Q6 What is your current employment status?

- Employed (1)
- Unemployed (2)
- Student (3)
- Retired (4)
- Other: ________________________________________________
- Prefer not to answer (6)

Q7 If employed, what is your current occupation?
________________________________________________________________

Q8 Which of the following best describes your race?

- White (1)
- Black (2)
- Asian (3)
- Mixed race (4)
- Other: ________________________________________________
- Prefer not to answer (6)

End of Block: C
Q9 Do you own a desktop computer and/or laptop?

- Yes (1)
- No (2)
- Do not know (3)

Q10 Do you own a smartphone?

- Yes (1)
- No (2)
- Do not know (3)
<p>| | | | | | | | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Q11</td>
<td>Which of the following communication tools/applications have you heard of?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Adium (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Blackberry Messenger (BBM) (2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Blackberry Protect (3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ChatSecure (4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confide (5)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>eBuddy XMS (6)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Facebook Messenger (7)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FaceTime (8)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Google Hangouts (9)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>iMessage (10)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Jitsi (11)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Kik Messenger (12)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ostel (13)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pidgin (14)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>QQ (15)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Signal (16)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Silent Phone/Silent Text (17)

Skype (18)

Snapchat (Direct Snaps) (19)

Surespot (20)

Telegram (21)

TextSecure (22)

Threema (23)

Viber (24)

WhatsApp (25)

Wickr (26)

Yahoo! Messenger (27)

Instagram Direct Messages (28)

Twitter Direct Messages (29)

LinkedIn InMail (30)

Other: (31) ________________________________________________

End of Block: E

Start of Block: F
Which of the following communication tools/applications have you heard of?
<table>
<thead>
<tr>
<th>Q12</th>
<th>Heard of it, but have not used it (1)</th>
<th>Used it before, but stopped using it (2)</th>
<th>Use it currently (3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adium (x1)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Blackberry Messenger (BBM) (x2)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Blackberry Protect (x3)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>ChatSecure (x4)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Confide (x5)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>eBuddy XMS (x6)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Facebook Messenger (x7)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>FaceTime (x8)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Google Hangouts (x9)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>iMessage (x10)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Jitsi (x11)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Kik Messenger (x12)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Ostel (x13)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Pidgin (x14)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>QQ (x15)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Application</td>
<td>Selection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signal (x16)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Silent Phone/Silent Text (x17)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skype (x18)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Snapchat (Direct Snaps) (x19)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Surespot (x20)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telegram (x21)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TextSecure (x22)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threema (x23)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Viber (x24)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WhatsApp (x25)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wickr (x26)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yahoo! Messenger (x27)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instagram Direct Messages (x28)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Twitter Direct Messages (x29)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LinkedIn InMail (x30)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other: (x31)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Q13 What computing platforms do you use to message or communicate with your communication partners? (select all that apply)

- Android (e.g., Galaxy Nexus, Galaxy Samsung) (1)
- iOS (e.g., iPhone) (2)
- Mac OS X (3)
- Microsoft Windows (4)
- Other (5) ________________________________________________

End of Block: F

Start of Block: G

Q14 Do you have a computer science or engineering degree?

- Yes (1)
- No (2)

Q15 Have you ever configured a network firewall?

- Yes (1)
- No (2)
- Do not know (3)
Q16 Have you ever written a computer program?

- Yes (1)
- No (2)
- Do not know (3)

Q17 Have you ever changed your web browser’s search engine (e.g., Google, Yahoo! Search, Bing, Ask.com)?

- Yes (1)
- No (2)
- Do not know (3)

Q18 Have you ever changed your web browser’s homepage?

- Yes (1)
- No (2)
- Do not know (3)

Q19 Have you ever registered a domain name?

- Yes (1)
- No (2)
- Do not know (3)
Q20 Have you ever designed a website?

- Yes (1)
- No (2)
- Do not know (3)

Q21 Have you ever unscrewed anything on your PC, laptop, or mobile phone?

- Yes (1)
- No (2)
- Do not know (3)

End of Block: G

Start of Block: H

Q22 Have you ever lost data because of an infected computer (e.g., a virus)?

- Yes (1)
- No (2)
- Do not know (3)
Q23 Have you ever been impersonated (or your personal account credentials been stolen)?

- Yes (1)
- No (2)
- Do not know (3)

Q24 Have you ever fallen for a phishing email?

- Yes (1)
- No (2)
- Do not know (3)

Q25 Has your personal data ever been misused?

- Yes (1)
- No (2)
- Do not know (3)

Q26 Have you ever received spam?

- Yes (1)
- No (2)
- Do not know (3)
End of Block: II
Appendix B

Pre-Screening Questionnaire (Private Browsing)
Q1
Please indicate your gender.

- Male (1)
- Female (2)
- Non-binary (3)
- Other: ____________________________
- Prefer not to answer (5)

Q2
Please indicate which of the following ranges your age falls within.

- Under 18 (1)
- 18 – 24 (2)
- 25 – 34 (3)
- 35 – 44 (4)
- 45 – 54 (5)
- 55 – 64 (6)
- 65 – 74 (7)
- 75+ (8)
- Prefer not to answer (9)
Q3 Which of the following best describes your race?

- White (1)
- Black (2)
- Asian (3)
- Mixed race (4)
- Other: ________________________________ (5)
- Prefer not to answer (6)

End of Block: A

Start of Block: B

Q4 What is your highest level of education? If you are currently enrolled, please specify the highest level/degree completed.

- Some high-school education (1)
- High-school education or equivalent (2)
- Vocational training (e.g., NVQ, HNC, NHD) (3)
- Associate’s degree (e.g., AS, AB) (4)
- Some college/undergraduate education; no degree (5)
- College/undergraduate degree (e.g., BSc, BA) (6)
- Graduate/postgraduate degree (e.g., MSc, MA, MBA, PhD) (7)
- Other: ________________________________ (8)
Q5 What is your current employment status?

- Employed (1)
- Unemployed (2)
- Student (3)
- Retired (4)
- Other: ________________________________
- Prefer not to answer (6)

End of Block: B

Start of Block: C

Q6 Please select the digital security requirements that you have at work, if any.

- Sending emails with encryption (1)
- Using a dedicated phone for work tasks (2)
- Using two-factor authentication to access your work devices (3)
- Always using a VPN when working on work activities (4)
- Using private browsing (9)
- Other: ________________________________
- I do not have digital security requirements. (7)
- Prefer not to answer (6)
Q7  Do you receive training about digital security or privacy at work?

- Yes, yearly (1)
- Yes, a few times a year (2)
- Yes, monthly (3)
- Yes, other: (7) ________________________________
- No (4)
- Prefer not to answer (5)

Q8  Do you feel at risk due to your job duties?

- Yes, physical risk due to stalking, threats, or attack from people who do not like what I do. (1)
- Yes, cyber risk due to stalking, threats, or attack from people who do not like what I do. (2)
- Yes, other: (3) ________________________________
- No (4)
- Prefer not to answer (5)
Q9 Which of the following best describes your educational background or job field?

- I have an education in, or work in, the field of computer science, computer engineering, or IT. (1)
- I do not have an education in, nor do I work in, the field of computer science, computer engineering, or IT. (2)
- Prefer not to answer (3)

Q10 Have you written a computer program?

- Yes (1)
- No (2)
- Do not know (3)
Q11 How familiar are you with the following programming languages?

<table>
<thead>
<tr>
<th></th>
<th>Extremely familiar (1)</th>
<th>Very familiar (2)</th>
<th>Moderately familiar (3)</th>
<th>Slightly familiar (4)</th>
<th>Not familiar at all (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C++</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Java</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JavaScript</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PHP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Python</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ruby</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q12 How often do people ask you for computer-related advice?

- Never (1)
- Sometimes (2)
- Most of the time (3)
- Always (4)
Q13 How often do you use the following web browsers?

<table>
<thead>
<tr>
<th>Browser</th>
<th>Have not heard of it (1)</th>
<th>Have heard of it, but have not used it (2)</th>
<th>Have used it before, but stopped using it (3)</th>
<th>Use it currently (4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brave (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firefox (2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Chrome (3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Explorer (4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Edge (5)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Opera (6)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safari (7)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tor Browser (8)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other: (9)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q14 Why do you currently use more than one web browser, and what do you use each browser for?

________________________________________________________________
________________________________________________________________
Q15 Which web browser do you use the most, and why?

________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________

Q16 How many hours do you spend daily on your desktop and/or laptop browsing?

________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________

Q17 How many hours do you spend daily on your mobile phone browsing?

________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________
Appendix B. Pre-Screening Questionnaire (Private Browsing)
Appendix C

Survey: Evaluating the End-User Experience of Telegram
Start of Block: A

Q1 Please enter your Prolific Academic ID.

End of Block: A

Start of Block: B

Q2 Have you ever used the Telegram instant messaging app?

☐ Yes, I currently use Telegram. (1)

☐ Yes, I had used Telegram in the past, but stopped using it. (2)

☐ No, I have not used Telegram. (3)

End of Block: B

Start of Block: C

Display This Question:

If Have you ever used the Telegram instant messaging app? = Yes, I had used Telegram in the past, but stopped using it.
Q3 Why did you decide to use Telegram? (please select all that apply)

☐ I was involved in an activity where everyone involved was using it (1)
☐ Many of the people I know were using it (2)
☐ My contacts were using it (3)
☐ Telegram was easy to use (4)
☐ I felt Telegram was secure (5)
☐ Telegram was fun to use (6)
☐ Telegram was fast to use (7)
☐ Other: (8) ________________________________________________

Display This Question:
If Have you ever used the Telegram instant messaging app? = Yes, I had used Telegram in the past, but stopped using it.

Q4 What did you value most about Telegram? (please drag and drop the elements to rank them from the most to the least valuable)

_____ Easy to use (1)
_____ Secure (2)
_____ Fun to use (3)
_____ Fast to use (4)
_____ Please move this option to the bottom (9)
_____ That I can stay in touch with the people I know who are using it (5)
_____ Other: (6)

End of Block: C

Start of Block: D
Q5 What did you use Telegram for? (please select all that apply)

☐ Communicating with family members, friends and/or colleagues (1)

☐ Making plans (2)

☐ Arranging meetings (3)

☐ Discussing work (4)

☐ Sharing personal views (e.g., political beliefs) (5)

☐ Campaigning for a cause (6)

☐ Other: (7) ________________________________________________
Q6. Why did you decide to stop using Telegram? (please select all that apply)

- I didn’t have a use for it (1)
- It was hard to make Telegram work (2)
- I didn’t trust Telegram or its makers (3)
- I already used other messaging apps (4)
- I had heard negative things about people who use Telegram (5)
- My contacts had stopped using it (6)
- Other: (7) ________________________________________________

Display This Question:
If Have you ever used the Telegram instant messaging app? = Yes, I had used Telegram in the past, but stopped using it.

Q7. How long ago did you stop using Telegram?

- Less than six months ago (1)
- 6-12 months ago (2)
- 1-3 years ago (3)
- Longer than 3 years ago (4)

Display This Question:
If Have you ever used the Telegram instant messaging app? = Yes, I had used Telegram in the past, but stopped using it.
Q8 Did you ever share sensitive information using Telegram? By sensitive, we mean information that was for the intended recipient only, and which you would not want others to have.

   - Yes, I shared sensitive information using Telegram (1)
   - No, but I shared sensitive information using a messaging app other than Telegram (2)
   - No, I did not share sensitive information using any messaging app (3)
   - I don’t remember (4)

End of Block: D

Start of Block: E

Display This Question:

  If Have you ever used the Telegram instant messaging app? = Yes, I had used Telegram in the past, but stopped using it.

Q9 Were your one-to-one (not group) communications using Telegram end-to-end encrypted?

   - Yes, they were end-to-end encrypted (1)
   - Yes, but I had to turn end-to-end encryption on (2)
   - No, they were not end-to-end encrypted (3)
   - I don’t know what encryption is or why it is important (5)
   - I don’t know (4)

Display This Question:

  If Have you ever used the Telegram instant messaging app? = Yes, I had used Telegram in the past, but stopped using it.
Q10 Were your group communications using Telegram end-to-end encrypted?

- Yes, they were end-to-end encrypted (1)
- Yes, but I had to turn end-to-end encryption on (2)
- No, they were not end-to-end encrypted (3)
- I don't know what encryption is or why it is important (5)
- I don't know (4)
- I didn't use Telegram's group chat (6)

Display This Question:
If Have you ever used the Telegram instant messaging app? = Yes, I had used Telegram in the past, but stopped using it.

Q11 When you answered the questions above, did you consider:

- Telegram's secret chats (1)
- Telegram's non-secret chats (2)
- All Telegram's chats in general (3)
- I did not know Telegram has different types of chat (4)

End of Block: E
Q12 For each of the following actions (reading, listening to, modifying, and impersonating), select who you think could do it.

<table>
<thead>
<tr>
<th>Action Description</th>
<th>Could read my Telegram messages (1)</th>
<th>Could listen to my Telegram phone calls (2)</th>
<th>Could modify my Telegram communications (3)</th>
<th>Could impersonate me on Telegram (communicate with others pretending to be me) (4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No one (9)</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>People who work at Telegram (1)</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>Someone with a technical background or a computer science degree (2)</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>People who are up to no good (3)</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>The government of the country I live in (in this case, the UK government) (4)</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>Another country’s government (5)</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>My Internet service provider (ISP) (6)</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>Corporations other than the company that makes/develops Telegram (7)</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>People who have physical access to my mobile phone (11)</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
</tbody>
</table>
If Have you ever used the Telegram instant messaging app? = Yes, I had used Telegram in the past, but stopped using it.

Q13 When you answered the question on the previous page, did you consider:

- Telegram's secret chats (1)
- Telegram's non-secret chats (2)
- All Telegram's chats in general (3)
- I did not know Telegram has different types of chat (4)
Q14 Why did you decide to use Telegram? (please select all that apply)

☐ I was involved in an activity where everyone involved was using it (1)

☐ Many of the people I know were using it (2)

☐ My contacts were using it (3)

☐ Telegram was easy to use (4)

☐ I felt Telegram was secure (5)

☐ Telegram was fun to use (6)

☐ Telegram was fast to use (7)

☐ Other: (8) ________________________________________________________

---

Display This Question:
If Have you ever used the Telegram instant messaging app? = Yes, I currently use Telegram.

----

Q15 What do you value most about Telegram? (please drag and drop the elements to rank them from the most to the least valuable)

_____ Easy to use (1)
_____ Secure (2)
_____ Fun to use (3)
_____ Fast to use (4)
_____ Please move this option to the bottom (7)
_____ That I can stay in touch with the people I know who are using it (5)
_____ Other: (6)

End of Block: I

Start of Block: J
Q16 What do you use Telegram for? (please select all that apply)

☐ Communicating with family members, friends and/or colleagues (1)

☐ Making plans (2)

☐ Arranging meetings (3)

☐ Discussing work (4)

☐ Sharing personal views (e.g., political beliefs) (5)

☐ Campaigning for a cause (6)

☐ Other: (7) ________________________________________________

Q17 Have you ever shared sensitive information using Telegram? By sensitive, we mean information that was for the intended recipient only, and which you would not want others to have.

☐ Yes, I have shared sensitive information using Telegram (1)

☐ No, but I have shared sensitive information using a messaging app other than Telegram (2)

☐ No, I haven't shared sensitive information using any messaging app (3)

☐ I don’t remember (4)
Display This Question:
If Have you ever used the Telegram instant messaging app? = Yes, I currently use Telegram.

Q18 Are your one-to-one (not group) communications using Telegram end-to-end encrypted?

- Yes, they are end-to-end encrypted (1)
- Yes, but I have to turn end-to-end encryption on (2)
- No, they are not end-to-end encrypted (3)
- I don't know what encryption is or why it is important (5)
- I don't know (4)

Display This Question:
If Have you ever used the Telegram instant messaging app? = Yes, I currently use Telegram.

Q19 Are your group communications using Telegram end-to-end encrypted?

- Yes, they are end-to-end encrypted (1)
- Yes, but I have to turn end-to-end encryption on (2)
- No, they are not end-to-end encrypted (3)
- I don't know what encryption is or why it is important (5)
- I don't know (4)
- I don't use Telegram's group chat (6)
Q20 When you answered the questions above, did you consider:

- Telegram's secret chats (1)
- Telegram's non-secret chats (2)
- All Telegram's chats in general (3)
- I did not know Telegram has different types of chat (4)
Q21 For each of the following actions (reading, listening to, modifying, and impersonating), select who you think could do it.

<table>
<thead>
<tr>
<th>Action</th>
<th>Could read my Telegram messages (1)</th>
<th>Could listen to my Telegram phone calls (2)</th>
<th>Could modify my Telegram communications (3)</th>
<th>Could impersonate me on Telegram (communicate with others pretending to be me) (4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No one (9)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>People who work at Telegram (1)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Someone with a technical background or a computer science degree (2)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>People who are up to no good (3)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>The government of the country I live in (in this case, the UK government) (4)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Another country’s government (5)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>My Internet service provider (ISP) (6)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Corporations other than the company that makes/develops Telegram (7)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>People who have physical access to my mobile phone (11)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>
If Have you ever used the Telegram instant messaging app? = Yes, I currently use Telegram.

Q22 When you answered the question on the previous page, did you consider:

- Telegram's secret chats (1)
- Telegram's non-secret chats (2)
- All Telegram's chats in general (3)
- I did not know Telegram has different types of chat (4)

Q23 When you start communicating with a new contact using Telegram, have you ever needed to wait for your contact to go online?

- Yes, I sometimes need to wait (1)
- No, I send messages immediately (2)
- I'm not sure (3)
Q24 What is your main instant messaging app?

- BlackBerry Messenger (1)
- Facebook Messenger (2)
- Google Hangouts (3)
- iMessage (4)
- Instagram Direct (5)
- KakaoTalk (6)
- Signal (7)
- Skype (8)
- Slack (9)
- Snapchat (10)
- Telegram (11)
- Viber (12)
- WeChat (13)
- WhatsApp (14)
- Other: (15) ________________________________
Q25 Do you consider your main instant messaging app ($Q24/ChoiceGroup/SelectedChoices$) to be more useful than, as useful as, or less useful than Telegram?

- More useful (1)
- As useful as (2)
- Less useful (3)

Q26 Why do you think $Q24/ChoiceGroup/SelectedChoices$ is more useful than Telegram?

____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________

Q27 Why do you think $Q24/ChoiceGroup/SelectedChoices$ is as useful as Telegram?

____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
Display This Question:
If you consider your main instant messaging app (${q://QID187/ChoiceGroup/SelectedChoices}) to be... = Less useful

Q28 Why do you think ${Q24/ChoiceGroup/SelectedChoices} is less useful than Telegram?

End of Block: Q

Start of Block: R

Display This Question:
If Have you ever used the Telegram instant messaging app? != No, I have not used Telegram.
And What is your main instant messaging app? != Telegram

Q29 Did you ever share sensitive information using ${Q24/ChoiceGroup/SelectedChoices}? By sensitive, we mean information that was for the intended recipient only, and which you would not want others to have.

○ Yes, I shared sensitive information using ${Q24/ChoiceGroup/SelectedChoices} (1)

○ No, but I shared sensitive information using a messaging app other than ${Q24/ChoiceGroup/SelectedChoices} (2)

○ No, I did not share sensitive information using any messaging app (3)

○ I don’t remember (4)
Q30 Are your one-to-one (not group) communications using ${Q24/ChoiceGroup/SelectedChoices}$ end-to-end encrypted?

- Yes, they are end-to-end encrypted (1)
- Yes, but I have to turn end-to-end encryption on (2)
- No, they are not end-to-end encrypted (3)
- I don’t know (4)
- I don’t know what encryption is or why it is important (5)

Q31 Are your group communications using ${Q24/ChoiceGroup/SelectedChoices}$ end-to-end encrypted?

- Yes, they are end-to-end encrypted (1)
- Yes, but I have to turn end-to-end encryption on (2)
- No, they are not end-to-end encrypted (3)
- I don’t know what encryption is or why it is important (5)
- I don’t know (4)
- I don’t use ${Q24/ChoiceGroup/SelectedChoices}$’s group chat (6)
Display This Question:

If Have you ever used the Telegram instant messaging app? != No, I have not used Telegram.

And What is your main instant messaging app? != Telegram
Q32 For each of the following actions (reading, listening to, modifying, and impersonating), select who you think could do it.

<table>
<thead>
<tr>
<th></th>
<th>could read messages (1)</th>
<th>could listen to phone calls (2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>People who work at</td>
<td></td>
<td></td>
</tr>
<tr>
<td>${Q24/ChoiceGroup/SelectedChoices} (1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Someone with a technical background or a computer science degree (2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>People who are up to no good (3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The government of the country I live in (in this case, the UK government) (4)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Another country’s government (5)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>My Internet service provider (ISP) (6)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corporations other than the company that makes/develops ${Q24/ChoiceGroup/SelectedChoices} (7)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other: (8)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No one (9)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I don’t know (10)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

End of Block: S

Start of Block: T
If you have ever used the Telegram instant messaging app? = No, I have not used Telegram.

Q33 Why did you decide to use ${Q24/ChoiceGroup/SelectedChoices}$? (please select all that apply)

- [ ] I was involved in an activity where everyone involved was using it (1)
- [ ] Many of the people I know were using it (2)
- [ ] My contacts were using it (3)
- [ ] ${Q24/ChoiceGroup/SelectedChoices}$ was easy to use (4)
- [ ] I felt ${Q24/ChoiceGroup/SelectedChoices}$ was secure (5)
- [ ] ${Q24/ChoiceGroup/SelectedChoices}$ was fun to use (6)
- [ ] ${Q24/ChoiceGroup/SelectedChoices}$ was fast to use (7)
- [ ] Other: (8) ________________________________________________

If you have ever used the Telegram instant messaging app? = No, I have not used Telegram.

Q34 What do you value most about ${Q24/ChoiceGroup/SelectedChoices}$? (please drag and drop the elements to rank them from the most to the least valuable)

1. Easy to use
2. Secure
3. Fun to use
4. Fast to use
5. Please move this option to the bottom
6. That I can stay in touch with the people I know who are using it
7. Other:
Q35 What do you use for? (please select all that apply)

- [ ] Communicating with family members, friends and/or colleagues (1)
- [ ] Making plans (2)
- [ ] Arranging meetings (3)
- [ ] Discussing work (4)
- [ ] Sharing personal views (e.g., political beliefs) (5)
- [ ] Campaigning for a cause (6)
- [ ] Other: ________________________________________________ (7)

Display This Question:
If Have you ever used the Telegram instant messaging app? = No, I have not used Telegram.
Q36 Have you ever shared sensitive information using $\{Q24/ChoiceGroup/SelectedChoices\}$? By sensitive, we mean information that was for the intended recipient only, and which you would not want others to have.

- Yes, I have shared sensitive information using $\{Q24/ChoiceGroup/SelectedChoices\}$ (1)
- No, but I have shared sensitive information using a messaging app other than $\{Q24/ChoiceGroup/SelectedChoices\}$ (2)
- No, I haven't shared sensitive information using any messaging app (3)
- I don’t remember (4)

End of Block: U

Start of Block: V

Display This Question:
If Have you ever used the Telegram instant messaging app? = No, I have not used Telegram.

Q37 Are your one-to-one (not group) communications using $\{Q24/ChoiceGroup/SelectedChoices\}$ end-to-end encrypted?

- Yes, they are end-to-end encrypted (1)
- Yes, but I have to turn end-to-end encryption on (2)
- No, they are not end-to-end encrypted (3)
- I don't know what encryption is or why it is important (5)
- I don’t know (4)

Display This Question:
If Have you ever used the Telegram instant messaging app? = No, I have not used Telegram.
Q38 Are your group communications using ${Q24/ChoiceGroup/SelectedChoices}$ end-to-end encrypted?

- Yes, they are end-to-end encrypted (1)
- Yes, but I have to turn end-to-end encryption on (2)
- No, they are not end-to-end encrypted (3)
- I don't know what encryption is or why it is important (5)
- I don't know (4)
- I don't use ${Q24/ChoiceGroup/SelectedChoices}$'s group chat (6)
Q39 For each of the following actions (reading, listening to, modifying, and impersonating), select who you think could do it.

<table>
<thead>
<tr>
<th>Action</th>
<th>Could read my messages (1)</th>
<th>Could listen to phone calls (2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No one (9)</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>People who work at</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>People who have physical access to my mobile phone (11)</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Other: (8)</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>I don’t know (10)</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>People who are up to no good (3)</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>The government of the country I live in (in this case, the UK government) (4)</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Another country’s government (5)</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>My Internet service provider (ISP) (6)</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Corporations other than the company that makes/develops</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>The government of another country (5)</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Corporations other than the company that makes/develops</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Other: (8)</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>I don’t know (10)</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
</tbody>
</table>
Q40  Please indicate which of the following ranges your age falls within.

- 18 – 24 (2)
- 25 – 34 (3)
- 35 – 44 (4)
- 45 – 54 (5)
- 55 – 64 (6)
- 65 – 74 (7)
- 75+ (8)
- Prefer not to say (9)

Q41  Please indicate your gender.

- Male (1)
- Female (2)
- Other (4)
- Prefer not to say (5)
Q42 What is your highest level of education?
If you are currently enrolled, please specify the highest level/degree completed.

- Some secondary education (1)
- Secondary education or equivalent (2)
- Vocational training (e.g., NVQ, HNC, NHD) (3)
- Associate’s degree (e.g., AS, AB) (4)
- Some college/undergraduate education; no degree (5)
- College/undergraduate degree (e.g., BSc, BA) (6)
- Graduate/postgraduate degree (e.g., MSc, MA, MBA, PhD) (7)
- Other: (8) ____________________________________________________________________

Q43 Which of the following best describes your educational background or job field?

- I have an education in, or work in, the field of computer science, computer engineering, or IT. (1)
- I do not have an education in, nor do I work in, the field of computer science, computer engineering, or IT. (2)
- Prefer not to say (3)

Q44 Please provide any additional comments on the survey overall.
__________________________________________________________________________________
__________________________________________________________________________________
__________________________________________________________________________________
Appendix D

Survey: Exploring User Mental Models of End-to-End Encrypted Communication Tools
Q1
Please enter your Prolific Academic ID.

________________________________________________________________

End of Block: A

Start of Block: B

Q2 Have you heard of the term “end-to-end encryption”?

☐ Yes, I have heard of the term “end-to-end encryption”, and I feel confident explaining what it means. (1)

☐ Yes, I have heard of the term “end-to-end encryption”. However, I do not feel confident explaining what it means. (2)

☐ No, I have not heard of the term “end-to-end encryption”. (3)

End of Block: B

Start of Block: C

Q3 Imagine you are considering using a new tool (or application) named Soteria to communicate with your family members, friends, colleagues, and others. When you install Soteria, the following message is displayed: “Soteria’s communications (messages, phone calls, and video calls) are end-to-end encrypted.”

Imagine that one of your friends has asked you the questions below about what Soteria does. To the best of your knowledge, please answer these questions.

Q4 Why should your friend use Soteria? Make sure you describe Soteria’s features and benefits.
Q5 What are the drawbacks of using Soteria, if any?

Q6 As far as you know, what does it mean that Soteria’s communications are end-to-end encrypted?

Q7 What do the ends in “end-to-end encryption” refer to?

End of Block: C
Q8
Imagine you are going to use Soteria as your primary method of communication for this scenario:
$\text{S[ez://Field/scenario]}$.

Even if you would not do what is described above in real life, please answer the remaining questions in this section to the best of your ability according to how you would act, feel, or respond if you encountered this scenario in real life.
Q9 Based on what you know about Soteria, which of the following, if any, do you think could (1) read your Soteria messages (2) listen to your Soteria phone calls (3) modify the content of your Soteria communications (e.g., text messages), and/or (4) impersonate you (i.e., communicate with others using your Soteria account)?

**Please recall you are using Soteria for the following scenario:** S{e://Field/scenario}.

<table>
<thead>
<tr>
<th></th>
<th>could read your Soteria messages? (1)</th>
<th>could listen to your Soteria phone calls? (2)</th>
<th>could modify your Soteria communications? (3)</th>
<th>could impersonate you on Soteria? (4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>People who work at Soteria (1)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Someone with a technical background or a computer science degree (2)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>People who are up to no good (3)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Your country’s government (in this case, the UK government) (4)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Another country’s government (5)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Your Internet service provider (ISP) (6)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Corporations other than the company that makes/develops Soteria (7)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Other: (8)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td><strong>No one</strong> (9)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>
Q10 How confident are you that your overall answers to the question above were correct?

<table>
<thead>
<tr>
<th>Level of confidence (1)</th>
<th>Not at all confident (1)</th>
<th>Slightly confident (2)</th>
<th>Somewhat confident (3)</th>
<th>Moderately confident (4)</th>
<th>Extremely confident (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
</tbody>
</table>

End of Block: E

Start of Block: F

Carry Forward Selected Choices - Entered Text from "Based on what you know about Soteria, which of the following, if any, do you think could (1) read your Soteria messages (2) listen to your Soteria phone calls (3) modify the content of your Soteria communications (e.g., text messages), and/or (4) impersonate you (i.e., communicate with others using your Soteria account)? Please recall you are using Soteria for the following scenario: $\langle e://Field/scenario\rangle$.
"
Q11 How upset would you be about the following accessing (reading, listening to, or modifying your Soteria communications), or using your Soteria account to communicate with others?

Please recall you are using Soteria for the following scenario: $e://Field/scenario$.

<table>
<thead>
<tr>
<th>People who work at Soteria (x1)</th>
<th>Not at all upset (1)</th>
<th>Slightly upset (2)</th>
<th>Somewhat upset (3)</th>
<th>Moderately upset (4)</th>
<th>Extremely upset (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Someone with a technical background or a computer science degree (x2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>People who are up to no good (x3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Your country’s government (in this case, the UK government) (x4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Another country’s government (x5)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Your Internet service provider (ISP) (x6)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corporations other than the company that makes/develops Soteria (x7)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other: (x8)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>No one</strong> (x9)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Q12 Why do you think someone with a technical background or a computer science degree could gain access to (read, listen to, or modify) your Soteria communications, or impersonate you on Soteria?

Please recall you are using Soteria for the following scenario: \$\{\text{Field/scenario}\}.$
Q13  Do you think the following types of communication are less secure than, more secure than, or as secure as the text messages you would send on Soteria?

<table>
<thead>
<tr>
<th>Type of Communication</th>
<th>Less secure than Soteria text messages (1)</th>
<th>More secure than Soteria text messages (2)</th>
<th>As secure as Soteria text messages (3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Images/photos sent using Soteria (1)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Videos sent using Soteria (2)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>File attachments sent using Soteria (3)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Voice notes sent using Soteria (4)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Phone calls made using Soteria (5)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Video calls made using Soteria (6)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>SMS text messages (7)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Landline phone calls (8)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Mobile phone calls made using cellular data (e.g., 3G, 4G) (9)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Email messages (10)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

End of Block: H

Start of Block: I

Q14  When using Soteria, how would you verify the identity of the person you communicate with? In other words, how would you make sure that you are talking to (or messaging) the right person?
Q15 Please list three examples of services, tools, or applications, if any, that you consider having the same security guarantees as Soteria?

- Example 1: (1) ________________________________________________
- Example 2: (2) ______________________________________________
- Example 3: (3) ________________________________________________

Q16 In this section of the survey, we will ask you questions about your use of different communication tools/applications in real life. These questions are no longer related to Soteria.

Q17 Do you own a desktop computer and/or laptop?

- Yes (1)
- No (2)
- Do not know (3)
Q18 Do you own a smartphone?

- Yes (1)
- No (2)
- Do not know (3)

Q19 In the following question, please indicate from which of these sources you learn information about technology and computing devices (in general).

- Online, TV, or print media. For example, a news article, TV show, blog post, or advertisement. (1)
- My school, college, university, or workplace (2)
- My fellow students, co-workers, or other professional peers (3)
- My family members or friends (4)
- Librarians (5)
- Vendors or merchants. For example, a salesperson at Apple Retail Store, Maplin Electronics, or Carphone Warehouse. (6)
- Service providers. For example, BT Broadband, O2, Vodafone, or Virgin Media. (7)
- Other: (8) ________________________________

End of Block: L

Start of Block: M
Appendix D. Survey: Exploring Mental Models of End-to-End Encrypted Tools
Q20 Which of the following communication tools/applications have you heard of?

☐ Adium (1)
☐ Blackberry Messenger (BBM) (2)
☐ Blackberry Protect (3)
☐ ChatSecure (4)
☐ Confide (5)
☐ eBuddy XMS (6)
☐ Facebook Messenger (7)
☐ FaceTime (8)
☐ Google Hangouts (9)
☐ iMessage (10)
☐ Jitsi (11)
☐ Kik Messenger (12)
☐ Ostel (13)
☐ Pidgin (14)
☐ QQ (15)
☐ Signal (16)
Silent Phone/Silent Text (17)
Skype (18)
Snapchat (Direct Snaps) (19)
Surespot (20)
Telegram (21)
TextSecure (22)
Threema (23)
Viber (24)
WhatsApp (25)
Wickr (26)
Yahoo! Messenger (27)
Instagram Direct Messages (28)
Twitter Direct Messages (29)
LinkedIn InMail (30)
Other: (31) ________________________________________________
Carry Forward Selected Choices - Entered Text from "Which of the following communication tools/applications have you heard of?"
<table>
<thead>
<tr>
<th>Tool</th>
<th>How often do you use the following tools/applications?</th>
<th>Used before, but stopped using it (2)</th>
<th>Use it currently (3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adium (x1)</td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Blackberry Messenger (BBM) (x2)</td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Blackberry Protect (x3)</td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>ChatSecure (x4)</td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Confide (x5)</td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>eBuddy XMS (x6)</td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Facebook Messenger (x7)</td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>FaceTime (x8)</td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Google Hangouts (x9)</td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>iMessage (x10)</td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Jitsi (x11)</td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Kik Messenger (x12)</td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Ostel (x13)</td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Pidgin (x14)</td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>QQ (x15)</td>
<td></td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Application</td>
<td>Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signal (x16)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Silent Phone/Silent Text (x17)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skype (x18)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Snapchat (Direct Snaps) (x19)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Surespot (x20)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telegram (x21)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TextSecure (x22)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threema (x23)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Viber (x24)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WhatsApp (x25)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wickr (x26)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yahoo! Messenger (x27)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instagram Direct Messages (x28)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Twitter Direct Messages (x29)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LinkedIn InMail (x30)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other: (x31)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Q22  Please indicate which of the following ranges your age falls within.

- Under 18  (1)
- 18 – 24  (2)
- 25 – 34  (3)
- 35 – 44  (4)
- 45 – 54  (5)
- 55 – 64  (6)
- 65 – 74  (7)
- 75+  (8)
- Prefer not to answer  (9)

Q23  Please indicate your gender.

- Male  (1)
- Female  (2)
- Non-binary  (3)
- Other:  (4) ________________________________________________
- Prefer not to answer  (5)
Q24 What is your highest level of education?
If you are currently enrolled, please specify the highest level/degree completed.

- Some high-school education (1)
- High-school education or equivalent (2)
- Vocational training (e.g., NVQ, HNC, NHD) (3)
- Associate’s degree (e.g., AS, AB) (4)
- Some college/undergraduate education; no degree (5)
- College/undergraduate degree (e.g., BSc, BA) (6)
- Graduate/postgraduate degree (e.g., MSc, MA, MBA, PhD) (7)
- Other: (8) ________________________________________________

End of Block: O
Start of Block: P

Q25 Which of the following best describes your educational background or job field?

- I have an education in, or work in, the field of computer science, computer engineering, or IT. (1)
- I do not have an education in, nor do I work in, the field of computer science, computer engineering, or IT. (2)
- Prefer not to answer (3)
Q26 Have you written a computer program?

- Yes (1)
- No (2)
- Do not know (3)

Q27 What is your current employment status?

- Employed (1)
- Unemployed (2)
- Student (3)
- Retired (4)
- Other: ________________________________________________
- Prefer not to answer (6)
Q28 Please select the digital security requirements that you have at work, if any.

- Sending emails with encryption (1)
- Using a dedicated phone for work tasks (2)
- Using two-factor authentication to access your work devices (3)
- Always using a VPN when working on work activities (4)
- Other: (5) ________________________________
- I do not have digital security requirements. (7)
- Prefer not to answer (6)

Q29 Do you receive training about digital security or privacy at work?

- Yes, yearly (1)
- Yes, a few times a year (2)
- Yes, monthly (3)
- Yes, other: (7) ________________________________
- No (4)
- Prefer not to answer (5)
Q30 Do you feel at risk due to your job duties?

☐  Yes, physical risk due to stalking, threats, or attack from people who do not like what I do. (1)

☐  Yes, cyber risk due to stalking, threats, or attack from people who do not like what I do. (2)

☐  Yes, other: (3) ________________________________________________

☐  No (4)

☐  Prefer not to answer (5)

End of Block: Q

Start of Block: R
Q31 Which of the following political parties in the United Kingdom most clearly represents your political views?

- Conservative Party (1)
- Labour Party (2)
- Liberal Democrats (3)
- UKIP: UK Independence Party (4)
- Green Party (5)
- Plaid Cymru (6)
- Scottish National Party (7)
- Democratic Unionist Party (8)
- Other: (9) ________________________________
- None (10)

Q32 Which of the following most clearly matches your current political views?

- Very conservative (1)
- Conservative (2)
- Neutral (3)
- Liberal (4)
- Very liberal (5)
- Prefer not to answer (6)
Q33
Do you lean toward conservative, liberal, or neither?

- Conservative (1)
- Liberal (2)
- Neither (3)
- Prefer not to answer (4)

Q34
Which of the following best describes your race?

- White (1)
- Black (2)
- Asian (3)
- Mixed race (4)
- Other: ________________________________
- Prefer not to answer (6)
Q35 Please rate the overall difficulty of this survey.

- Very difficult (1)
- Somewhat difficult (2)
- Neither easy nor difficult (3)
- Somewhat easy (4)
- Very easy (5)

Q36 Please rate your overall satisfaction with the survey.

- Good (1)
- Neutral (2)
- Bad (3)

Q37 Please provide any additional comments on the survey overall.

____________________________________________________________________
____________________________________________________________________
____________________________________________________________________
____________________________________________________________________

End of Block: S
Appendix E

Survey: Secure Group
Communications: Investigating User Needs and Practices
Q1 Please enter your Prolific Academic ID.


Q2 How frequently do you use instant messaging tools for group chat?

- Daily (1)
- 4–6 times a week (2)
- 2–3 times a week (3)
- Once a week (4)
- Rarely (6)
- Never (5)
Q3 Please mark which of the following tools, if any, you have used. (select all that apply)

- Blackberry Messenger (17)
- Discord (18)
- Facebook Messenger (9)
- Google Hangouts (7)
- iMessage (8)
- IMO (14)
- Instagram Direct (19)
- Kakaotalk (13)
- KIK (16)
- Line (10)
- Marco Polo (4)
- Signal (2)
- Skype (12)
- Slack (6)
- Snapchat (15)
- Telegram (3)
| □ | Viber (11) |
| □ | WeChat (5) |
| □ | WhatsApp (1) |
| □ | N/A (23) |
Q4 For what purposes do you use instant messaging tools for group communication?
________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________

Q5 What, if anything, do you like about using instant messaging tools for group communication?
________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________

Q6 What, if anything, do you dislike about using instant messaging tools for group communication?
________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________

Q7 How do you choose which instant messaging tools to use for group communication?
________________________________________________________________
________________________________________________________________
Q8 When using instant messaging tools for group communication, who do you talk to? (select all that apply)

☐ Immediate/nuclear family members (1)

☐ Extended family members (2)

☐ Friends (3)

☐ Work colleagues (4)

☐ Other (7) ____________________________________________

☐ I prefer not to answer (8)
Q9 On average, how large are your instant messaging groups?

- 3–5 people (1)
- 6–10 people (2)
- 11–20 people (3)
- 20+ people (4)
- My groups vary largely in size. (6)
- Unsure / I prefer not to answer (7)

Display This Question:

*If On average, how large are your instant messaging groups? = My groups vary largely in size.*

Q10 Why do your instant messaging groups vary largely in size?

____________________________________________________________________
____________________________________________________________________
____________________________________________________________________
____________________________________________________________________
____________________________________________________________________

Page Break
Q11 Have you ever been removed from an instant messaging group without your permission?

- Yes (1)
- No (2)
- Unsure / I prefer not to answer (4)

Display This Question:
If Have you ever been removed from an instant messaging group without your permission? = Yes

Q12 If you are willing, please share why you were removed from an instant messaging group without your permission.

________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________

Display This Question:
If Have you ever been removed from an instant messaging group without your permission? = Yes

Q13 How did you feel after having been removed from an instant messaging group without your permission?

________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________

________________________________________________________________
Q14 Should people ask the group for permission before inviting others to join an instant messaging group you are a member of?

- Yes (1)
- No (2)
- It depends (3)
- Unsure / I prefer not to answer (4)

Q15 Why do you want other people to ask the group for permission before inviting others to join an instant messaging group you are a member of?

________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________
Q16 When do you review the member list of an instant messaging group? (select all that apply)

☐ When I first join a group  (1)
☐ When a new member joins the group  (2)
☐ When a member leaves the group  (3)
☐ I check every now and then to see if anything has changed  (4)
☐ I never review the member list  (5)
☐ Unsure / I prefer not to answer  (6)

Q17 Have you ever been in an instant messaging group chat where one or more members of the group chat only rarely participate in the group conversation?

☐ Yes  (1)
☐ No  (2)
☐ Unsure  (3)

Display This Question:
If Have you ever been in an instant messaging group chat where one or more members of the group chat... = Yes

Q18 How did you feel about having an instant messaging group chat where one or more members of the group chat only rarely participate in the group conversation?

________________________________________________________________
________________________________________________________________
________________________________________________________________
Q19 How comfortable are you with other members of an instant messaging group saving and/or sharing your conversations with non-members?

- Extremely uncomfortable (1)
- Somewhat uncomfortable (2)
- Neither comfortable nor uncomfortable (3)
- Somewhat comfortable (4)
- Extremely comfortable (5)
- Unsure / I prefer not to answer (6)
Q20 Are there topics that make you uncomfortable to read or discuss in instant messaging groups you are a member of? (select all that apply)

- ☐ Religion (1)
- ☐ Politics (2)
- ☐ Medical health (3)
- ☐ Mental health (4)
- ☐ Sexuality (5)
- ☐ Drug use (6)
- ☐ Other (8) ________________________________________________
- ☐ Unsure / I prefer not to answer (9)
Q21 Has anyone ever shared something in an instant messaging group that placed you in an awkward position?

- Yes  (1)
- No  (2)
- Unsure / I prefer not to answer  (4)

Q22 If you are willing, please share how what was shared put you into an awkward position.

________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________

Q23 How did you respond to someone sharing something that placed you in an awkward position?

________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________

Q24 Have you ever joined an instant messaging group because you were interested in the topic being discussed and not because of who the group members were?

○ Yes (23)
○ No (24)
○ Unsure / I prefer not to answer (25)

Display This Question:
If Have you ever joined an instant messaging group because you were interested in the topic being discussed and not because of who the group members were? = Yes

Q25 What topics were discussed in these groups?

____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________

Display This Question:
If Have you ever joined an instant messaging group because you were interested in the topic being discussed and not because of who the group members were? = Yes

Q26 Do you recall a time when privacy was a concern for you when joining or participating in these groups?

○ Yes (23)
○ No (24)
○ Unsure / I prefer not to answer (25)
Q27 If you are willing, please share what your privacy concerns were when joining or participating in these groups.

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

End of Block: D

Start of Block: E

Q28 Have you ever shared sensitive information in an instant messaging group?

○ Yes (1)

○ No (2)

○ Unsure / I prefer not to answer (4)

Q29 If willing, please share the types of sensitive information you have shared in an instant messaging group.

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________
Q30 What does it mean to you that an instant messaging tool is secure for group communication?
________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________

Q31 What do you personally do to make sure your instant messaging group communications are secure?
________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________

Page Break
Q32 How do you decide if an instant messaging tool is secure for group communication?

________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________

Q33 Are there any instant messaging tools you believe are secure for group communication?

○ Yes (1)

○ No (2)

○ Unsure / I prefer not to answer (3)

Display This Question:
If Are there any instant messaging tools you believe are secure for group communication? = Yes

Q34 Please specify which tools you believe to be secure for group communication.

________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________
Q35 Have you ever been concerned that someone is not who they say they are when using instant messaging for group communication?

- Yes (1)
- No (2)
- Unsure / I prefer not to answer (3)

Q36 Why were you concerned that someone is not who they say they are when using instant messaging for group communication?

________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________

Q37 How do you verify that someone is who they say they are when using instant messaging for group communication?

________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________

Display This Question:

If Have you ever been concerned that someone is not who they say they are when using instant messaging... = Yes
Q38 What is your age?

- Under 21 (1)
- 21-34 (2)
- 35-44 (3)
- 45-54 (4)
- 55-64 (5)
- 65+ (6)
- I prefer not to answer (7)

Q39 What is your gender?

- Male (1)
- Female (2)
- Other (3) ____________________________________
- I prefer not to answer (4)
Q40 Please specify your ethnicity.

- White or Caucasian (1)
- Black or African American (2)
- Asian (3)
- Pacific Islander (4)
- Mixed race (5)
- Other (specify) (6) _________________________________
- I prefer not to answer (7)

Q41 What is the highest level of school you have completed or the highest degree you have received?

- Less than high school degree (1)
- High school graduate (high school diploma or equivalent including GED) (2)
- Some college but no degree (3)
- Associate's degree in college (2-year) (4)
- Bachelor's degree in college (4-year) (5)
- Master's degree (6)
- Professional degree (JD, MD) (8)
- Doctoral degree (7)
- I prefer not to answer (9)

End of Block: F

Start of Block: G
Q42 Please rate the overall difficulty of this survey.

- Very difficult (1)
- Somewhat difficult (2)
- Neither easy nor difficult (3)
- Somewhat easy (4)
- Very easy (5)

Q43 Please rate your overall satisfaction with the survey.

- Good (1)
- Neutral (2)
- Bad (3)

Q44 Please provide any additional comments on the survey overall.

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

End of Block: G