ABSTRACT

Title of dissertation:	USER PERCEPTIONS OF AND ATTITUDES TOWARD ENCRYPTED COMMUNICATION
	Wei Bai Doctor of Philosophy, 2019
Dissertation directed by:	Professor Michelle L. Mazurek Department of Electrical and Computer Engineering

As people rely more heavily on online communication, privacy becomes an increasingly critical concern. Users of communication services (e.g., email and messaging) risk breaches of confidentiality due to attacks on the service from outsiders or rogue employees, or even government subpoenas and network surveillance. End-to-end encryption, in which anyone cannot read the user's content, is the only way to fully protect their online communications from malicious attackers, rogue company employees, and government surveillance. Although in recent years we have witnessed considerable efforts to push end-to-end encryption into broader adoption, and indeed several popular messaging tools have adopted end-to-end encryption, some obstacles still remain which hinder general users from proactively and confidently adopting end-to-end encrypted communication tools and acknowledge their security benefits.

In this dissertation, we investigated the adoption of end-to-end encrypted communication from a variety of user-centered perspectives. In the first part, we conducted a lab study (n=52), evaluating how general users understand the balance

between the usability and security for different key management models in end-to-end encryption. We found that participants understood the models well and made coherent assessments about when different tradeoffs might be appropriate. Our participants recognized that the less-convenient exchange model was more secure overall, but found the security of the key-directory based model to be "good enough" for many everyday purposes.

In the second part, we explored how general users value the usability and security tradeoffs for different approaches of searching over end-to-end encrypted messages. After systematizing these tradeoffs to identify key feature differences, we used these differences as a basis for a choice-based conjoint analysis experiment (n=160). We found that users indicated high relative importance for increasing privacy and minimizing local storage requirements. While privacy was more important overall, after the initial improvement was made, further improvement was considered less valuable. Also, local storage requirement was more important than adding marginal privacy.

Since significant research indicated that non-expert users' mental models about end-to-end encryption led them to make mistakes when using these tools, in the third part of this dissertation, we took the first step to tackle this problem by providing high-level, roughly correct information about end-to-end encryption to non-expert users. In a lab study, participants (n=25) were shown one of several variations on a short tutorial. Participants were asked about their understanding of end-to-end encryption before and after the tutorial, as well as which information they found most useful and surprising. Overall, participants effectively learned

many benefits and limitations of end-to-end encryption; however, some concerns and misconceptions still remained, and our participants even developed new ones. The results provided insight into how to structure new educational materials for end-to-end encryption.

USER PERCEPTIONS OF AND ATTITUDES TOWARD ENCRYPTED COMMUNICATION

by

Wei Bai

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2019

Advisory Committee:
Professor Michelle L. Mazurek, Chair/Adviser
Professor Tudor Dumitras
Professor Charalampos (Babis) Papamanthou
Dr. Patrick Gage Kelley, Google
Prof. Wayne Lutters, Dean's Representative

Dedication

To my family.

Acknowledgments

I owe my gratitude to all the people who have made this thesis possible and because of whom my graduate experience has been one that I will cherish forever.

First and foremost, I would like to express my sincere gratitude to my PhD advisor, Professor Michelle Mazurek, for giving me this invaluable opportunity to get my hands on the challenging and extremely interesting projects in the field of usable security. With her insightful supervision, I learned how to be a researcher, to think critically, and to produce high-quality work with a positive attitude. During the years we worked closely together, she gave me generous guidance, unwavering support and enthusiastic encouragement to proceed along this adventure. It has been truly a pleasure to work with and learn from her.

I would also like to thank other members in my dissertation committee, Prof. Tudor Dumitras, Prof. Charalampos (Babis) Papamanthou, Dr. Patrick Gage Kelley, and Prof. Wayne Lutters for their time and valuable comments. I am fortunate to work closely with them during my PhD studies, from class projects to research proposals, from discussing research ideas to writing up publications. I am fortunate to learn from their expertise and I feel honored to have them in my dissertation committee.

I also acknowledge my colleagues in the Security, Privacy, People lab (SP2) – Elissa Redmiles, Daniel Votipka, Kelsey Fulton, Rock Stevens, Omer Akgul, Noel Warford, Debjani Saha – for their discussions, support, and friendship. The good times we have shared together throughout the past few years are really unforgettable.

Last but not least, I owe my deepest gratitude to my family. My parents and parents-in-law have been extremely supportive of me throughout the process and are always encouraging me whenever I feel down. My wife, Fan Zhang, deserves special thanks for her endless love and company. I am extremely fortunate to have her in my life. I believe all the joys and sorrows I have experienced help me become a better person, son, and husband.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

As people rely more heavily on online communication, privacy becomes an increasingly critical concern. Users of communication services (e.g., email and messaging) risk breaches of confidentiality due to attacks on the service from outsiders or rogue employees, or even government subpoenas and network surveillance. End-to-end encryption, in which anyone cannot read the user's content, is the only way to fully protect their online communications from malicious attackers, rogue company employees, and government surveillance. Although in recent years we have witnessed considerable effort to push end-to-end encryption into broader adoption [1–4], and indeed several popular messaging tools such as WhatsApp and iMessage have adopted end-to-end encryption, some obstacles still remain that hinder general users from proactively and correctly using end-to-end encryption tools and acknowledging their security benefits [5–8].

In this dissertation, we investigated the adoption of end-to-end encrypted communications from a variety of user-centered perspectives which have not been explored before: first, how do users perceive the tradeoffs among different key management models in end-to-end encryption; second, how do users tradeoff for search in encrypted communications; and third, how to help non-expert users understand better about end-to-end encryption so that they can use these tools more effortlessly and confidently.

1.1 User Tradeoffs for Key Management Models

Progress toward better usability and thus wider adoption of end-to-end encryption has been made in recent years. Apple applied seamless end-to-end encryption to its iMessage and FaceTime services [9,10]. By centrally distributing public keys, Apple ensures the encryption is transparent to users, bringing end-to-end encryption to millions of iPhone, iPad, and Mac users. This design, however, leaves open the possibility that Apple itself could carry out a man-in-the-middle attack to break its users' privacy, for example at the request of law enforcement authorities [11,12]. Popular messaging app WhatsApp has also implemented end-to-end encryption for text, voice, and video communications [13]. As with iMessage, WhatsApp centrally distributes public keys; however, users can optionally verify each other's keys manually or via QR code. Google and Yahoo! are reportedly developing similar approaches for email, with an added monitoring protocol that allows users and third parties to audit the key directory for consistency and transparency [14–16]. Some security experts have suggested that given this potential man-in-the-middle attack, these services should not be recommended to end users. As just one example, one security researcher suggests that "iMessage remains perhaps the best usable covert communication channel available today if your adversary can't compromise Apple. ... If one desires confidentiality, I think the only role for iMessage is instructing someone how to use Signal [1]" [12].

In a sense, the issue comes down to whether the benefit from many more people adopting encrypted communications is outweighed by the reduced security inherent in the central key distribution model. While security experts are best positioned to understand the technical differences between models, end users will ultimately be faced with the choice of which platforms and products to install and use. Researchers have considered the needs of some highly privacy-sensitive users, such as journalists and activists [17, 18]. To our knowledge, however, no one has asked average users for their opinions about these tradeoffs. This means that although security experts may understand the risks and benefits of different tools, as a community we do not understand how an average user will weigh different factors in deciding whether to adopt or ignore various encrypted communication technologies.

To understand how non-expert users feel about these tradeoffs, we undertook a 52-person lab study. We introduced participants to two encryption models: an *exchange* model in which participants manually exchange keys (analogous to traditional PGP) and a *registration* model in which participants sign up with a central service that distributes keys (analogous to iMessage). For each model, we asked them to complete several encrypted communication tasks; we also gave them a short, high-level explanation of each model's security properties. (We varied the order of presentation to account for biases.) We then asked participants to comment on the security and usability of each model, as well as their overall opinion of the tradeoffs involved. The experiment was designed, insofar as possible, to avoid comparisons

[1] An end-to-end encrypted communication tool: `https://whispersystems.org/`

based on user-interface design and focus instead on the underlying properties of each encryption model.

We found that participants understood the two models fairly well and expressed nuanced insights into the tradeoffs between them. As predicted, participants found the registration model considerably more convenient than the exchange model. More interestingly, while the exchange system was considered more secure overall, the difference was slight: both the general trust that large email providers would not risk their reputations by cheating and reasonable concerns about participants' own ability to correctly implement the exchange model mitigated this difference. Separately, we asked about half of our participants to evaluate the auditing model proposed in CONIKS [19], which is similar to that in maybe development by Google and Yahoo!, and we found that for many users it provides a meaningful additional degree of confidence in the registration model's privacy.

Overall, our results suggest that users recognize the benefit of the exchange model for very sensitive communications, but find the more-usable registration model sufficient for the majority of everyday communications they engage in. While there are risks to this model, some of which can be alleviated by auditing, we argue that the marginal benefit of broad adoption will outweigh these risks. Historically, encryption schemes that require significant user effort have never gained broad popularity. Trying to convince average users to exclusively use more complicated schemes, when they often don't see a need for the added protection, may instead keep them away from using any encryption at all. Rather than spreading undue alarm about the risks of registration models, or forcing users into only exchange models, we recommend that policymakers and designers present tradeoffs clearly and encourage adoption of usable but imperfect security for the many scenarios where it may be appropriate.

1.2 User Tradeoffs for Search in Encrypted Communication

In recent years, more online communication services, especially instant messaging tools, have adopted end-to-end encryption; for example, WhatsApp and Apple's iMessage have brought end-to-end encrypted messaging to millions of users by default [9, 13]. While these popular tools have been moving in the right direction for securing communication, email adoption has not caught up [5].

While end-to-end encryption provides important privacy benefits, it can complicate functionality in a variety of ways that can potentially inconvenience end users. As one example, message searching (i.e., recovering a previously sent or received message using keywords) is a critical function for many users, especially for email [20–22]. When messages are end-to-end encrypted, searching their contents becomes complicated. Straightforward solutions in which the communication service maintains a central searchable index cannot be applied directly, as the communication service cannot read and index messages. To avoid this, instant messaging systems typically use a local index, in which messages decrypted on a device are indexed (and can therefore be searched) on that device.

An alternative to local indexing is to support searching over encrypted content. During the past two decades, researchers have made significant progress on *searchable encryption*, or mechanisms that can support searching encrypted data on an untrusted server without revealing the content of the messages or of the search queries [23–28]. These techniques are gradually being adopted by industry, e.g., for databases. While they have not yet been applied specifically for messaging, researchers have begun to explore this potential use case.

Both of these approaches to enable search for end-to-end encrypted messaging have benefits and drawbacks, in terms of security properties and in terms of utility for end users. To our knowledge, these tradeoffs have not been systematically explored from the point of view of end users. In this work, we take a first step toward filling that gap. First, we systematize the tradeoffs of these solutions in four dimensions: search expressiveness, performance, portability, and security across devices. This approach allows us to identify key features (that apply to both messaging and email) that may influence users' preferences. We then apply this systematization to design a choice-based conjoint analysis study focusing on email. We choose to study email specifically because of the prominence of search in an email setting, as well as the tendency for email archives to be relatively large and long-lived. Study participants were asked to make a series of choices between email-service *profiles* with different usability and security features; the results allow us to quantify the importance of each feature relative to the others in the email setting [29–31]. This methodology has been adopted in previous research to investigate users' online privacy concerns [32–34].

Our experiment (n=160) compared six features that may affect users' preferences for encrypted communication: price, multi-word search, partial-word search, privacy, local storage and synchronization across devices. We find that privacy is the second-most important feature, after price: participants indicated they would pay on average $0.85 per month to reduce service providers' access to the contents of their messages and search queries. However, minimizing the use of local storage was almost as highly valued. We also find that participants' web skills, along with their self-reported level of privacy concern, influence their choices.

Our results suggest that users were able to understand the usability and privacy tradeoffs broadly. There is a potentially valuable niche for applying searchable encryption rather than a local index to email messaging, to support users who want more privacy than in an unencrypted service but who also highly prioritize limiting space on mobile devices.

1.3 Improving Non-Experts' Understanding of End-to-End Encryption

Despite significant improvement, recent research has shown that many non-expert users have difficulty using end-to-end encryption (E2EE) correctly within these tools and recognizing the security benefits they do (and don't) provide [5, 6, 8, 35]. These difficulties are not simply caused by poor usability or interface design; rather, they occur in large part because users hold incorrect mental models of E2EE. Even interfaces that hide the majority of the details of encryption and decryption from users may require users to complete some tasks, such as authentication ceremonies and key changes; without reasonable mental models for the process, users struggle to complete these tasks [6,7,36,37]. Further, incorrect mental models can cause users to wrongly believe that other communications approaches (such as standard text messaging) are more secure than E2EE messaging, or to believe that all privacy protections are inevitably futile in the face of skilled adversaries, reducing use of E2EE where it might be appropriate [5]. Additionally, incorrect mental models may lead users to underestimate valid risks, such as vulnerability to malware at endpoints.

One ideal solution might be to design software that — in interface if not in underlying technical operation — would "more closely align with users' existing mental models" [8]. However, this is likely to prove difficult (at least in the near future), as existing models are fairly far from correct and not well aligned with the inherent technical characteristics of encryption systems. Instead, enabling users to make appropriate decisions about how to meet their privacy needs may require at least somewhat improving mental models, perhaps via better explanations [8].

While it is neither possible nor desirable to ask all or even many users to become cryptography experts, we can work to improve high-level mental models and help non-expert users understand basic threat models and mitigations. In this work, we take an initial step toward this goal by exploring how to explain high-level E2EE concepts to non-experts, with a focus on what they find most important and surprising. In a qualitative lab study (n=25), participants were shown a short tutorial containing one or more modules explaining aspects of E2EE: a high-level overview; details about the kinds of surveillance risks E2EE can and cannot protect against; a debunking of common misconceptions; and a more detailed but only lightly technical description of how E2EE works. Before and after the tutorial, participants answered questions about their understanding of E2EE and its security properties. We also asked participants to provide feedback on the tutorial contents, to critique E2EE explanations drawn from popular messaging tools' current documentation, and to design a short explanation highlighting the most important aspects of E2EE. Taken together, these tasks allow us to investigate how users respond to different educational approaches, what aspects of E2EE they find most important or most surprising, and which elements should be emphasized in future educational interventions. While we do not expect many general users will want to complete even short formal tutorials like the ones we tested, we hope that insights from our study can be used to inform the design of informal educational efforts, such as interstitial informational screens within messaging apps.

We find that overall our tutorials are effective at conveying high-level security properties of E2EE, including potential weaknesses at endpoints. They also correct certain existing misconceptions about who has access to messages in transit. We find that the risks module effectively conveys ideas about the relative risk of E2EE and non-E2EE communications, but the misconceptions module does not effectively address confusion about integrity and authenticity. The technical description increased understanding somewhat for some participants, but also promoted misunderstanding for others, and was not considered particularly important or useful. The critique activities, meanwhile, revealed several points of confusion within existing messages. Overall, participants' responses suggest that emphasizing confidentiality, clearly conveying the limitations of E2EE protections, and reducing complexity are the most important properties for effective education.

1.4 Dissertation Structure

This dissertation is structured as follows: Chapter 2 lists related work; Chapter 3 describes how general users balance the tradeoffs of different key management models in end-to-end encryption; Chapter 4 introduces general users' tradeoffs for search in encrypted communications; Chapter 5 presents our work to improve non-expert users' mental models about end-to-end encryption; Chapter 6 lists our recommendations to the community, and Chapter 7 concludes the dissertation and provides future research directions.

Chapter 2: Related Work

In this chapter, we explained the work this dissertation built on. Our related work includes the following areas: the history of end-to-end encryption; the usability of end-to-end encryption; the social factors and mental models in end-to-end encryption adoption; advances in searchable encryption; habits of email search, organization and mobile usage; application of conjoint analysis; and the educational principles we followed to design our educational tutorials.

2.1 History of End-to-End Encryption

Diffie and Hellman proposed public-key cryptography in 1976, a cryptographic system that used key pairs, where the public keys could be disclosed publicly, and the private keys were only known to owners. Computing private keys from public keys were computationally infeasible [38]. This work suggested that a public directory would allow anyone to send private messages to anyone else; and in 1978, the RSA algorithm made the idea practical [39]. This idea led to the OpenPGP standard (RFC 4880) [40]. In 1991, John Zimmerman developed PGP, a software following the OpenPGP standard which supported sending public-key encrypted email, where the RSA algorithm was used to encrypt session keys [41]. However, in this original design, there was no guarantee that a public key was truly belonged to someone. To alleviate this key verification problem, in the second version, he proposed a "web of confidence" (later known as web of trust) for establishing key authenticity [42]. In a web of trust, users can sign each others' keys to endorse their authenticity, and can choose to accept keys that come with signatures from "trusted introducers." Despite this, key verification has remained problematic for many years [2]. Several other email systems also followed the OpenPGP standard, such as GPG Tools [43] and web browser extension Mailvelope [44].

In 1999, the Internet Engineering Task Force (IETF) published RFC 2633 that defined Secure/Multipurpose Internet Mail Extensions (S/MIME), which takes a centralized approach to key distribution: all users have public-key certificates signed by a certification authority (CA), which are distributed along with any signed emails sent by that user [45]. S/MIME allowed straightforward integration of encryption to email clients like Microsoft Outlook and Netscape Communicator and was adopted by some corporate organizations with the capability to manage keys hierarchically, but was not adopted broadly by consumers.

However, both PGP and S/MIME don't really take off. More recently, several researchers and companies have explored ways to split the difference between completely decentralized and completely centralized key management. Gutmann proposed applying *key continuity management (KCM)*, in which keys are trusted on first use but key changes are detected (KCM verifies whether the current key is the same as the previous one), to email [46]. In Apple's iMessage, private keys are generated on users' devices and the corresponding public keys are uploaded to Apple's proprietary directory service. Since private keys are not shared among devices, when sending a message to a user with multiple devices, the message is encrypted once for each device [9, 47]. A reported vulnerability in the iMessage encryption mechanism points to the importance of validating the security of any end-to-end-messaging system [48]. WhatsApp uses a related approach based on the Signal Protocol, but allows users to confirm the authenticity of each other's keys if they choose to [13].

Originally to monitor the certificate issuing in HTTPS, in *certificate transparency*, publicly auditable append-only logs can be used to determine whether rogue certificates have been signed using a stolen CA key [49]. Ryan extended this approach for end-to-end email encryption in pursuit of less cumbersome and more secure approaches to key management [50]. CONIKS extends certificate transparency to allow users to efficiently monitor their own key entries and to support security in the key directory [19]. Google and Yahoo! are exploring variations of this transparency approach for their end-to-end encryption extension [15, 16]. Each of these approaches trades off a different amount of security for convenience.

Other researchers have proposed alternatives to standard public-key encryption that are designed to be more usable. Fahl et al. proposed *Confidentiality as a Service (CaaS)* [51], which operates on a registration model mostly transparent to users. This approach uses symmetric cryptography and splits trust between the communications provider and the CaaS provider. Neither individually can read private messages, but if the two collude they can.

2.2 The Usability of End-to-End Encryption

During the past two decades, researchers and practitioners have made a considerable effort to understand problems with deployment of end-to-end encrypted communication tools and make them more accessible to users.

In 1999, Whitten and Tygar published the now-seminal *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0* [1]. This paper evaluated the interface for PGP 5.0 and found that most users (two-thirds) were unable to successfully sign and encrypt an email in the 90 minute session. This led to a series of follow-on studies for improving user interface designs, such as mitigating problems identified in previous systems [2, 52], whether to adopt automatic encryption and decryption [4, 53], using understandable metaphors [54], designing more informative indicators [55], and whether to integrate with existing systems [56].

Many researchers have focused on the problems of key exchange and management in end-to-end encrypted systems [3, 19, 50, 51, 57, 58]. Garfinkel et al. evaluated *key continuity management* (KCM), and concluded that it was a workable model. Fahl et al. evaluated their CaaS model in a Facebook messaging users study, and found that participants could successfully use this approach to encrypt Facebook conversations [57]. Lerner et al. proposed *Confidante*, a prototype that used *Keybase* [59] to centrally manage public keys and also possibly private keys protected by users' passwords [60]. They showed that lawyer and journalist participants made fewer mistakes using *Confidente* made fewer mistakes than Mailvelope [44]. Some other studies evaluated modern end-to-end encrypted systems and found that users were still susceptible to Man-in-the-Middle (MitM) attacks due to human errors [6,36,37,61,62]. Unger et al. surveyed secure communication tools in 2015, and evaluated their security, usability and ease-of adoption properties [63].

These studies, except [63], largely ask users to do tasks they are unfamiliar with and focus on success rates (key pairs generation and collection, sending and decrypting messages, comparing fingerprints, etc.). They provide valuable insight into how effectively novices can learn a particular system, how specific user interface design choices impact users, and where the difficulties lie. However, users are rarely presented with multiple potential encryption infrastructure models. One study was conducted by Ruoti et al. compared the usability of three key management models: passwords, public key-directory, and identity-based encryption [64]. We note that this study was done after our work in Chapter 3 was published.

2.3 Social Factors and Mental Models in End-to-End Encryption Adoption

Social factors and network effects play an important role in adoption of secure messaging. McGregor et al. considered the specific security and encryption needs of journalists protecting confidential sources, finding that adoption is frequently driven by source preferences and that existing models do not meet some important journalistic needs, such as verifying the authenticity of sources [17]. When evaluating *Confidante*, Lerner et al. also conducted a user study about journalists and lawyers. Their findings suggested that journalists and lawyers had security and operational requirements “divergent enough that they may require different encrypted communication tools entirely” [60]. These studies suggest that to promote adoption of encrypted messaging, the research community must consider the overall ecosystem of features and tradeoffs within which users make adoption decisions.

Beyond explicit usability, users’ mental models have also been found to be fundamental in influencing users’ decisions to (not) adopt encrypted communication tools. Often, users believe that they have no reason to encrypt their email because they have “nothing to hide,” or because they cannot imagine anyone being interested in the messages they are sending [65]. In an interview study at an unnamed non-violent, direct-action (NVDA) organization (which one might expect to be more interested and aware of the benefits of encryption), Gaw et al. found that employees believed “routine use of encryption [was] paranoid [behavior]” [18].

Although E2EE has been more broadly adopted in messaging tools than in email, DeLuca et al. found that users did not prioritize security and privacy when selecting messaging apps [35]. Relatedly, Abu-Salma et al. found that “usability is not the primary obstacle to adoption” [5]; instead, fragmented user bases, lack of interoperability, and limited knowledge about security were significant barriers. These researchers also found that users held misconceptions about the benefits and weaknesses of E2EE — for example, believing that secure communications tools are inevitably futile in the face of powerful hackers — that hinder adoption. Wu et al. explored users’ (mis)conceptions of encryption in depth, identifying four mental models of encryption [8].

The misconceptions identified by these studies imply that improving mental models could support adoption of secure messaging tools. To date, little research has explored how to do this. The Electronic Frontier Foundation (EFF) published a secure-messaging scoreboard to inform users about the security properties of various messaging tools [66]; however, this effort was later abandoned because lay users had difficulty understanding its contents [5]. Tong et al. tested a lock-and-key metaphor for public and private keys [54], with preliminary results indicating some improved understanding. We adopt this lock-and-key metaphor in a portion of our tutorial, described below. Albese et al. explored a variety of different short metaphors explaining the concept of E2EE but did not find any that were particularly successful [67]. Other work has included brief user-education materials as part of a larger study, but did not focus on how to design these materials effectively [6, 58, 68].

2.4 Searchable Encryption

Searchable encryption was first introduced in 2000 by Song. et al., using a symmetric encryption scheme [23]. Since then, numerous works have improved search efficiency and protocol security [24–28, 69, 70]. Many companies have integrated searchable encryption capabilities into products, primarily database systems [71–75]. Fuller et al. provide an overview of searchable encryption solutions from academia and industry, characterizing the tradeoffs between different solutions [76].

Although many searchable encryption solutions have been proposed and evaluated, to our knowledge, only two studies have been done to understand users' perceptions toward such solutions. The first study was a 10-participant pilot that evaluated users' experiences using a web interface to query searchably-encrypted databases [76]. The study found that participants cared more about the expected times than minimizing the mean response. The second study was a 13-participant lab study about a Chrome extension which supported searching end-to-end encrypted emails in Gmail, where participants were provided an email set by researchers and asked to search for specific keywords [77]. They claimed that encrypted search could be applied without violating usability of current non-encrypted systems. We note that the later study was conducted after our work presented in Chapter 4.

2.5 Email Search, Organization, and Mobile Usage

Searching emails, unlike other information retrieval tasks such as web search, is to refind "stuff I have seen" [78]. Researchers have spent significant effort to understand how users search their emails and help them to do so more effectively.

In a lab study, Elsweiler et al. explored some email search query characteristics on Mozilla Thunderbird, e.g. the query length and the field submitted on [79]. They found some factors about the email, such as the time the email was received, whether the searched email was accessed recently, etc. had some correlation with users' email search query choices. In a followup field study, Harvey et al. discovered some search behavioral patterns in email, such as whether and how often the same or similar queries were submitted by the same user, and when users clicked through emails after users performed a search [80]. They also found that some behaviors patterns in email search contrasted with those in web search. Whittaker et al. found that preparatory behaviors such as creating folders are inefficient and do not improve email retrieval success [81]. Cecchinato et al. found that users searched their emails in personal and work account differently due to different email management strategies [20].

More recently, researchers have been able to examine search queries from large email providers and identify broad patterns. Carmel et al. found that among Yahoo! Mail users, most search queries are fully formulated by users (rather than suggested by the email service), and most contain only one word [22]. Similar query lengths were found in Outlook queries [21]. Among the Outlook queries, 18% contained "advanced" search operators, primarily the "from:" and "to:" operators used to specify email senders and recipients. Users are increasingly accessing emails via mobile devices rather than desktops or laptops, reaching 62% in 2019 [82]. Another email marketing report in 2018 also indicate that 75% of consumers say they use their smartphones most often to check email [83].

These email habits will affect users' preferences for searching encrypted as well as plaintext email, and they informed the design of our choice-based analysis, as detailed in Chapter 4.

2.6 Conjoint Analysis for Valuating Privacy

Conjoint analysis is a statistical method for understanding users' relative preferences among multiple-attribute products or services [29–31], and researchers have adopted it to understand various aspects of users' online privacy preferences. Krasnova et al. used computer-aided Adaptive Conjoint Analysis (ACA) to investigate users' privacy values in online social networks (OSN) [33]. They expressed users' preferences for different attributes, including privacy, in monetary value, which allowed them to compare preferences among different features easily. In our study in Chapter 4, we also adopt monetary values as a basis of comparison. Burda et al. explored users' cloud-storage choice decisions by employing a choice-based conjoint analysis [34]. They found that users preferred client-side encryption over server-side encryption, and estimated providing client-side encryption is equivalent to between 0.86 and 1.66 Euros per month. Pu et al. conducted both a full-profile and a choice-based conjoint analysis to understand the factors that influence social app users' valuation of their own and their friends privacy, measured by how much data was collected by an app [32, 84]. They found that app users valued all of their friends' privacy smaller than their own's [32], but vice versa in [84]. Our work in Chapter 4 also adopted the choice-based conjoint analysis.

2.7 Design Principles for Educational Material

The principles and methods used in designing educational material and procedures can have a significant impact on how users gain skills and learn new knowledge. In the work presented in Chapter 5, we designed our tutorial to incorporate some best practices from learning science.

The principle of contiguity states that "the effectiveness of multimedia instruction increases when words and pictures are presented contiguously (rather than isolated from one another)" [85]. We therefore designed our tutorial to include illustrative slides with narration, and used pilot testing to identify a good balance between graphics and words.

In line with recommendations to use first- and second-person point-of-view and make educational materials conversational [86], we designed our examples of encrypted communication to incorporate the participant as a sender/receiver.

Learning science also recommends giving learners opportunities to stop and think about what they have learned, as well as learning-by-doing ("knowledge and skills are acquired and strengthened through actual practice") [87, 88]. We incorporated these ideas by asking participants repeatedly to reflect on what they had learned in the tutorial and what they would want to share with family and friends, as well as a design task exercising their new knowledge.

Chapter 3: User Tradeoffs for Key Management Models

Historically, end-to-end encryption has been difficult for people to use, but tools in recent years have made it more broadly accessible, largely by employing key-directory services. These services sacrifice some security properties for convenience. In a 52-person interview study, we asked participants to complete encryption tasks using both a traditional key-exchange model and a key-directory-based registration model. We also described the security properties of each and asked participants for their opinions. We found that participants could learn to understand properties of different encryption models and make coherent assessments about when different tradeoffs might be appropriate. Participants recognized that a less convenient key exchange model was more secure overall, but considered the key-directory approach to have security sufficient for most everyday purposes.

3.1 Study Design

We used a within-subjects lab study to examine participants' concerns and preferences regarding the usability and security of end-to-end email encryption. Each participant was introduced to two general models for key management, *ex-*

change and *registration*. For both models, we described a public key as a *public lock*. This approach, inspired by Tong et al., avoids overloading the term "key" and was used to provide a more intuitive understanding of how public-key pairs operate [54].

In the exchange model, similar to traditional PGP, participants generate a key pair and then distribute the public locks to people they want to communicate with. We offered participants several methods for exchanging locks: the same email account they would use for encrypted communication, a secondary email account, posting the public lock on Facebook or sending via Facebook Messages, or using a simulated "key server" to upload their lock to a public directory. (These options were presented to each participant in a random order.) Simulated correspondents (played during the study by a researcher) sent back their own public locks via the same mechanism the participant chose, or via the mechanism the participant requested.

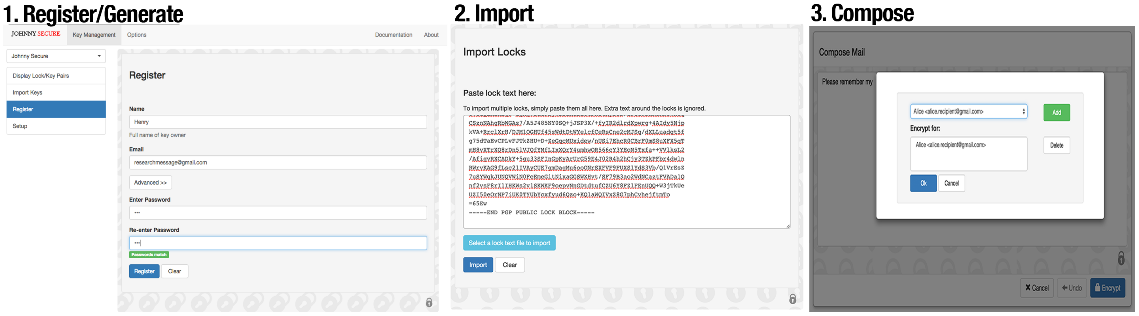
In the registration model, participants again generate a key pair. In this case, they "register" their public lock with a simulated key directory service; correspondents' locks were pre-installed to simulate automatically retrieving them from the directory. Participants were thus able to send and receive encrypted email from all simulated correspondents immediately upon creating and registering their own keys. In iMessage and other tools such as WhatsApp and Signal, the key generation step itself is completely transparent to users, who may never realize a key was created; we chose instead to make key generation explicit to help users understand the process.

Within each model, participants were asked to complete a series of simulated tasks, such as exchanging encrypted emails in a role-playing scenario (see details below); they were also introduced to a brief, non-technical review of the security properties of each model. Participants were asked to give their opinions about each model immediately after completing the tasks and security learning for that model. We also conducted an exit interview regarding the overall usability and security of each model, whether participants would use it themselves or recommend it to others, and in what circumstances it might or might not be appropriate.

We chose a within-subjects study because we were primarily interested in how participants would understand and value the tradeoffs among the options. As shown in Table 5.2, we varied the order of activities to account for ordering effects. Participants were assigned round-robin to one of these four possible orders of activities.

First activity	**Second**	**Third**	**Fourth**
ET (Exchange, Tasks)	ES	RT	RS
ES (Exchange, Security learning)	ET	RS	RT
RT (Registration, Tasks)	RS	ET	ES
RS (Registration, Security learning)	RT	ES	ET

Table 3.1: The order of activities varied across participants. Each participant worked with either the Exchange (E) or the Registration (R) model first. Within each model, participants either completed the encryption Tasks (T) first or learned about Security properties (S) first. Throughout the dissertation, participants are labeled by first activity; e.g., participant RT3 completed encryption tasks for the registration model first.



Name: Henry

Full name of key owner

Email: researchmessage@gmail.com

Enter Password: •••

Re-enter Password: •••

Paste lock text here:

To import multiple locks, simply paste them all here. Extra text around the locks is ignored.

```
CSznNAhgRbWGAz7/A5J485NY0SQ+jJSP3X/+fyIR2dlrdXpwrg+4AIdy5Njp
kVA+RrclXrH/DJM1OGHUf45zWdtDtWYelcfCeRsCne2cMJSq/dXLLuadqt5f
g75dTaEvCPLvFJTkZHU+D+ZeGqcMUxidew/nUSi7EhcR0CBrF0mS8uXFX5qT
mH8vXTrXQ8rDn5lVJQfYMfLIxXQrY4umhwOR566cY3YEoN5Txfa++VVlksL2
/AfiqvRXCADkY+5gu33SFInGpKyArUrG59E4J02R4h2hCjy3TZkPFbr4dwln
RWrvKAG9fLsc2lIVAyCUE7gmDaqMu6ooONrSXFVF9FUXSlYdS3Vb/Q1VrEsZ
7uSYWqkJUNQVWiN0FeEmeGitNixaGGSWXHvt/SF79B3ao2WdNCaztFVADa1Q
nf2vsF8rIlIHKWs2vlSKWKF9oepvNnGDtdtufCZU6Y8FZ1FEnUQQ+W3jTkUe
UZI50eOrNP7iUK0TYUbYcxfyud6Qzo+KQlaWQIVxZ8G7phCvhejftmTo
=65Ew
-----END PGP PUBLIC LOCK BLOCK-----
```

Alice <alice.recipient@gmail.com>

Encrypt for:

Alice <alice.recipient@gmail.com>

Figure 3.1: To use our extension, participants first generated (or registered) a key pair. Participants using the exchange model then needed to import recipients' locks. Finally, when composing encrypted emails, they clicked the Encrypt button (shown in the lower right of Step 3) to bring up a modal dialog to select recipients.

3.1.1 Encryption tasks

The set of encryption-related tasks for each model is shown in Table 3.2. In both models, participants were asked to generate a key pair locally. In the exchange model, participants then exchanged public locks with simulated friend Alice, including both sending Alice their lock and importing the lock received in return. In the registration model, participants registered with a simulated central service and had their public lock automatically "uploaded" and others' locks automatically "imported." After the locks were exchanged or the participant registered, participants composed and sent an encrypted email to Alice. A researcher, posing as Alice, sent an encrypted response. As a slightly more complex task, participants were asked to send an encrypted email to a group of two recipients. This task was designed to get participants to begin to consider how the two models scale. Finally, we asked participants to consider how they would handle several other situations, including communicating with larger groups of people and various possible errors related to losing or publicizing one's own private key or losing other users' public locks. The possible errors were specific to each model and are shown in Table 3.2. In the interest of simplicity, we did not include any email signing (or signature verification) tasks.

Encryption tasks were completed using a Gmail account created especially for the study and a Chrome browser extension based on Mailvelope [44]. We modified Mailvelope to remove its branding, change the labels to match our lock/key metaphor, and reduce the interface to include only those features relevant to the study tasks. Figure 3.1, right shows a screenshot of sending encrypted email with our extension. As in Mailvelope, users of our extension compose an email and then use an "Encrypt" button to select recipients. Upon receiving encrypted email, users are prompted to enter their password to decrypt it (with the option to save the password and avoid future prompting).

We created two versions of our extension, one for exchange and one for registration, taking care to make them as similar as possible. The only two visible differences were (1) changing the "Generate lock/key pair" menu item and subsequent screen (exchange model, Figure 3.1, left) to read "Register" (registration model) and (2) a lock import screen (Figure 3.1, center) that was only relevant in the exchange model.

We also provided participants with detailed instructions to help them use the Chrome extension. By simplifying the interface, keeping it consistent, and providing detailed instructions, we hoped participants' reactions would better reflect

Task #	Exchange Model	Registration Model
1	Generate public lock/private key pair	Register public lock/private key pair
2	Exchange public locks with Alice	N/A
3	Send encrypted email to Alice	Send encrypted email to Alice
4	Decrypt received email from Alice	Decrypt received email from Alice
5	Exchange public locks with Bob and Carl	N/A
6	Send encrypted email to Bob and Carl	Send encrypted email to Bob and Carl
7	Decrypt received email from Bob and Carl	Decrypt received email from Bob and Carl
8	Imagine sending encrypted email to 10 people.	Imagine sending encrypted email to 10 people.
9	Consider misconfigurations: a. Lose Alice's public lock b. Lose own private key c. Publicize own private key	Consider misconfigurations: N/A b. Lose own private key c. Publicize own private key

Table 3.2: The encryption-related tasks completed by participants. The tasks differed slightly in the two models.

the inherent properties of each model rather than idiosyncrasies of a particular interface.

3.1.2 Description of security properties

We provided participants with short, non-technical descriptions of possible attacks on each model.

Exchange model For the exchange model, we described a man-in-the-middle attack in which the attacker could intercept or replace keys during the exchange process: “For example, when you try to get the public lock from Dave, the attacker secretly switches the public lock to his own. You think you have Dave’s public lock, but in fact you have the attacker’s. As a result, the attacker can read your email. The attacker will then use Dave’s public lock and send the encrypted email to Dave, so that neither you nor Dave realize the email has been read.” We mentioned that this type of threat doesn?t happen usually, because it requires the attacker to have much power and resources to achieve this. We also showed participants the illustration in Figure 3.2.

We decided not to include an option for key signing in our exchange model both because we thought it would add unnecessary complexity to our explanations and because it does not change the underlying requirement to trust some keys that are manually exchanged.

Registration model For the registration model, we primarily described a man-in-the-middle attack enabled by the key directory service: “When you try to send encrypted emails to Dave, you think the database will return Dave’s public lock to you. But in fact, it returns the attacker’s lock, so the attacker can read your

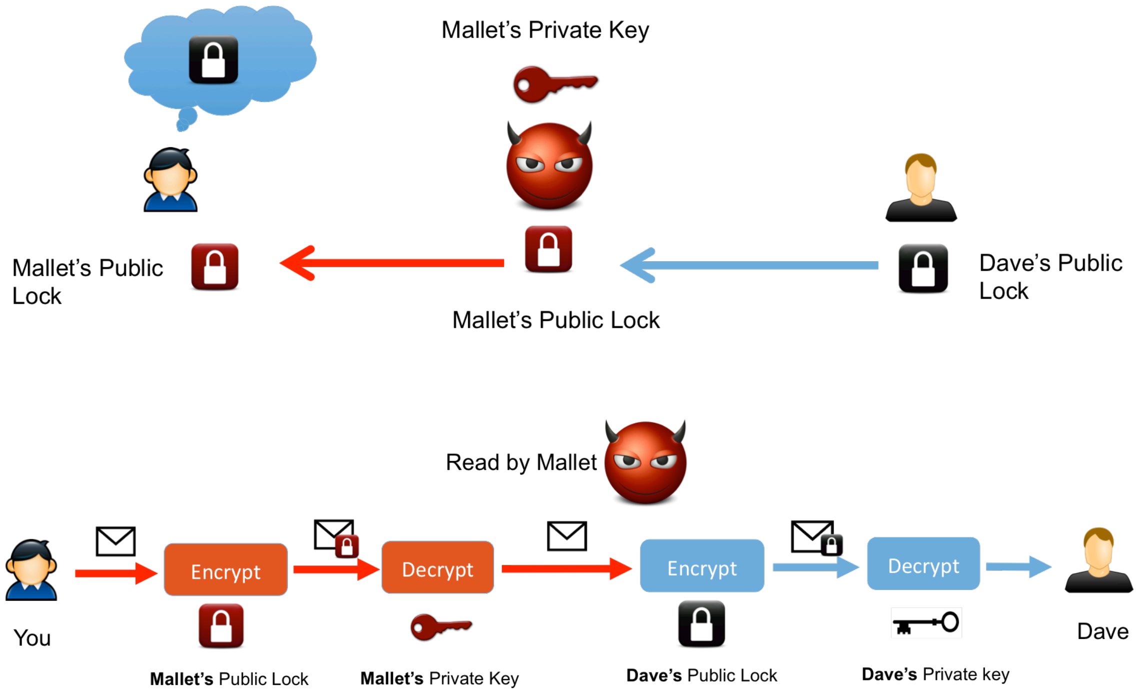


Figure 3.2: Possible attacks on the exchange model

email. Therefore, you need to trust the email provider in this system." We showed participants the illustration in Figure 3.3.

In addition, we described two variations on the basic key directory approach: the Confidentiality as a Service (CaaS) variation [51, 57], and an auditing model similar to the one proposed by Google and CONIKS [16, 19]. Because these approaches are not currently in wide use the way the iMessage-analogous system is, they were treated as secondary options. The auditing model was added (to the end of the interview, to maintain consistency with earlier interviews) during recruiting, and was therefore presented only to 24 participants.

The security of the CaaS variation was described as follows: "There is a third-party service (not the email provider) as an intermediary. In this version, neither

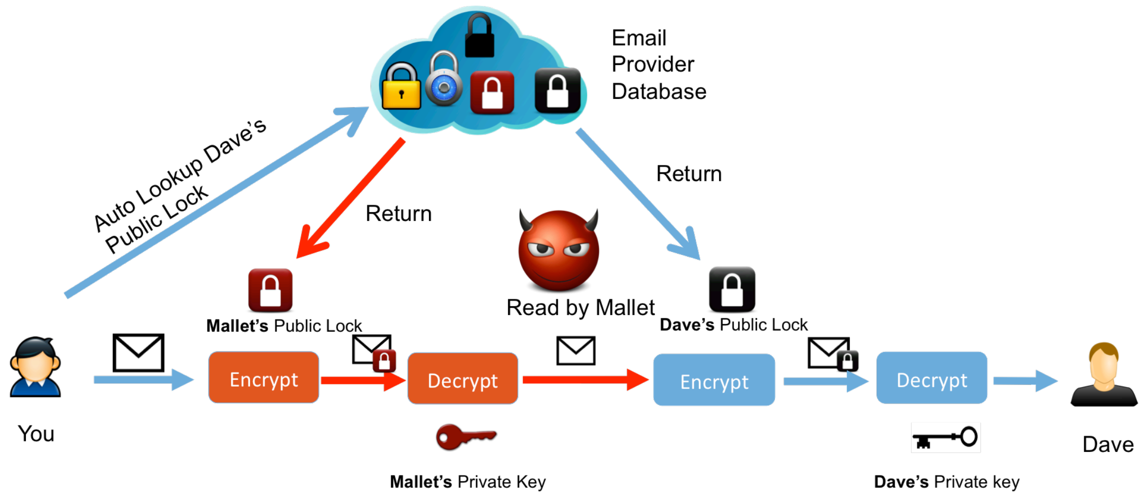


Figure 3.3: Possible attacks on the registration model

the third-party service nor your email provider can read your email themselves. However, if your email provider and the third-party service collaborate, they can both read your email. Therefore, you need to trust that the two services are not collaborating."

We described the auditing variation as follows: "The email provider stores all users' public locks, just like [the primary registration model]. But there are other parties (auditors) who audit the email provider, to ensure it is giving out correct public locks. These auditors may include other email providers, public interest groups, and software on your devices. If the email provider gives you a public lock that doesn't belong to the recipient, or gives someone else the wrong public lock for you, these auditors will notify you. You (or someone else) may use the wrong lock temporarily (for an hour or a day) before you are notified. In this model, you don't need to trust your email provider, but you need to trust the auditors and/or the software on your device. Because there are several auditors, even if one auditor does not alert you another one probably will."

3.1.3 Participant feedback

Participants were asked questions after completing tasks for each model and at the end of the process. After completing tasks and learning about security for each model, participants were asked for their agreement (on a five-point Likert scale) with the following statements:

- The task was difficult (for each task).
- The task was cumbersome (for each task).
- The system effectively protected my privacy.

The first two questions were repeated for each task in Table 3.2. Before answering, participants were reminded that difficult tasks would require intellectual effort or skill, while cumbersome tasks would be tedious or time-consuming. After each Likert question, we asked participants to briefly explain their answer choice (free response).

After completing all tasks and learning about all security models, participants were asked several summative questions, including:

- Willingness to use each system, on a five-point Likert scale, and why.
- Willingness to recommend each system, on a five-point Likert scale, and why.
- What the participant liked and disliked about each system.

3.1.4 Recruitment

We recruited participants 18 or older who were familiar with Gmail and Chrome and who send and receive email at least 3 times per week. We placed flyers around our university campus and the surrounding area, advertised via email listservs for the university, and advertised on web platforms like Craigslist. All interviews were conducted in person at our university campus; interviews were video recorded with the explicit consent of participants. Participants were paid $20 for a one-hour study and were reimbursed for parking if utilized. Our study protocol was approved by the university's Institutional Review Board.

Participants took part in the study in multiple batches between August 4, 2015 and Feb 5, 2016. For context, all of the participants engaged in the study well after Edward Snowden revealed details of the National Security Agency's broad surveillance of digital communications [89], but before Apple publicly fought the Federal Bureau of Investigation to not weaken the security of a locked and encrypted iPhone [90]. We include this to note that average users' views of security, privacy, and here specifically, encryption are a moving target. Future events may continue to shift public opinion on the importance of encrypted communications.

3.1.5 Data analysis

We used statistical analysis to investigate participants' responses to the exchange and registration models. To account for our within-subjects design, we used the standard technique of including random effects to group together responses from each participant. We used a cumulative-link (logit) mixed regression model (CLMM), which fits ordinal dependent variables like the Likert scores we analyzed [91]. We included three covariates: whether the participant performed tasks or learned about security first, whether the encryption model she was evaluating was seen first or second, and the encryption model itself (exchange or registration). This approach allows us to disentangle the ordering effects from the main effects we are interested in. For each encryption model, we tested regression models with and without the obvious potential interaction of encryption type with order of exposure to that type, selecting the regression model with the lower Akaike information criterion (AIC) [92].

Qualitative data was independently coded by two researchers using textual microanalysis [93]. After several iterative rounds of developing a coding scheme, the researchers each independently coded the full set of participant responses, with multiple codes allowed per response. The researchers originally agreed on more than 94% of the codes, then discussed the instances of disagreement until consensus was reached. Where appropriate, we report prevalence for the final qualitative codes to provide context.

3.1.6 Limitations

Our methodology has several limitations. Our lab study participants had only limited exposure to the different encryption models, and their opinions might change after working with the models for a longer period or in the real world scenarios.

Participants also only imagined their responses to misconfigurations, rather than actually handling them. Nonetheless, we argue that first impressions like the ones we collected influence whether people will try any tool for long enough to develop more-informed opinions. It is well known that study participants may rate tools they examine more favorably (acquiescence bias) [94], which may explain the high rate of participants reporting they wanted to use or recommend each model. Because we are primarily interested in comparing results between models, we believe this has limited impact on our overall results; however, the absolute ratings should be interpreted as a ceiling at best.

In order to provide participants with any understanding of the security properties of each model, we had to prime them with descriptions of possible attacks. While this priming was unavoidable, we endeavored to keep the security descriptions as neutral as possible so that priming would affect both models approximately equally.

To avoid overwhelming participants, we evaluated a limited subset of possible encryption models and possible tasks; in particular, we left out key signing as well as any email signing or signature verification tasks. We did this because we believe signing to be the most difficult aspect of cryptography for non-experts to understand (see e.g., [1]), but including it might have provided a broader spectrum of user opinions.

Our registration model, unlike, for example, iMessage, was not completely invisible to participants. We believe it was necessary to give participants something to do other than just sending a normal email, in order to help them think through the tradeoffs involved. While presumably using a fully transparent variation would only have increased the convenience gap between the two models, prior work indicates that taking any steps at all increases feelings of security [4]. This may have contributed to the small observed security gap between the two models, but we argue that a version with no intervention required would lead to underestimations of security. Because we added the auditing model late, we were not able to get as much feedback about it or to compare it quantitatively to the other models we examined. In addition, because all participants encountered it last, their responses may reflect some ordering effects. Nonetheless, we believe the qualitative data we collected does provide interesting insights. Future work can examine all these alternatives in more detail.

As with many lab studies, our participants do not perfectly reflect the general population, which may limit the generalizability of our results.

3.2 Participants

A total of 96 people completed our pre-screening survey. We interviewed the first 55 who qualified and scheduled appointments. Three participants were excluded for failing to understand or respond coherently to any directions or questions.

Demographics for the 52 participants we consider are shown in our papers [58, 95]. Among them, 60% were male and 80% are between the ages of 18-34, which is somewhat maler and younger than the general American population. 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, math, or engineering.

Despite this high rate of technical participants, most had little experience with computer security. We measured security expertise using a slightly adapted version of the scale developed by Camp et al. [96]. Higher scores indicate security expertise; the maximum score is 5.5 and the minimum score is zero. Only two of our participants scored 3 or higher.

Using a Kruskal-Wallis omnibus test, we found no significant differences among our four conditions in age, gender, country of origin, or security expertise ($p > 0.05$).

3.3 Results and Analysis

We present participants' reactions to the convenience and security of each model, followed by a discussion of their overall preferences among the models.

3.3.1 Registration is more convenient

Unsurprisingly, our participants found the registration system considerably more convenient, rating the exchange system as significantly more cumbersome and more difficult. Figure 3.4 and Tables 3.3 and 3.4 show the results of the CLMM for cumbersome and difficult, respectively, for Task 8: imagining sending email to a group of 10 people. In reading the CLMM tables, the exponent of the coefficient indicates how much more or less likely participants were to move up one step on the Likert scale of agreement.

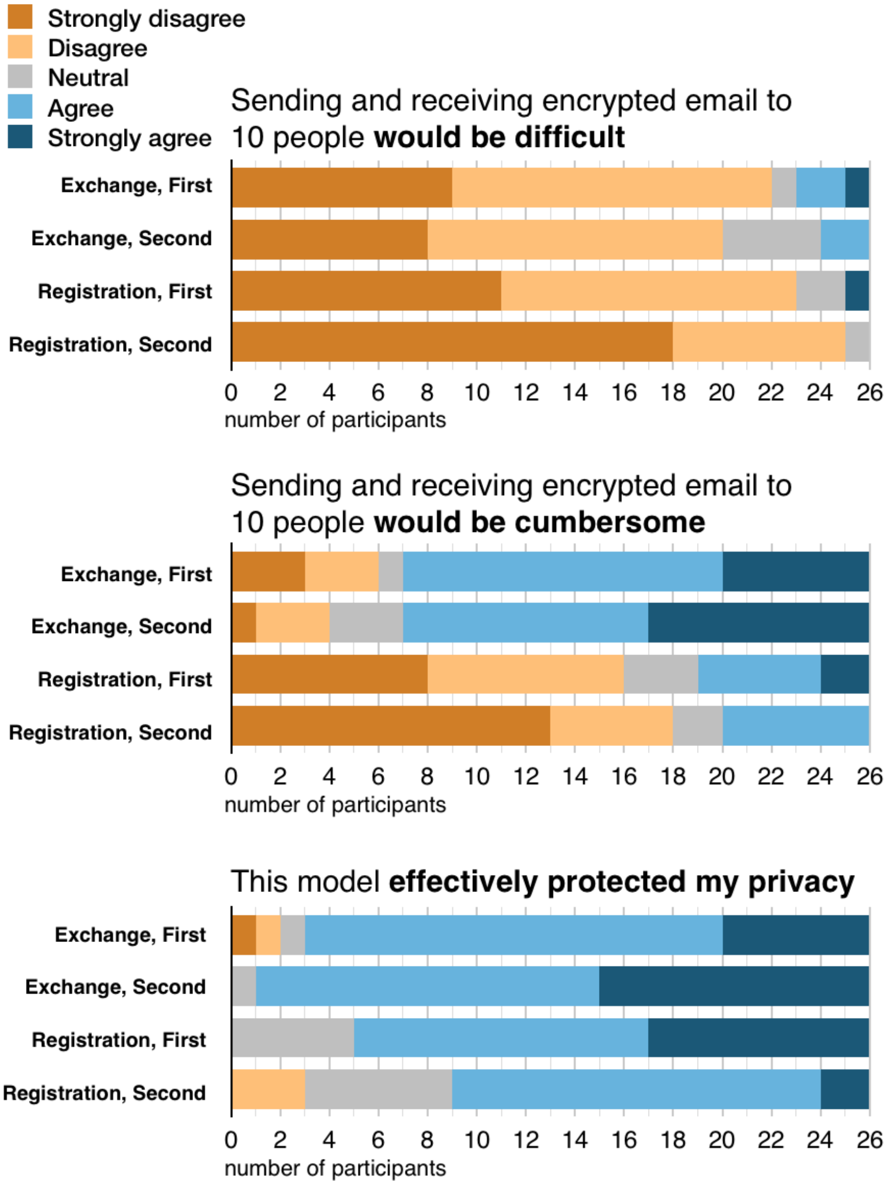


Figure 3.4: Participants' ratings of difficulty and cumbersomeness (Task 8) as well as whether participants thought the model protected their privacy. Labels indicate which model participants evaluated along with whether they saw that model first or second; e.g., "Exchange, First" indicates ratings for the exchange model among those who saw it first, which includes ET and ES participants.

For cumbersomeness the exchange model was associated with almost a $20x$ increase in likelihood of indicating more agreement. The exchange model was also about $5x$ more likely to be perceived as more difficult.

Factor	**Coef.**	**Exp(coef)**	**SE**	***p*-value**
tasks first	0.010	1.010	0.589	0.986
second model	-0.166	0.847	0.393	0.673
exchange	2.978	19.656	0.567	<0.001*

Table 3.3: Regression table for cumbersomeness, Task 8. The non-interaction model was selected. Non-significant values are greyed out; significant values are indicated with an asterisk.

Factor	**Coef.**	**Exp(coef)**	**SE**	***p*-value**
tasks first	-0.282	0.754	0.747	0.706
second model	-0.726	0.484	0.460	0.115
exchange	1.674	5.333	0.520	0.001*

Table 3.4: Regression table for difficulty, Task 8. The non-interaction model was selected. Non-significant values are greyed out; significant values are indicated with an asterisk.

Participants' comments generally supported this finding: that the exchange model was dramatically more cumbersome and somewhat more difficult. Within the exchange model, the most tedious task was manually exchanging locks and the most commonly mentioned reason was waiting for a correspondent's public lock. ES9 was concerned that the exchange model was “time-consuming, especially sending urgent emails. I have no choice but to wait for” the correspondent’s public lock. RS5 agreed, saying “There are so many steps to exchange locks.” RS13 mentioned that the cumbersomeness of exchanging locks was mainly related to initialization: “If their locks are already there, it would not be cumbersome. But if I have to ask them to send me locks person by person, it’s more cumbersome.” One participant (ET10) worried it would be additionally cumbersome to use the exchange model on a phone due to copying and pasting public keys.

Several participants expressed concern that users with low digital literacy might have trouble with the exchange model or prefer the registration model. For example, RS12 recommended the registration model “especially to people that don’t know very well how to use a computer . . . old people, like my father.” ET2 agreed that the registration model is “easy to teach others to use.”

While few participants considered any of the tasks very difficult, choosing a mechanism for exchanging locks was considered the most difficult step by a few participants, such as RS4, who mentioned having to “think about a safe way to exchange public locks,” and RS10, who was concerned about making an exchange error while multitasking.

Other concerns related to the general issue of convenience included scalability and misconfiguration. As RT9 said, “When I send to more people, I have to be very careful, especially when I choose to send them my public locks separately. I need to control every step is correct.” ET13 said, “When I exchange locks with ten people, I can send my lock, which is kind of easy. But I have to get ten replies for their locks. I can easily get lost. And if I exchange with 100 people, it'll be a nightmare." A few participants were concerned about the difficulty of recovering from misconfiguration, and ET10 was particularly worried that others' mistakes could cause additional hassle for her: "If other people lose their private keys and send me new public locks, I will be overwhelmed." RS12 agreed that "if accidents or mistakes happen, it bothers both parties to do extra steps."

The inconvenience of the exchange model could potentially be mitigated somewhat by posting the key publicly or semi-publicly (on a key server or Facebook profile), rather than sending it individually to different recipients. About a third of our participants chose this option: 34 used the primary email, 20 used the secondary email, 10 used Facebook chat, five posted to the Facebook profile, and 13 used the key server. (Some participants chose multiple methods during different tasks.) However, few of the participants who used the public or semi-public methods mentioned the added convenience as a reason for their choice. RT12 said exchanging locks is "not too cumbersome, it's manageable through the lock server to exchange locks." On the other hand, a few participants chose the key server because they thought it was more secure than other choices we provided.

3.3.2 The perceived security gap is small

We found that participants understood and thought critically about the security properties we explained to them for each model. Surprisingly, they found the exchange model to be only marginally more secure than the registration model, for a variety of reasons.

Exchange: Manual effort may lead to vulnerability Most participants believed the exchange model was most secure overall, with 48 (out of 52, 92.3%) agreeing or strongly agreeing that this model protected their privacy. Nonetheless, participants also expressed concern that managing key exchange themselves would create vulnerabilities. More than half (27 out of 52) of participants were concerned about the security of the medium used to exchange locks.—ET4 worried that 'the key server [could] be manipulated or compromised." RT7 had several such concerns, including that an attacker could break into her Facebook account to post an incorrect public lock, or that public Wi-Fi in a coffee shop could be unsafe for transmitting locks. Overall, she said, "There are too many exchanges between different people. Exchanging [locks] to many people may go wrong." Others, like RS5, worried that their internet service provider could "sit between my recipient and me" and switch locks to execute a man-in-the-middle attack. ET7 was one of several participants who noted that "If I send the public locks and encrypted emails using the same email provider, it's not very secure." RT9 thought the ability to choose from different mechanisms to exchange locks provided added security, but worried that "people may choose a particular way in real life. It's their habits, so that attackers may anticipate" their choices and take advantage of their known routine. ES10 asked his recipients to send back his public lock, both through Facebook and via email, so he could verify for himself that the received public locks were not altered.

Other participants were concerned about making a mistake during the ongoing responsibility of managing keys. As ET10 put it, “Every time when I send or get a public lock ... there is a probability, even though not high, that my privacy is compromised. Then when I exchange public locks with many people, this probability will increase exponentially.” RS12 worried that “I don’t know what I actually need to do when I lose or publicize my private key. I am not confident about my answers. Non-tech experts may make mistakes.”

Other participants mentioned that careless or compromised users could ruin the security of a whole group. ES12 said, “If I send to Alice, and she decrypts and goes away, then other people can see the email or even copy that email.” ET8 said that “Within a company, if one person is hacked, then the whole company is hacked. It’s hard to track the source, just like rotten food in the refrigerator.” ET4 agreed that “There can be attacks on users with weak security, which may impair the whole user system.”

Registration: Some concern but generally trusted As expected, many participants were concerned about the need to trust email providers in the registration model. As ES5 said, having the email provider store “all public locks ... is not very comfortable.” Despite this, however, most participants (38 out of 52) trusted the system protecting their privacy. Also, the CLMM results in Table 3.5 and Figure 3.4 indicate that the order in which the models were introduced played a significant role. Participants who saw the registration model first were more comfortable with it: 9 of 26 who saw registration first strongly agreed that the model protected their privacy, compared to only 3 of 26 who had already heard about the more-secure exchange model. None of the participants who saw registration first disagreed that the model protected their privacy, while 3 did so after seeing the exchange model first.

Factor	**Coef.**	**Exp(coef)**	**SE**	***p*-value**
tasks first	-0.332	0.717	0.527	0.528
second model	-1.684	0.186	0.699	0.016*
exchange	-0.288	0.750	0.670	0.668
second model :: exchange	2.818	16.740	1.124	0.012*

Table 3.5: Regression table for privacy. The interaction model was selected. Non-significant values are greyed out; significant values are indicated with an asterisk.

This general confidence in the registration model reflects many participants' belief that even though email providers could compromise the security of the primary registration model, they would be unlikely to. Ten participants mentioned that they trust their own email provider (presumably if they didn't they would switch services). ET11 mentioned that his email provider "knows me, I have my name there," and ET12 said that "All public locks are stored in a database, and I trust the database. This database provides extra security." ET13 provided a slightly different view: that some email providers are untrustworthy in well-known ways. "Everyone knows the Gmail potential vulnerabilities. And some people who are particularly hiding some information from the U.S. government, they will choose Yandex email from Russia, because they'd rather be intercepted by the Russian government, instead of the U.S. government. . . . If you are an activist in US, and you don't want the U.S. government to know what you are up to, so I will choose some email services I feel comfortable with."

Several (7 participants) were specific about which kind of providers they would trust: RT8 would trust "certain big companies, not small companies," because big companies must protect their reputations. RT10 felt similarly, with an important caveat, mentioning that big companies like "Google and Yahoo! don't do such things [violate users' privacy] usually, unless the government forces them to do so. In general, it's secure." ET11 would choose an email provider with many users since "the more people using it, the more reliable." RT2, on the other hand, preferred to trust institutions like universities that "own their own email server" to better protect her privacy.

Also contributing to the general comfort level with the registration model is that participants do not believe most or any of their communication requires high security. RT4 said "encryption is not necessary for me," and RS8 agreed, saying "If I have some private information, I won't put it on the Internet."

CaaS and auditing: Some additional perceived security for registration

Out of all 52 participants, twenty-two participants preferred the CaaS variation to the primary registration model, and 12 preferred the primary model to CaaS; the rest rated the two variations the same. The most popular explanation for preferring CaaS was a belief that different companies would not collude. RS7 said that the two parties would not collude because they do not "even trust each other." ES12 was cautiously positive, saying "This separation makes me feel good. However, [the two parties] still can possibly collaborate.” Relatedly, ES8 suggested that the CaaS approach was more secure because “If one party is screwed up, you have another one to protect [your email]. You are still safe.” These comments have implications for the auditing model as well; the belief that different parties are unlikely to collude and recognition that distributing trust spreads out possible points of failure would also point to more trust in the auditing model.

On the other hand, four users thought the primary registration model was more secure than the CaaS variation because adding more intermediate systems and providers reduces overall security. RS1, for example, said that “involving more systems may complicate the system, so it is less trustful.” A few users said that the possibility of collaboration invalidates the entire model: for example, ES13 said “I don’t trust that much the whole system. I am afraid they may collaborate.” Two participants (ET4, RS13) were afraid that in CaaS the two parties might collaborate for a sufficiently large gain. For example, RS13 said “They will not collaborate for one or two person’s email, but for many, a group of people.”

Other participants were concerned about whether the third party in CaaS was trustworthy. ET11 worried that “the third party service is not verified,” and RT9 said his opinion “depends on who the two entities are. If the two companies are big names, like Gmail and Facebook, it seems more secure. Also if they do different types of services [from each other], it’s more secure.”

The 24 participants who were briefly exposed to the auditing variation gave generally positive feedback. ES9 was happy that “somebody is supervising” lock distribution and watching for problems, and ET13 said “Obviously it’s extra secure.

Other parties are verifying it, like an anti-virus system telling me if something goes wrong." ET8 appreciated that "if something goes wrong, I will be notified." The presence of many auditors reassured participants that collusion was unlikely; for example, RT10 commented that "it's less likely that all auditors [would] do something bad," and RS12 appreciated that "there are many auditors who can notify me."

Several participants, however, were concerned about the reliability of the auditors: RS9 said, "I want to know who these auditors are, . . . their reputations, and whether they are truly independent." Similarly, RT13 said, "Am I able to choose auditors? This is a big question. The principle is good . . . but I want to know who they are and how to choose them, because I need to trust them." One user (ET10) was concerned that auditors from competing companies might have incentives to lie about each others' behavior, making it hard to know who to trust. According to ET11, involving more parties reduced the overall trustworthiness: "Putting trust to only one party is better."

Ten participants expressed concern about the time lag for notification, noting that "a lot emails have already been sent" with even an hour's delay (ES10). RT11 said "It should be immediate notification. Even an hour is too late. . . . Something bad has already happened." Others, however, were more pragmatic: "Immediate notification is ideal, but I don't expect immediateness in reality" (RT9). ET13 said the time lag "is a vulnerability. It depends on how often I send encrypted emails. If I use it very often, then it's vulnerable." Similarly, RT12 pointed out that "If I don't send the email, it doesn't matter, but in this case, I don't receive the wrong locks.

. . . Notification happens after the fact that I already received the wrong lock."

3.3.3 Overall comparison between systems

After exposing them to both models, we asked participants whether they would use or recommend the exchange model, the primary registration model, or the CaaS registration model. Figure 3.5 shows that the exchange model and CaaS variation were slightly preferred to the primary registration model. The number of participants who agreed or strongly agreed to use or recommend each model were 27, 23, and 28 (use) and 29, 21, and 28 (recommend). The CLMM results (Tables 3.6 and 3.7), which take the exchange model as a baseline, show no significant difference between exchange and either variation of registration for would-use, but do show that the primary registration was recommended less frequently than the exchange model. The 95% confidence intervals for each model indicate no significant differences between the primary and CaaS registration models in either case.

The regression models also indicate that participants who completed the encryption tasks before hearing about security properties were less likely to use or recommend any model than those who heard about security properties first. We hypothesize that participants who used the encryption extension before hearing about security anchored on the inconvenience of the tool rather than its privacy benefits. While this does not provide useful insight about comparing the different systems, it does underline the need for careful consideration about how new encryption tools are presented to the public.

Factor	**Coef.**	**Exp(coef)**	**SE**	***p*-value**
tasks first	-0.606	0.546	0.308	0.049*
second model	-0.026	0. 975	0.291	0.930
registration (primary)	-0.376	0.687	0.358	0.294
registration (CaaS)	-0.077	0.926	0.360	0.823

Table 3.6: Regression table for whether participants would use each model. The non-interaction model was selected. Exchange is the base case for model type. Only whether participants completed tasks first or heard about security first was significant.

Factor	**Coef.**	**Exp(coef)**	**SE**	***p*-value**
tasks first	-0.678	0.508	0.303	0.025*
second model	-0.198	0.820	0.291	0.496
registration (primary)	-0.915	0.401	0.368	0.013*
registration (CaaS)	-0.490	0.613	0.366	0.180

Table 3.7: Regression table for whether participants would recommend each model to others. The non-interaction model was selected. Exchange is the base case for model type. Primary registration is significant (less recommended vs. exchange), while CaaS is not significantly different from exchange. Participants who completed the encryption tasks before hearing about security properties were signficantly less likely to recommend any model.

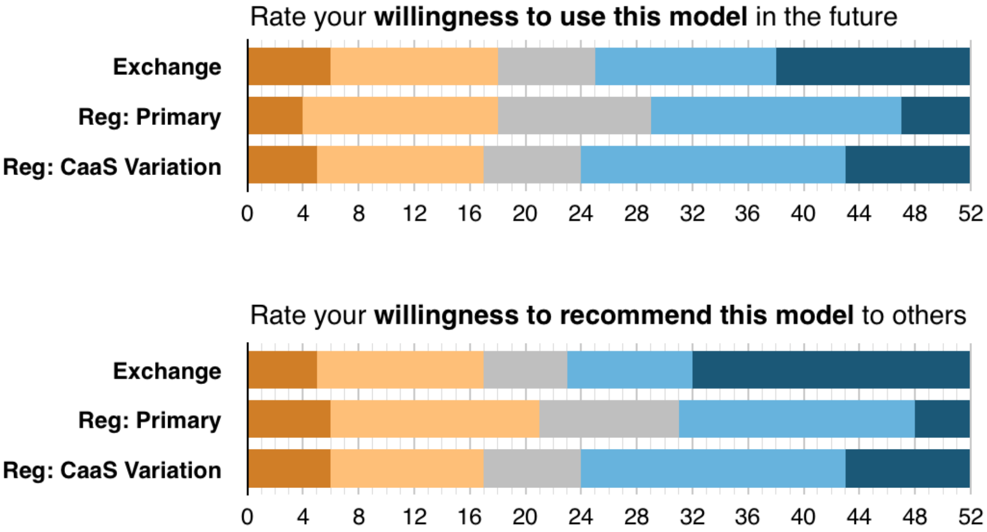


Figure 3.5: Participants' ratings of whether they would use or recommend each model.

We asked participants why they would or would not use each system, and categorized each participant's self-reported most important reason as related to security, usability, or both. (Details of participants' usability and security opinions for each system were discussed in Sections 3.3.1 and 3.3.2 respectively.) For participants who would not use a system, we also included having no need for encryption as a separate category. Figure 3.6 shows the results. Some participants gave more than one answer; a few did not give meaningful responses.

Unsurprisingly, the perception of better security attracted participants to the exchange model, while poor usability drove them away. Participants' reactions to the two registration models were more complicated. In both cases, insufficient security was the most common reason for rejecting the systems; however, participants who said they would use the primary registration model were evenly split between

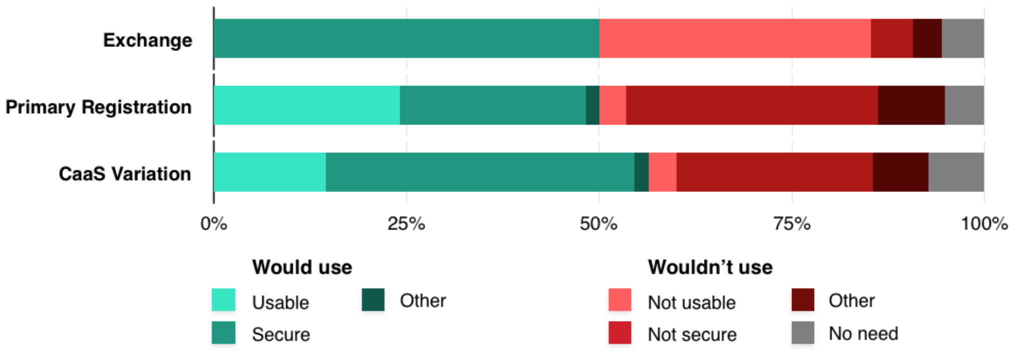


Figure 3.6: The most significant reason why participants would and would not use each model. We note here that while the number of participants who would use each system is similar, their reasoning varies. For example, prospective users of the exchange model uniformly cite security, while prospective users of the two registration models cite a mixture of security and usability.

whether its usability or its security was more important. Participants who said they would use the CaaS model largely but not uniformly cited its security properties.

Participants who said they would use the exchange model generally described using it for high-security information only, or only at a small scale. ES6 exemplified this trend, saying the exchange model is "the safest one. I want to use it in small scale, like one or two people, ... like private and personal things. But I don't want to use it every day." RS9 felt similarly: "I think this system is more effective with fewer people, maybe under ten. I would use it when I send my credit card information to my Mom, instead of QQ or Wechat [two instant messaging services]." ES10 said he would use the exchange model for client projects, which should be kept secret until they are finished. Among the 27 participants who agreed they would want to use the exchange model, none mentioned using it with a large group; 16 said they would use it for very private information while only one said she would use it for general or everyday emails.

In contrast, participants who said they would use either variation of the registration model mentioned "contacting a large number of customers" for payroll or financial information (ET6) as well as "party and meeting announcements" (ET9, RS13). RT8 said she would use the registration model for information that was "overall private, but would not be a disaster if disclosed, e.g., my daughter is sick." ES7, a teacher, said she would use the exchange model only for "extremely sensitive information, such as SSNs," while she would use the registration model to send "location information or grade information." In total, 15 participants who wanted to use either variation of the registration model mentioned general email or large-scale communications.

These results suggest that although most participants said they would use both systems at least sometimes, quite a few wanted encryption only in specific circumstances. Between the exchange and registration models, however, our participants found the registration model useful in a broader variety of circumstances.

Using vs. recommending As expected, most participants (44) who said they would use a system also said they would recommend it to others, and vice versa, but a few gave interesting reasons for answering differently. ET4 said he would not use the exchange model because it was too cumbersome, but would recommend it to others who have stronger privacy requirements. Similarly, RT4 said that "encryption is not necessary for me," but recommended the CaaS variation of the registration model because it is “easier to use [than the exchange model] and more secure than the vanilla [primary] registration system.”

Registration vs. no encryption We did not explicitly ask participants to compare these encryption models to unencrypted email. However, 5 participants who had concerns about the security of the registration model (total 14 rated less than 4) also mentioned that it does provide a valuable security improvement over unencrypted email. ET7 said “The email is not raw, which is another layer of security. ... Doing encryption gives me a security sense that I lock my door myself.” RT12, explaining why he would use the primary registration model, noted that “I have to trust the email provider, which is problematic, but . . . it’s better than raw email.”

In line with findings from prior work [4], for some participants the process of taking any manual steps (such as generating a key pair in either model) increased their confidence that protection was occurring; for example, RS6 said “extra steps give me a security sense.”

Auditing model We asked participants who heard about the auditing model whether they would use it; overall, it proved popular. Of the 24 participants who were introduced to the auditing model, 15 said they would like to use it. Of these, 10 preferred it to any other model discussed. For example, ES11 said, “It’s best among all systems mentioned in the experiment, because somebody else is policing them, just like watchdogs. If someone is reading your email, they might be caught.” RT8 preferred the auditing model to any other option because “unlike the other models . . . instead of using [the attacker's] public lock blindly, I will get the update, 'Oh, that's the wrong public lock, you should not use this.'"

Four found the auditing model superior to the other registration models, but preferred the exchange model in at least some circumstances. RS10 said he would send personal information including banking data using the auditing model, but "if I worked in a government department, I would still use the exchange model." RT12 said the audit model is "slightly better than [the primary] registration model . . . because in [the primary registration] model I don't know if wrong locks happened. But overall, the lock exchange system has extra steps, extra layers of security, so I like it best among all the systems." Several of these 15 participants noted the possible time lag in notification as an important disadvantage, but were willing to use the model anyway. This generally positive reaction, combined with the preference to split risk among different parties in the CaaS model, suggests that the auditing model has strong potential to meet with user approval.

Eight participants said they would not use the auditing model (one was unsure). One of these (RS11) preferred it to all other models but believed he had no need to encrypt his email, and three found it worse than the exchange model. Four said it was worst among all models discussed, either because they did not trust the auditors or because the time lag was too great.

3.3.4 Participant understanding

Despite receiving only a short introduction to each encryption system, most of our participants demonstrated thoughtful understanding of key concepts for each, suggesting that they provided credible opinions throughout the experiment.

Handling misconfiguration We asked participants to consider how they would handle various possible misconfigurations in each model. Our primary goal was to prompt them to consider usability issues related to longer-term key maintenance, but this section of the interviews also offered a chance to evaluate participants' understanding of the different security models. Most participants were capable of reasoning correctly about these error scenarios.

Participants were presented with five different misconfiguration scenarios across the two models (see Table 3.2). Thirty-nine of 52 participants (75%) responded to all five scenarios with a straightforwardly correct answer, such as asking Alice to resend a lost public key (task 9a, exchange) or generating a new lock-key pair and redistributing the lock to all correspondents (task 9b, exchange). Seven additional participants (13.5%) provided such answers to at least three of the scenarios. One participant (RS13) mentioned recovering keys from a backup (such as a USB drive) rather than generating a new key pair.

We note several interesting misconceptions among those participants who got at least one scenario wrong. Four participants responding to task 9c (accidentally publicizing their own private key, in either model) suggested changing their password within the encryption extension; the password unlocks access to the private key, but a new password would not help if the key has already been exposed. Another participant (RS7) suggested for 9c that "I will send my email to a third person I trust, and ask that person to encrypt the email for me and send to my recipients. Similarly, he will decrypt the [response] email for me and forward it to me." This shows interesting security thinking but misses the potential for the message to be captured during the first step. Other common answers included getting tech support from the company that developed the encryption extension[1] and simply "I don't know."

Overall, participants were largely able to engage with these misconfiguration scenarios, demonstrating working understanding of the encryption tools; remaining misconceptions highlight areas in which more education, clearer directions in the tools, and more frequent use of encryption may be helpful.

Thinking about security Our participants made several thoughtful points about encryption, security, and privacy that apply across models. ES4 mentioned that an extra benefit (of any encryption model) is a reduction in targeted ads: The "email provider can collect data through my emails, and then present ads. . . . I don't want that. [Using this tool] the ads will not appear."

ES10 expressed concern that an email encryption provider (in either model) might collect your private key, especially if you are using Apple email on an Apple

[1] While completely reasonable in practice, this answer does not demonstrate understanding of the encryption model's security properties and so was not counted as "correct" for this purpose.

device or Google email in Chrome, etc. One participant (RS9) was concerned about using public computers. This is potentially a problem for both encryption models, which assume the private key is securely stored on the user's local device. She was also concerned that the act of sending a lock might itself catch the interest of attackers; another participant (RS11) liked the sense of security provided by both encryption models but thought it might seem paranoid to worry about others reading his emails. Similar concerns were raised in GAW et al. [18]. ES12 expressed concern that the centralized nature of the registration model would provide a juicier target for an attacker than many individuals participating in the exchange model. ET10 worried that encryption would bypass an email provider's virus-detection system.

Several (11) participants liked that the exchange model allowed them to explicitly control who would be able to send them encrypted email. ES2 said he would "know the person whom I sent the public locks to," and RT3 liked that "who can send me encrypted emails [is] controlled by myself." RS13 said that "if I communicate with a group of people, it's easy to kick someone out of the group." A similar level of control can be implemented in a registration model; our findings suggest this is a feature at least some users value.

Although many participants understood and reasoned effectively about the security properties we presented, some retained incorrect mental models that have implications for the ongoing design of encryption systems. RS1 incorrectly believed that since he could not understand an encrypted message since it looked completely random, no one else (including his email provider) would be able to either. Others were concerned about keeping their public locks secret in the exchange model; three split their locks across different channels in an effort to be more secure. For example, RS2 sent half of his public lock through the secondary email account and posted the other half on the key server. RT7 thought it would be insecure to store public locks: “After I send my lock to other people, others may not delete my public lock. . . . I may also forget to do so after I import others’ locks. The fewer people know my public lock, the safer.” Relatedly, ES13 worried that in the auditing model, the auditors “are scanning my lock. It sounds like more people are watching me besides the email provider, and I don’t feel good.”

Several participants also had concerns and misconceptions about how keys are managed across multiple devices, regardless of model. System designers may want to provide help or information on these points.

Evaluating tradeoffs In deciding which system(s) they preferred, participants explicitly and deliberately made tradeoffs among their security and usability features. For example, ES13 said he would use the exchange model because “Exchanging locks makes it more private for me,” despite the fact that “it takes time to exchange locks.” ES10 also preferred the exchange model: “Having something better than baseline is one approach. But if I compare to perfect security I am trying to get, it’s another approach. . . . When you want to use it, you really want it to be very well protected.”

On the other hand, RT13, who said he would not use the exchange model, commented that “The negotiating process maybe gives me safer feelings, more protection. But on the other hand . . . the disadvantage is it is time consuming, cumbersome, tedious, more complicated, and this is the price I have to pay for more protection."

RS7 said she would use the primary registration model because it is "easy to use, and I think most of us trust our email provider," although she understood that "there are some possible threats." ET8, in contrast, would not use the primary registration model because "[Although] it's easy to send encrypted emails, especially to many people. But security concern is the reason I don't want to use it." According to ES12, the exchange model "is more straightforward. Only I and the other person [recipient] get involved in the communication, and no others." These comments and others demonstrate that participants understood pros and cons of the different models and thought carefully about how to balance them.

3.4 Conclusion

In this work, we conducted a 52-person lab study to understand how general users balance the usability and security tradeoffs for different key management models in end-to-end encryption. We found that users could understand at least some high-level security properties and could coherently trade these properties off against factors like convenience. We found that while participants recognized that the exchange model could provide better overall privacy, they also recognized its potential for self-defeating mistakes. Similarly, our participants acknowledged potential security problems in the registration model, but found it "good enough" for many everyday purposes, especially when offered the option to audit the system and/or split trust among several parties. Therefore, trying to convince average users to exclusively use more complicated schemes, when they often don't see a need for the added protection, may instead keep them away from using any encryption at all, given that many users already believe encryption is either too much work or unnecessary for their personal communications. Rather than spreading undue alarm about the risks of key-directory based models, or forcing users into only exchange models, we recommend that policymakers and designers present tradeoffs clearly and encourage adoption of usable but imperfect security for the many scenarios where it may be appropriate.

Chapter 4: User Tradeoffs for Search in Encrypted Communication

End-to-end message encryption is the only way to fully protect message privacy. However, searching over end-to-end encrypted messages is complicated. Several popular communication tools (e.g., WhatsApp, iMessage) circumvent this inconvenience by storing the search index locally on the devices. Another approach, called searchable encryption, allows users to search encrypted messages without storing the search index locally. Although popular in academic research, this approach has not been deployed in communication tools. These approaches have inherent tradeoffs between usability and security properties, yet little is known about how general users value these tradeoffs. In this part of work, we systematize these tradeoffs in order to identify key feature differences. We use these differences as the basis for a choice-based conjoint analysis experiment (n=160), in which participants make a series of choices between email services with competing features. The results allow us to quantify the relative importance of each feature. We find that users indicate high importance for increasing privacy and minimizing local storage requirements. While privacy is more important overall, local storage is more important than adding additional marginal privacy after an initial improvement. These results suggest the potential for searchable encryption to fill an important niche in meeting users' communication needs.

4.1 Design Space for Search in Encrypted Communication

In this section we characterize security and usability tradeoffs for searching encrypted communications.

We first consider a **cloud index** (CI), defined as follows. When a new message arrives at the user's device, it is decrypted locally and then tokenized. Using a secret *tokenization key* stored on the local device, these tokens are encrypted, and a mapping between tokens and the associated message identifier is uploaded to the cloud-based search index. To search for messages containing a keyword w, the user's device uses the tokenization key to generate an encrypted token for w and sends it to the server. The server looks this token up in an index and returns all associated message identifiers. This approach is based on searchable encryption techniques such as those described by Stefanov et al. and Bost [27, 28].

We contrast this approach with a **local index** (LI). When a new message arrives, it is decrypted locally, and its contents are added to an unencrypted search index stored on the local device. All queries are handled locally, so no information about the index or queries is provided to the communications service. This is the approach used by WhatsApp and iMessage.

As a basis of comparison, we also include two control approaches: **no end-to-**

end encryption (None) (as in most popular email services today) and **end-to-end encryption without search** (NoSearch) (as in services like Mailvelope [44]).

We do not include ORAM-based [97] schemes, as they are not yet sufficiently practical in terms of performance.

We compare our four chosen approaches on the following metrics:

- Expressiveness: The types of search expressions supported by each solution.
- Performance: The cost of searching and of updating the search index in server storage, client storage, bandwidth consumption, and time.
- Portability: How well each solution can be scaled to multiple devices, including initializing a new device and routinely switching devices.
- Security: Threat models each solution can and cannot defend against.

4.1.1 Expressiveness

In this section, we consider the types of search expressions each approach can support. We surveyed current mainstream email and instant messaging systems, including Gmail, Outlook, Apple Mail, Yahoo Mail, WhatsApp, and iMessage, to create the following list of currently supported and widely used search techniques:

- Exact single word. Users search for one word, and get back messages containing exactly that word.
- Multiple-word boolean. The search expression contains more than one keyword. By default these are typically combined via AND, but OR and NOT

	None	**NoSearch**	**CI**	**LI**
Expressiveness				
Exact single word	✓	—	✓	✓
Multi-word boolean	✓	—	✓	✓
Exact string	✓	—	—	✓
Partial word	✓	—	—	✓
Aux. expressions:				
Sender/recipient	✓	✓	✓	✓
Subject line	✓	—	✓	✓
Date	✓	✓	✓	✓
Label or folder	✓	—	✓	✓
Performance				
Server storage	$\mathcal{O}(N)$	—	$\mathcal{O}(N)$	0
Client storage	0	—	$\mathcal{O}(WlogD)$	$\mathcal{O}(N)$
Bandwidth	$\mathcal{Q}+\mathcal{L}$	—	$\mathcal{Q}+\mathcal{L}+\mathcal{U}$	0
Latency	low	—	low	low

Table 4.1: Supported search expressions and performance for different search approaches. For expressions, ✓indicates that an expression type is supported; expression types that cannot be effectively supported are indicated with "—". We note that current industry products do not necessarily support all types of expressions; this analysis is based on capabilities rather than implemented products. For performance, $\mathcal{Q}$, $\mathcal{L}$ and $\mathcal{U}$ mean the size of query content, returned list of identified items, and update information, respectively.

are also potential options.

- Exact string. A query that returns all messages that contain the exact multi-word string, in order. This is often implemented as a query string enclosed in quotation marks.

- Partial word. The system returns any messages containing words that are superstrings of the provided keyword.

- Auxiliary expressions. These expressions, which are sometimes referred to as advanced search operators, allow the user to specify that specific keyword should be found in a specific field, such as the sender or subject line; to specify a date range within which to search; or to specify a label or folder within which to search.

Our results are summarized in Table 4.1. In the None approach, the service has access to all plaintext messages and therefore can support all types of search expressions. In contrast, in the NoSearch approach the server cannot search over encrypted messages at all, so only searches based on the sender/recipient and the date are available. The date can always be observed by the communications service, and the sender and recipient cannot be easily encrypted if the message is to be correctly delivered.[1] If subjects and labels/folders are also encrypted, they cannot be searched over, although we observe that current tools, such as Mailvelope, do not encrypt subjects and labels/folders and therefore can be searched.

[1] There are some email services that provide identity anonymity, e.g. TorGuard (`https://torguard.net/anonymous-email.php`), but this consideration is out of scope for this paper.

	None	**NoSearch**	**CI**		**LI**	
			Basic	Password	Basic	Password
Portability						
Old_msg	Yes	No	No	Yes	No	Yes
Index	Shared	—	Own	Shared	Own	Inherited
Security						
Keyword	All	None	More	$\mathcal{P}$	Less	$\mathcal{P}$
Message	All	None	More	$\mathcal{P}$	Less	$\mathcal{P}$

Table 4.2: Portability and security for variations of the CI and LI approaches. For portability, the first row concerns whether old messages (from before device activation) can be read and searched on new devices. The second row concerns how indexes are constructed — independently per device ("own"), "shared" across devices, or "inherited" from another device. For security, the extent to which search keywords and messages is indicated (on a relative scale, in order) as "All", "More", "Less", and "None." $\mathcal{P}$ means security depends on the password strength.

In the LI case, all information is obtained from plaintext emails and stored on the local device; as such, all the expressions we consider are supported. The nature of the CI approach inherently allows single keywords and their boolean combinations; however, boolean combinations leak more information about the user's search patterns and therefore their message contents [98]. As the number of keywords involved in these combinations increases, search performance in the CI approach degrades. Recent research measuring email usage patterns, however, suggests that the average number of keywords per email search query is only about 1.5, suggesting that the common case for multi-word boolean searching is reasonable for CI systems. Searchable encryption could support exact multi-word strings by indexing n-grams of various lengths; however, as this would degrade performance even more quickly, and strings of length greater than two or three words would quickly become impractical, we consider it unsupported.

We next consider whether CI can support arbitrary partial keywords. There are some partial solutions, but those proposed in [99–101] did not support updates, and both [102] and [103] adopted ORAM schemes. Some partial keyword search is possible if word stemming (e.g., Porter Stemmer [2]) is applied before message indexing, and the keyword is exactly the anticipated stem. Overall, we consider this unsupported.

As to auxiliary expressions, CI can support sender/recipient and date expressions for the same reasons that NoSearch can, described above. If subject lines and labels/folders are encrypted, they can be tokenized and searched just like message contents, so we say that these expressions are feasible. We distinguish this from the None case, where these items can be either encrypted or searched, but not both.[3]

4.1.2 Performance

We next consider performance metrics with which to evaluate each search solution. In particular, we consider the cloud and local storage space required,

[2] https://tartarus.org/martin/PorterStemmer/

[3] We note that email systems may not be able to create and populate labels or folders automatically because they cannot read email contents.

bandwidth consumption in search and update operations, and latency in search and update operations. The results are summarized in Table 4.1.

The notation used in this section is as follows: N denotes the total number of keyword/message pairs, W is the number of unique keywords, and D is the total number of encrypted messages. We use the performance reported in [28] as a reference example for a searchable encryption scheme, because it provides a good balance between performance and other metrics.

First we consider server and local storage requirements. For NoSearch, there is no index, and for None, the index is stored entirely in the cloud and is approximately proportional to N, adjusted for some data compression. For LI, the index is stored entirely locally, and is again roughly proportional to N, adjusted for data compression. For CI, the situation is more complex. Some local storage is required, roughly proportional to $W \log D$, but the bulk of storage is in the cloud. This storage is proportional to N, but larger than the storage required for None because of encryption-scheme overhead. In the Bost scheme, for example, each keyword/message pair requires 32B of cloud storage [28].

We next consider bandwidth consumed during search queries and updates. Trivially, NoSearch consumes no bandwidth; because LI is purely local it similarly consumes none. None consumes bandwidth equal to submitting the query content and returning the list of identified items. CI operates similarly, but with additional overhead caused by the encryption scheme. CI also requires the client to send update information in order to index a new message. Bost's scheme requires 16B per input token and 32B per output keyword/message pair during search, along with 32B per newly indexed keyword/message pair.

Finally, we consider latency. CI is more time consuming, both in search and in updates, than the LI and None approaches, because it requires additional computation. However, overall the latency performance of such schemes has become very fast. Microbenchmarks reported in [28] demonstrate that searching among 140 million keyword/message pairs, with 10 results returned, requires only 24 μs. This latency will increase as the number of keyword/message pairs — and in particular, the number of unique keywords — increases. Updates, upon receiving and indexing a new encrypted message, can generally occur in the background rather than while the end user is waiting; Bost reports an update throughput of around 4,300 keyword/message pairs per second.

4.1.3 Portability

Previous studies have shown that the number of devices people use to access their email has grown over the past few years [20, 104]. Therefore, it is important to consider how each solution can be scaled to more than one device.

None solutions, of course, are trivially portable. The portability of NoSearch, CI and LI solutions depends primarily on the underlying key management model, as shown in Table 4.2. In the basic model, as adopted by Mailvelope [44], the key pair is generated locally and the key is not shared with other devices. As such, when a new device is added to the ensemble, it does not have access to messages that were not encrypted for the new device's key. For both CI and LI, this means that devices cannot read or search messages from before device activation. Each device requires its own separate encrypted index, and upon activation the new device begins building its index from scratch.

An alternative model applies a password-protected approach to share keys. We refer to this as the *password-protected* variation. This model allows users to decrypt old messages on new devices by retrieving corresponding keys from the cloud, and it has been adopted by several existing products or research prototypes, such as *Confidante* [60], ProtonMail [105], and Threema [106]. For CI, sharing a password-protected key allows new devices to read and search all old messages, and allows different devices to share one index in the cloud. In the password-protected LI, a new device can access old messages and can inherit an existing index and update it as new messages are received.

There may be other portability solutions as well, but we consider these basic and password-protected approaches as exemplars for our analysis.

4.1.4 Security

This section briefly describes the threat model each solution can defend against, as well as its weaknesses. We focus on the ability of service providers (e.g., email companies) to learn their users' message contents and search queries. We do not address interception by third parties or endpoint compromise, as these are for the most part orthogonal to the implementation of search. We assume a semi-honest scenario, where the provider is curious but does not deviate from protocols.

We first consider our two controls, None and NoSearch. In None solutions, since all messages are in plaintext, the provider will learn all message contents as well as all of a user's search queries. This is how most email services currently work (e.g., Gmail [107]). We regard this solution as the lower bound for security. In NoSearch solutions, only the user can read messages sent to her, and all other parties, including the provider, cannot. There are no search queries, so the provider cannot learn them. We consider this solution the upper bound for security in our evaluation.

Table 4.2 shows some security features for CI and LI. Many different CI solutions provide more security than None, but less than NoSearch. Generally, the content of search queries is concealed but the search pattern, access pattern, and size pattern are revealed to the provider (for detailed definitions, we refer readers to [24]). Further, many proposed CI approaches achieve forward privacy, meaning that when a user searches for a keyword, if a later message containing the same keyword is added, the server cannot connect it to the prior search.

In the past few years, researchers have investigated how to exploit the information leaked by these schemes. CI solutions built from Bloom filters (e.g., [108, 109]) are potentially vulnerable to message recovery via leaked information [110]. There are also many proposed attacks for recovering search keywords, the details of which differ based on assumptions about the providers' abilities as well as about the composition and distribution of messages and search keywords. For example, providers who can send encrypted messages to the client, potentially from a spoofed address, can learn whether a user is searching within a set of candidate keywords [111].

For LI solutions, leaked information is minimal, as all searches are performed locally. However, eliminating leakage entirely has been proven impossible [112]; for example, the provider may observe patterns in which old messages are requested from the server (presumably after a local search has completed). Overall, we consider LI to be stronger than CI but not precisely as secure as NoSearch.

If we consider the special case of password-protected key and/or index material discussed in Section 4.1.3 above, the security of both CI and LI reduces to the strength of the user's password.

4.2 Email Preference Study

In the previous section, we identified several key tradeoffs related to search in encrypted communication systems. Choosing among these tradeoffs, however, requires understanding how users balance and prioritize different features. As a first step toward understanding this, we conducted a *choice-based conjoint analysis* study focused on email. In conjoint analysis, participants are presented with a set of product *profiles* that vary in several dimensions. By choosing among them, participants reveal their relative preferences among the various features [113, 114]. In this study, we asked participants to choose among email services with different features drawn from the tradeoff analysis presented in Section 4.1. In this section, we describe the features we selected, then detail the design of our study and our analysis approach.

4.2.1 Features and options

Features	**Feature Descriptions**	**Options**
Price	Monthly fee for signing up for the service	**$0.00 (free)** **$1.99 per month**
Multi-word Email Search	When you search emails, can you search using multiple words, for example, "home depot"?	**Yes** **No**
Partial-word Email Search	When you search emails, can you search with a partial word instead of a complete word, e.g., "amaz" vs "amazon"	**Yes** **No**
Storage on your device	How much local storage the service will use (on your computer or phone)	**Will use 5MB on your device**, equivalent to about 2-3 HD photos **Will use 500MB on your device**, equivalent to about 200 HD photos or 20 mobile apps
Syncing old email to a new device	After using the email service on one device (a phone or laptop) for several months, you buy a new device. You set up the email service on your new device. Can you read and search old emails on your new device?	**Yes – read and search all email** using the new device both before and after its activation. **No – read and search only email** after you configured the new device. You can't read and search old emails on your new device.
Privacy	What can your email service learn about your email and email search queries?	**Standard privacy**: Your email service can access the contents of all email and email search queries. This is how most email services currently work (Gmail, Yahoo! mail, Outlook, etc.) **Extra privacy**: Your email service can access the contents of certain emails and email search queries, but not all. The service can choose specific topics of high interest to learn about. **Maximum privacy**: Your email service cannot access the contents of any emails or email search queries.

Table 4.3: Features and options used in our conjoint analysis experiment. We selected six features, with two to three possible options for each.

For the rest of the paper, we define *feature* as a general property of a choice profile — for example, price or security posture — and we define *option* as one of various settings a given feature can take. For example, the price feature has options of $0.00 and $1.99.

Based on the tradeoffs identified in Section 4.1, we identified six features to examine: price, multi-word email search, partial-word email search, local (device) storage, portability of old messages to a new device, and privacy. Each feature has two or three possible options. All features and options are listed in Table 4.3.

The first feature we include is price; this is included because it is familiar to participants when thinking about value tradeoffs, and because it allows us to express the resulting valuations for different features in dollars. We chose to use a monthly fee to make the price a bit more meaningful for users on an ongoing basis. To set the price, we searched "secure email" in both Apple Store and Google Play, and looked at the top 50 returned apps; more than 90% were priced at \$1.99 or lower, and the majority are free. Therefore, we set two options for the price feature: \$0.00 and \$1.99. We note that setting the best possible price is not critical, as our main goal is to choose something differentiable enough to matter to users, but not so expensive that it overwhelms other features.

We chose two expressiveness features: multi-word search and partial-word search. These features are used relatively often for email search [22, 80], and they vary between the two main search solutions we consider. (For simplicity, we presented users with only "multi-word search" and did not differentiate between boolean and exact string matching.) We do not include single keyword, or auxiliary expressions that consider the sender/receiver or date, as they are supported by both LI and CI. More complex auxiliary expressions are also rarely used [21]. In the conjoint analysis, each expressiveness feature has two options: "yes" (available) or "no" (unavailable).

As discussed in Section 4.1.2, the most notable performance difference among approaches we consider is related to storage on the local device. The storage required, of course, depends on how many keyword-email pairs a particular user generates, and will increase over time as more messages are added. For simplicity, however, we set two possible options for the storage feature: 5MB of local storage (low storage) and 500MB of local storage (high storage). The 5MB figure represents CI and is adapted from Bost, reflecting 14 million keyword-message pairs and 213,349 unique keywords [28]. The 500MB figure is intended to represent LI and was selected as a round number roughly in line with the cloud storage requirements for the same Bost scenario (because for LI, all index data is stored locally instead of in the cloud). To make this size difference more intuitive for participants, we also describe the storage requirements in terms of the equivalent number of HD photos or apps.

For the portability feature, we selected the ability to work with old emails on new devices. This feature distinguishes the basic CI and LI approaches from their password-protected variations, and is relatively easy to explain. We describe this feature to participants as follows: "After using the email service on one device (a phone or laptop) for several months, you buy a new device. You set up the email service on your new device. Can you read and search old emails on your new device?" The possible options are "yes" and "no."

The final feature we consider is privacy. For ease of explanation to users, we describe the privacy feature as the ability of the email provider to access users' email contents and email search queries. Although the actual security properties of various searchable encryption schemes have subtle differences, for our users we simplify this feature into three options: *standard* privacy, *extra* privacy, and *maximum* privacy. Standard privacy describes a scenario with no end-to-end encryption, as is common in most email services today. (We found in pilot testing that summarizing this option as "low" or "no" privacy unduly alarmed users, so we chose standard to reflect the current common case.) The extra privacy option was described as allowing the provider to access "some but not all" message contents and search queries, with the provider having some choice of topics to learn about. This category was designed to approximate CI solutions. Lastly, maximum privacy was described as the provider being unable to learn any email or search querty contents. This option was designed to represent NoSearch as well as LI.

By asking users to choose among various combinations of these feature options, we can determine the relative value of each feature compared to the rest.

4.2.2 Study setup: Choice-based analysis

The feature set described in the previous section totals six features, with up to 96 ($2 \times 2 \times 2 \times 3 \times 2 \times 2$) possible option combinations for a single profile. In a traditional full-factorial, full-profile conjoint analysis, participants would be asked to rank all 96 of these possible profiles; clearly this is an untenable cognitive burden [114]. To address this, we elect to use a choice-based analysis, in which participants make a series of discrete choices between two profiles, rather than ranking a large set of profiles [115]. We also reduce the set of profiles we examine by using a fractional-factorial design that consists of a smaller number of orthogonal profiles [116]. Prior work has found that participants can handle as many as 17 choice sets without problems [117]. We therefore construct a set of 16 distinct choice pairs.

To choose the 16 distinct choice pairs, we generally follow the randomized approach suggested in [118]. A screenshot of a single choice pair is shown in Figure 4.1, and the screenshots of all 16 questions used in our study are shown in the appendix.

It is common in conjoint analysis to provide a “no choice” option, indicating that the participant will choose neither of the presented profiles. In this case, however, we are primarily interested in learning the relative value of the different features, so “no choice” options (indicating that a participant would prefer to keep her existing email service) are somewhat unhelpful. We instead provide a “no preference” option to allow a participant to indicate that the two choices are (to her) equivalent.

4.2.3 Protocol and recruitment

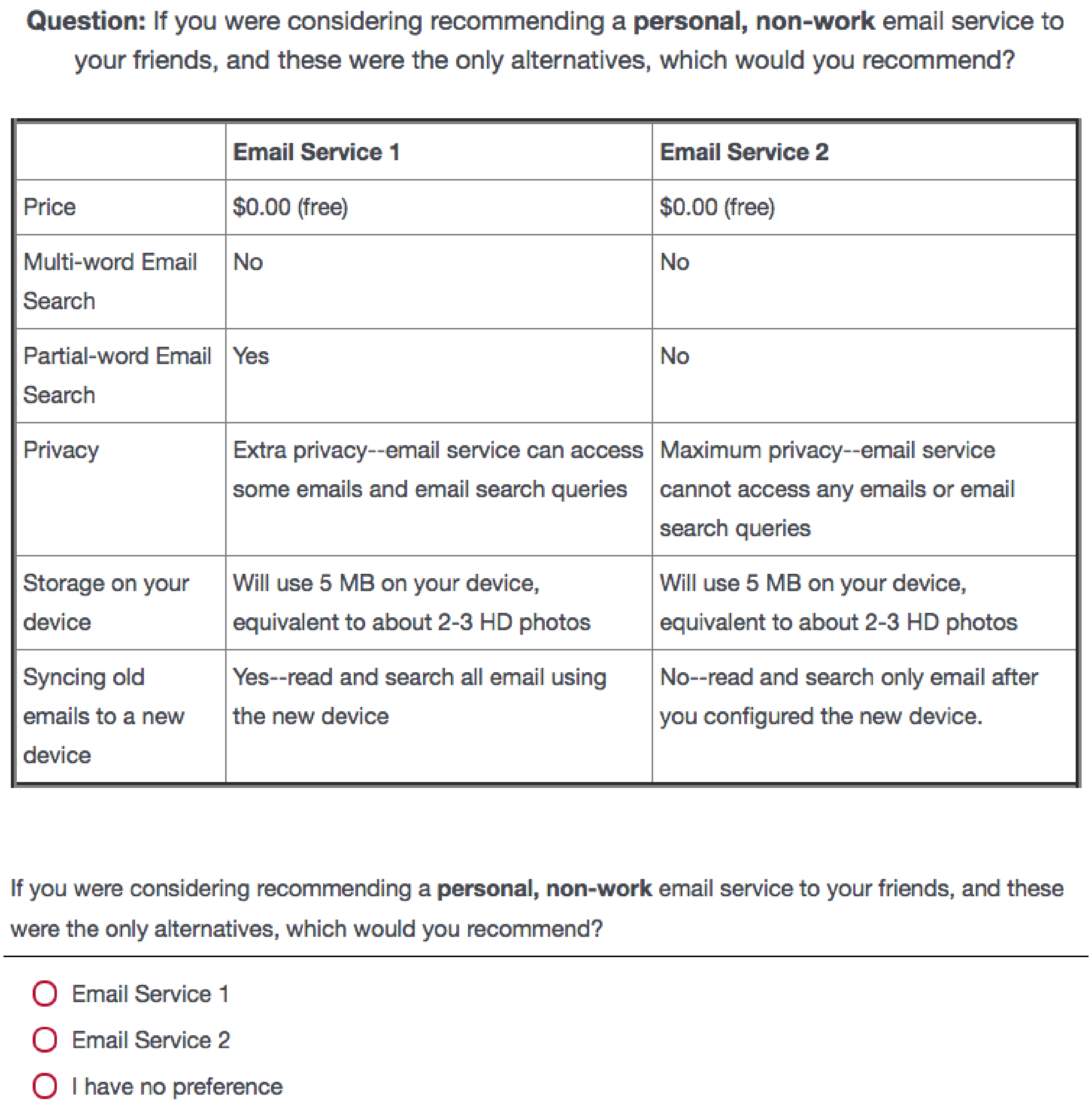
We recruited participants from Amazon’s Mechanical Turk crowdsourcing service [119] who are 18 or older and fluent in English. To improve data quality, we required participants to have completed at least 50 prior Human Intelligence Tasks (HITs) with a HIT approval rating over 95% [120]. Because perceptions of dollar value and privacy preferences are likely to vary across countries, we restrict recruitment to Turkers in the United States. We advertised our task as asking participants’ preferences about email services, and explicitly did not mention privacy to avoid self-selection bias. We prevented duplicate participation based on MTurk ID. Participants were paid $1.50 for the study, which was expected to take less than 15 minutes. On average, it took participants around 12 minutes to finish our questionnaire.

Study participants first received general instructions explaining that they would be required to answer questions about recommending a new email service to a friend. These instructions included the overall feature table (Table 4.3). To encourage participants to read these instructions carefully, we enforced a six-second delay before the participant could advance to the next screen. We also required participants to check a box agreeing that they would "read the instructions and each question carefully and think about your answer before you give it. We rely on our respondents being thoughtful and taking this task seriously."

The participant was then shown the choice-pair questions, one at a time, as shown in Figure 4.1. We presented the overall feature table above each question for the participant's ongoing reference.

After the choice-pair questions, we asked participants to answer knowledge, attitude, and demographic questions. These included the six-item abbreviated web-use skills index [121], which measures web-based tech savviness; the 10-item Internet Users' Information Privacy Concerns (IUIPC) [122], which measures consumer privacy concern; and standard questions about gender, age, ethnicity, education, and income. Several privacy concern scales have been developed, each of which has various benefits and drawbacks; the IUIPC is recommended by Preibusch in his survey [123].

Our study protocol was approved by the University of Maryland Institutional Review Board (IRB).



Question: If you were considering recommending a **personal, non-work** email service to your friends, and these were the only alternatives, which would you recommend?

	Email Service 1	**Email Service 2**
Price	$0.00 (free)	$0.00 (free)
Multi-word Email Search	No	No
Partial-word Email Search	Yes	No
Privacy	Extra privacy--email service can access some emails and email search queries	Maximum privacy--email service cannot access any emails or email search queries
Storage on your device	Will use 5 MB on your device, equivalent to about 2-3 HD photos	Will use 5 MB on your device, equivalent to about 2-3 HD photos
Syncing old emails to a new device	Yes--read and search all email using the new device	No--read and search only email after you configured the new device.

If you were considering recommending a **personal, non-work** email service to your friends, and these were the only alternatives, which would you recommend?

○ Email Service 1

○ Email Service 2

○ I have no preference

Figure 4.1: Screenshot of a choice question example

4.2.4 Data analysis

We used Hierarchical Bayesian (HB) models to analyze choice-based conjoint data. Compared with other statistical analysis methods, HB models are able to estimate participants' preferences not only at the aggregate level (i.e. general preferences from participants), but also at the individual level [124]. We applied the R package "bayesm" [125] to conduct this HB analysis.

In our HB analysis, we used *effects coding* method for categorical coding of feature options [126]. In effects coding, one option of each feature is chosen as the *baseline*, to which other options are compared. In our analysis, we selected the least desirable option for each feature ($1.99, no multi-word search, no partial-word search, standard privacy, 500MB local storage occupied, and no sync ability) as baselines.

After our conjoint analysis, we applied linear regression to estimate the effects of participants' web-use skill scores and three IUIPC scores (collection, awareness, and control) on their marginal valuation of privacy at different levels. In order to prevent possibly over-fitting models, we applied the standard backward-elimination model selection process, until the Akaike Information Criterion (AIC) is minimized [127]. For each regression model, we present what variables are selected, estimated coefficients, and p-values.

4.2.5 Limitations

Our study has several limitations. Amazon MTurkers are younger, better educated and more technical than the general U.S. population [128], which may limit the generalizability of our results. Our participants, though, (as detailed in Section 5.2.1) showed similar online privacy concerns to the IUIPC scores reported in [122].

Participants' self-reported preferences don't always match their revealed preferences [129, 130]. This means that overall, we expect privacy to be overvalued a bit in our results. However, requiring participants to make explicit tradeoffs (rather than simply asking about whether privacy is important) may mitigate this somewhat. We asked participants to recommend email services to their friends instead of using themselves, to make questions more neutral and less personally fraught. Although participants' recommendations may not always align with choices of their own use, this is a known technique for surveying about sensitive topics [131] and has been used when investigating app permissions [132]. Overall, we believe our results can provide a meaningful jumping-off point for understanding how users value tradeoffs between security and usability features in searchable encrypted messaging tools, but further work is needed to examine revealed preferences.

To avoid overwhelming our participants, or requiring them to understand complex technical distinctions, we presented participants with only three coarse levels of available security. In reality, various searchable encryption solutions have subtly but meaningfully different security guarantees [76], and these subtleties are not captured in our results. Future work can examine these alternatives in more detail.

More generally, we asked participants to make nuanced decisions that required reading and thinking about multiple features and option levels. Some participants may have answered carelessly, or used satisficing rather than thinking deeply about each option [133]. To mitigate this, we restricted MTurk recruitment (as described above), we kept the study short, and we iteratively tested our feature descriptions to make them as clear as possible.

4.3 Results

In this section, we present the demographics of our participants, their preferences among features and options, and the correlation between their privacy preferences and their online privacy concerns and web skills.

4.3.1 Participants

In May 2017, we collected 160 completed questionnaires. Self-reported demographics for the those 160 participants are shown in [134], which shows that 51.3% of our participants were male, 41.0% were in the age range of 30-39, 80.1% were Caucasian, and 43.6% held a bachelor's degree. In addition, 78% participants held neither a degree nor a job in an IT-related field, and 30% reported household income in the $50k-$75k range in 2016.

We also measured participants' web knowledge and online privacy concerns using two extensively validated scales. To assess web knowledge and skills, we adopt the six-item web-use skills index for the general population, developed by Hargittai et al. [121], which measures web skills on a Likert scale from 1 (low) to 5 (high). Our participants reported an average score of 4.2 (SD = 0.80). This is higher than the 3.4 average reported by Hargittai et al., which we attribute to MTurkers having higher than average internet skills and to population changes since the Hargittai data was collected in 2010.

To measure internet privacy concern, we adopt the 10-item IUIPC scale developed by Malhotra et al. [122]. There are several available scales for measuring privacy, each of which has known weaknesses; the IUIPC scale that we use is recommended by Preibusch as “a safe bet,” but should be interpreted carefully [123]. On a seven-point scale, with seven indicating highest privacy concern, our participants averaged 5.9 (SD=0.81) for consumer control, 6.3 (SD=0.66) for awareness of privacy practices, and 5.61 (SD=1.07) for data collection. These results are comparable to those Malhotra et al. reported: 5.7, 6.2, and 5.6 respectively.

4.3.2 Results for conjoint analysis

We present participants' preferences for different features and their options in this section. We follow the analysis procedures of Burda et al. [34]. We first calculated the individual and aggregated part-worth utilities for each option. Based on those utilities, we then estimate the relative importance of each feature, the utility changes between feature options and the corresponding monetary values in terms of dollars.

Features	**Options**	**Part-worth Utility**	**Part-worth Utility CI**	**Relative Importance**
Price	$0.00 (free)	1.856	[1.851, 1.860]	32.59%
	$1.99 per month	-1.856	[-1.860, -1.851]	
Privacy	Maximum privacy	1.219	[1.215, 1.223]	24.19%
	Extra privacy	0.190	[0.188, 0.192]	
	Standard privacy	-1.409	[-1.413, -1.405]	
Local Storage	5 MB	0.635	[0.630, 0.639]	17.38%
	500 MB	-0.635	[-0.639, -0.630]	
Sync old email to a new device	Yes	0.410	[0.409, 0.411]	9.36%
	No	-0.410	[-0.411, -0.409]	
Multi-word Search	Yes	0.460	[0.458, 0.463]	9.02%
	No	-0.460	[-0.463, -0.458]	
Partial-word Search	Yes	0.392	[0.391, 0.394]	7.46%
	No	-0.392	[-0.394, -0.391]	

Table 4.4: Part-worth utilities of feature options and feature relative importance. CI stands for "95% confidence interval".

4.3.2.1 Model fitting

First, we evaluate how well our estimated HB model is fit. In order to evaluate this goodness-of-fit, we conducted the test suggested in [135]. We calculated the *likelihood ratio* (LR) to measure how well our estimated model performs compared

Features	**Option** **Change**	**Utility** **Change**	**Utility** **Change CI**	**Dollar** **Value**	**Dollar** **Value CI**
Price	1.99 → 0.00	3.711			
Privacy	Standard → Extra	1.599	[1.438, 1.760]	0.86	[-0.05, 1.77]
	Extra → Maximum	1.029	[0.874, 1.185]	0.55	[-0.05, 1.16]
	Standard → Maximum	2.628	[2.351, 2.905]	1.41	[-0.01, 2.83]
Local Storage	500 MB → 5 MB	1.269	[0.928, 1.611]	0.68	[-1.12, 2.48]
Sync old email to a new device	No → Yes	0.819	[0.669, 0.970]	0.44	[-1.40, 2.29]
Multi-word Search	No → Yes	0.921	[0.781, 1.060]	0.49	[-0.21, 1.20]
Partial-word Search	No → Yes	0.785	[0.682, 0.888]	0.42	[-0.03, 0.87]

Table 4.5: Utility change in feature options and monetary values. CI indicates "95% confidence interval".

with a dummy model in which all parameters are zero [135]. This test shows that our estimated model is statistically valid with LR = 25.89 (p=0.001). In other words, the hypothesis that our estimated model and the null model are equal can be rejected. Second, we calculated the hit rate in our 16 choice questions by identifying for each participant the *profile* with the highest probability based on the estimated model, and then determining whether or not that participant actually chose this *profile*. The test results in a hit rate of 89.84%, compared to 33% random guessing, suggesting that our model is well-fitted.

	\$0	**Multi**	**Partial**	**Extra**	**Max**	**5MB**	**Sync**
\$0	1.00	-0.13	-0.04	0.03	0.18	-0.13	-0.07
Multi		1.00	0.05	0.03	-0.01	-0.10	0.06
Partial			1.00	0.35	-0.09	-0.07	0.12
Extra				1.00	0.03	-0.02	0.07
Max					1.00	-0.13	0.06
5MB						1.00	0.04
Sync							1.00

Table 4.6: Correlation matrix of non-omitted options in HB analysis. Notes: “multi” means multi-word search supportive; “partial” means partial-word search supportive; “extra” and “max” mean extra and maximum privacy, respectively; “5MB” means 5MB local storage needed; “sync” means synchronizing supportive.

4.3.2.2 Interpreting the model

The outcomes of Hierarchical Bayesian (HB) models are called *part-worth utilities*. Part-worth utilities are a unitless measure of the relative value of different options within each feature. We use the *effects coding* method for quantifying feature options [126]; as such, for each feature, the part-worth utilities will sum to 0, with the least-desirable option showing a negative part-worth utility. Part-worth utilities are calculated independently for each participant, then averaged to produce an overall result.

More formally, the probability of participant n choosing email service profile

j in question k is shown in Equation 4.1. X_{kj} is a (1×8) vector, representing the coding for "no preference," "$0," "multi-word search," "partial-word search," "extra privacy," "maximum privacy," "5MB local storage" and "sync ability" for email service j in question k. β is the vector for part-worth utilities. The coding for "no preference" is 1 when "no preference" option is chosen by a participant, and 0 otherwise. We included this additional factor in order to get better model fitting and parameter estimation [136].

$$P_{nkj} = \frac{exp\,(X_{kj}\beta)}{\sum_{i=1}^{J} exp(X_{ki}\beta)} \tag{4.1}$$

Because part-worth values are scaled arbitrarily, the values themselves cannot be directly compared across features; instead, only the difference in utility in changing from one option to another can be compared. For example, Table 4.4 shows that extra privacy has a part-worth utility of 0.190, while enabling partial-word search has a part-worth utility of 0.392. This cannot be interpreted directly to mean that extra privacy is of higher value than partial-word search. Instead, we see in Table 4.5 that the utility increase for enabling partial-word search is 0.785, while the increase from standard to extra privacy is 1.599. This means that when comparing these two option upgrades, the added privacy is more valuable.

For each part-worth utility, we also report a 95% confidence interval. The confidence interval helps to establish, with statistical confidence, the strength of apparent differences between features and options.

To more easily compare features, we use part-worth utilities to calculate the *relative importance* of each feature. Relative importance is defined as the ratio of the utility range for one feature to the sum of utility ranges across all features. Thus, relative importance (typically reported as a percentage) indicates how much a given feature contributes to a user's overall decision-making. In reporting aggregated relative importance, we calculate and then average the relative importance for all participants, rather than computing importance from average utilities.

Finally, to ease interpretation of the results, we calculate each utility change in terms of dollars. To do this, we divide the utility change from $1.99 to free by the price difference (trivially, $1.99); this yields the amount of utility change that is equivalent to $1.99 per month. We then scale the utility changes for other features accordingly.

4.3.2.3 Estimated user preferences

Table 4.4 presents the aggregated part-worth utilities and relative importance for each feature. Considering each feature independently, our results show the expected relations: participants prefer the options that are inherently "better" (such as free rather than paid, and more privacy rather than less). This serves as an additional face validation of our results.

We find that with a relative importance of 32.6%, price is on average the most important factor influencing participants' choice of an email service. Privacy, at 24.2%, is second. Overall, participants were willing to pay $0.86 per month to upgrade from standard to extra privacy, plus an additional $0.55 to upgrade to maximum privacy. This indicates that the marginal value of privacy, as with many goods, is decreasing: our participants seem to believe that once some privacy improvement is made, further increases are less valuable. Finding that participants value privacy relatively cheaply aligns well with previous work [137, 138].

The third most important factor, after price and privacy, is local storage, with a relative importance of 17.4%. From Table 4.5, we see that reducing local storage from 500 to 5 MB is worth about $0.68 per month. This is lower than, but somewhat comparable to, the $0.86 value of a privacy upgrade from standard to extra, and higher than the value of an upgrade from extra to maximum privacy. This suggests that to our participants, local storage is almost as important as privacy improvements, likely because emails are increasingly sent and received on mobile devices that have relatively limited storage.

The remaining features — synchronization, multi-word search, and partial-word search — each have a relative importance under 10%, with dollar values of $0.50 or less. These values are somewhat comparable to the value of upgrading from extra to maximum privacy in our taxonomy. Further, upgrading any two of these three features is as or more valuable than increasing from standard to extra privacy. Overall, then, while our participants value privacy more than these other features, the added value is limited.

It is perhaps somewhat surprising that synchronization is rated with such low importance, given that emails are increasingly accessed on multiple devices; however, Cecchinato et al. report that email is managed differently on different devices, and in many cases separate devices manage different accounts [20]. They further report that searching email occurs primarily on laptops and PCs rather than on smartphones. This may help to explain the relatively low value placed on synchronization in our results.

The relative unimportance of complex search capabilities also aligns well with prior work. For example, a recent large-scale study found that the majority of search queries contain only one word [22]. Earlier work reported the existence of "many" partial-word queries [80], but we find no other evidence that they are frequently used. Several large webmail services (e.g., Gmail) support partial-word searches only in limited contexts, so it may be that users have not developed the habit of depending on this feature.

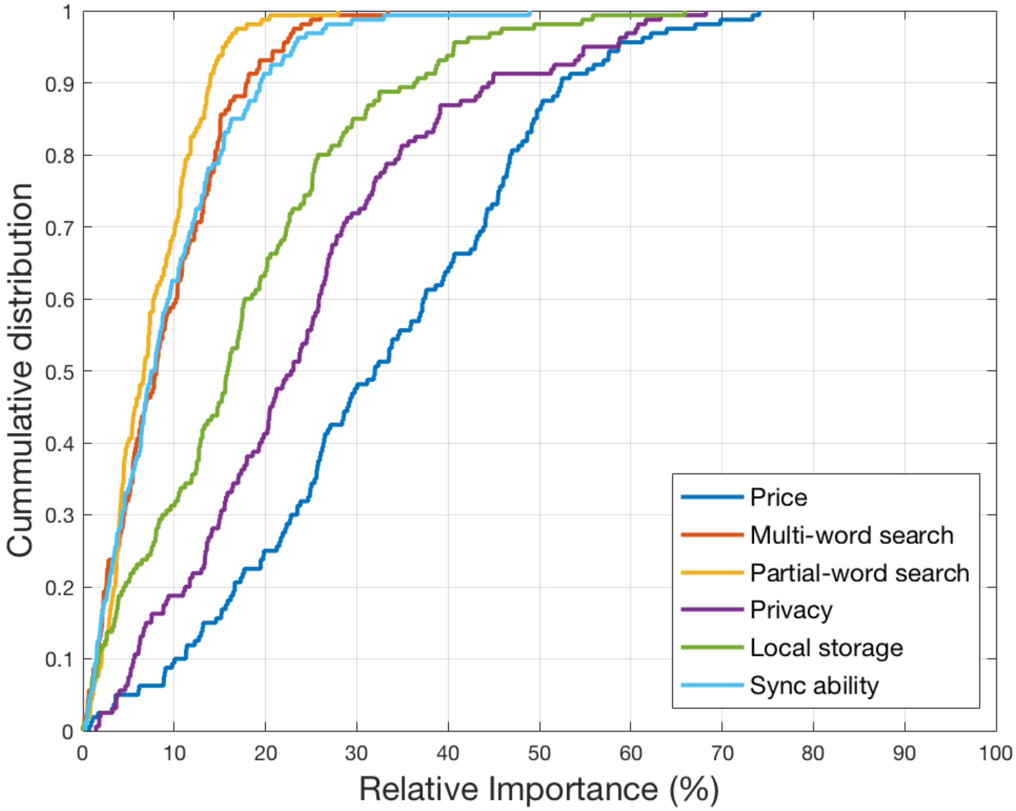


Figure 4.2: Cumulative distribution of all participants' relative importance for each feature.

4.3.2.4 Variation across participants

We next investigate in more detail how perceived relative importance for each feature varied among all participants. In Figure 4.2, we present the cumulative distribution of all participants' perceived relative importance for each feature. This figure shows that, as discussed above, price is overall most important, followed by privacy and then local storage, while the lowest-importance three features cluster closely together. Price, privacy, and local storage also show more diversity of importance; the largest preferences reach over 60-70%, while the smallest are very close to 0. On the contrary, participants have more consensus on the lower perceived relative importance of multi-word search, partial-word search and synchronization.

4.3.2.5 Correlation among features

Finally, we consider whether any of the features we tested are strongly correlated: that is, whether any of them are strongly preferred together, or are treated as mutually exclusive. We show the correlation matrix of non-baseline variables in the Hierarchical Baysian analysis in Table 4.6. Most of the off-diagonal elements in the table are fairly close to 0, which implies that there are no two particular features are strongly preferred together or mutually exclusive by participants. The largest correlation is partial-word search ability with standard privacy (0.35). This positive coefficient suggests an association between valuing partial-word search more and valuing privacy less.

4.3.3 Why do web skills and reported privacy concern matter?

Model	Factors	Coef.	St. Dev.	p-value
Std. to Extra	Collection	0.288	0.073	<0.001*
Std. to Max	Web	0.357	0.177	0.045*
	Collection	0.341	0.147	0.022*
	Awareness	0.508	0.297	0.0887
	Control	-0.493	0.232	0.035*

Table 4.7: Regression results for utility changes in privacy options. We separately model change from standard to extra and from standard to maximum privacy (R^2 = 0.083 and 0.075 respectively). These results indicate the final model chosen via backward selection. Statistically significant factors with p<0.05 are marked as *.

We next consider how participants' internet skills and generic privacy concerns affect their preferences for privacy within the email choices we present. To do this, we apply linear regression to model observed utility change as a function of a participant's scores on the web skills index as well as the three subscales of the IUIPC. We model change from standard to extra privacy, and then separately change from standard to maximum privacy.

To prevent possibly over-fitting our models, we applied the standard backward-elimination model selection process, until the Akaike Information Criterion (AIC) is minimized [127]. Our final regression results are shown in Table 4.7: we present which variables are selected, estimated coefficients and their standard deviations, and p-values.

The first model includes as a factor only the IUIPC Collection subscale. Malhotra et al. define Collection as degree of concern about "the amount of individual-specific data possessed by others relative to the value of benefits received" [122]. This model indicates that on average, for each one-point increase in concern as measured on this Likert subscale, participants value upgrading from standard to extra privacy an additional 0.288 of utility. This increase is significant.

The second model includes all the examined factors. The results indicate that greater web skills, as well as a higher Collection score, are significantly correlated with an increase in the utility of upgrading from standard to maximum privacy. On the other hand, participants with high scores on IUIPC Control — that is, a stronger belief that privacy is primarily a function of consumer control — place significantly lower value on upgrading from standard to maximum privacy. (The IUIPC Awareness score was not significantly correlated.)

Overall, these results suggest that people who are more tech-savvy, and who are more concerned about data collection, value privacy more highly; on the other hand, those who believe in the importance of individual control over data do not value it as strongly. We hypothesize that perhaps this is because the privacy options we offered to not exhibit individual fine-grained control, but rather allow the email service to observe information, or not.

4.4 Conclusion

In this study, we explored general users' tradeoffs for search in encrypted communications. We found that privacy was the most important non-price feature to our participants, and minimizing the use of local storage was almost as highly valued. These findings suggested that in the email context, although local indexing may largely be suitable, there might also be a niche for searchable encryption. For some users, the potential reduction in privacy relative to a local index will be worthwhile, in order to save on storage space. In particular, searchable encryption may have potential as a compromise: more privacy than the current standard, in which email services have plaintext access to all messages, while limiting some inconveniences that may prevent broader adoption of end-to-end encryption.

Chapter 5: Improving Non-Experts' Understanding of End-to-End Encryption

In recent years, several popular messaging apps have adopted end-to-end encryption, either by default [9, 139] or as an optional feature [140, 141]. As a result, E2EE is now readily available to millions of users. However, prior research indicates that general users have difficulty using end-to-end encrypted tools correctly and confidently, as well as recognizing their security benefits, in part because of incorrect mental models. We believe that enabling users to make appropriate decisions about how to meet their privacy needs may require at least somewhat improving mental models, perhaps via better explanations. In this chapter, we take an initial step toward providing high-level, roughly correct information about end-to-end encryption to non-experts. In a 25-people lab study, participants were shown one of several variations on a short tutorial. Participants were asked about their understanding of end-to-end encryption before and after the tutorial, as well as which information they found most useful and surprising. Overall, participants effectively learned many benefits and limitations of end-to-end encryption; however, some concerns and misconceptions still remained, and our participants even developed new ones. The results provided insight into how to structure new educational materials for end-to-end encryption.

5.1 Study Methodology

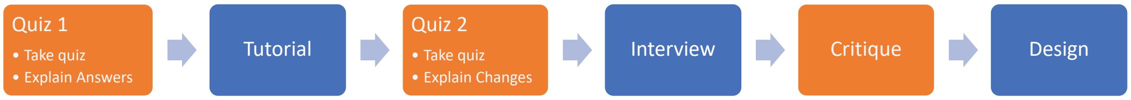


Figure 5.1: Study Procedure Flow Chart

We designed an in-person study to explore the process of explaining E2EE to non-experts from several different angles. Participants spent on average 63 minutes to complete the study.

5.1.1 Study procedure

We designed a primarily qualitative, between-subjects study to investigate how participants' understanding and perceptions could be influenced by introducing different aspects of E2EE. Each participant was shown a tutorial, which presented one or several aspects of E2EE. Before and after reading the tutorial, participants were asked to answer a set of quiz questions regarding their perceptions of E2EE, and then interviewed about why they selected their answers. We next asked them to comment on our tutorial, to critique some existing E2EE explanations from real apps, and to design a short message introducing E2EE in their own words. Figure 5.1 outlines our study procedure.

5.1.1.1 Initial quiz

After agreeing to our consent form, participants first completed a closed-item quiz printed on paper to assess their understanding of E2EE. In the quiz, participants were asked to imagine using a hypothetical E2EE messaging app, Textlight, to send a message to their friend Bob. We chose to use a fictional app so that answers would not reflect participants' impressions of existing companies or brands.

The questions explored participants' understanding of security properties of E2EE. To address confidentiality, we asked how difficult it would be for various adversaries to read the content of the message, including: hackers who could intercept communications, hackers who could infiltrate the app company, hackers who had previously installed malware on users' phones, ISPs, and government agencies. We also included two questions addressing integrity and authenticity, asking how difficult it would be for a third party to modify a message or send a response impersonating the recipient. All these questions included five possible answers on a scale from "very easy" to "very difficult." Finally, we asked about the relative security of different communications tools, including SMS text messaging, mobile phone calls, email, and instant messaging apps with and without E2EE. After they completed the quiz, we asked participants to explain their reasoning for each answer. The quiz questions are listed in Appendix C.1.

5.1.1.2 Tutorial and second quiz

We then presented to participants one of several variations of a tutorial we designed (details below), consisting of narration and accompanying PowerPoint slides. After the tutorial, participants completed the same quiz questions again and were asked to explain why they had (not) changed their answers. We deliberately conducted this second quiz before any further study tasks, so that answer changes would reflect the effect of the tutorial and not priming from other questions.

5.1.1.3 Tutorial feedback

We next asked participants to evaluate our tutorial, including how difficult it was to understand, how informative it was, and which parts they (dis)liked. We further asked participants to select the most and least surprising and important information from the tutorial, as well as the part of the tutorial they would most want their friends and family to learn about. Our goal with these questions was both to learn what did and did not work about our tutorial specifically, and also to learn which concepts to prioritize for educational interventions (such as short messages integrated into messaging tools).

5.1.1.4 Critique

Next, participants were shown two short texts (from six options) introducing E2EE. The six texts were taken from app descriptions, official websites, and/or whitepapers of existing secure communication tools, including LINE, WhatsApp, Telegram, Viber, Threema, and ProtonMail. Each participant was presented only two to avoid fatigue. We showed each message almost the same number of times and balanced them across different tutorial conditions. To avoid branding effects, in the texts we replaced the actual names of all six apps with Textlight (a fake app we made up for this purpose). Throughout this chapter, we labeled these six messages for convenience, which is shown in Table 5.1. Below is the example drawn from WhatsApp (Msg2); the other messages are provided in Appendix C.3.

Message ID	Msg1	Msg2	Msg3	Msg4	Msg5	Msg6
Tool Names	LINE	WhatsApp	Telegram	Viber	Threema	ProtonMail

Table 5.1: Critique messages for communication tools.

> Many messaging apps only encrypt messages between you and them, but TextLight's end-to-end encryption ensures only you and the person you're communicating with can read what is sent, and nobody in between, not even TextLight. This is because your messages are secured with a lock, and only the recipient and you have the special key needed to unlock and read them. For added protection, every message you send has its own unique lock and key. All of this happens automatically: no need to turn on settings or set up special secret chats to secure your messages.

We asked participants to give their general opinions about both messages, mark phrases or sentences that explained E2EE clearly (or not), describe what else they might like these messages to tell them, and choose which message they preferred. This task had three goals: (a) to gain explicit insight into participants' perceptions of existing short educational messages; (b) to indirectly observe what they had retained from the tutorial and/or any remaining misconceptions, as revealed by their reactions to the messages, and (c) to provide some setup for the subsequent design task.

5.1.1.5 Design

Finally, participants were given a design task: "Could you design a short introduction as if you want to teach other people about end-to-end encryption? We don't expect you to come up with a long document describing every aspect of E2EE. Instead, please pick the most important pieces you want to convey. Try to come up with the introduction within 200 words." Like the Critique task, this task had multiple concurrent goals: to gain insight into how to design future short educational interventions, and to observe how participants were able to put information from the tutorial into action.

5.1.2 Tutorial design

We designed four modules for our E2EE tutorial: a basic overview (O), a module focused on risks E2EE can and cannot protect against (R), a module explicitly debunking misconceptions reported in prior literature (M), and a more detailed (but still not overly technical) description of how E2EE works cryptographically

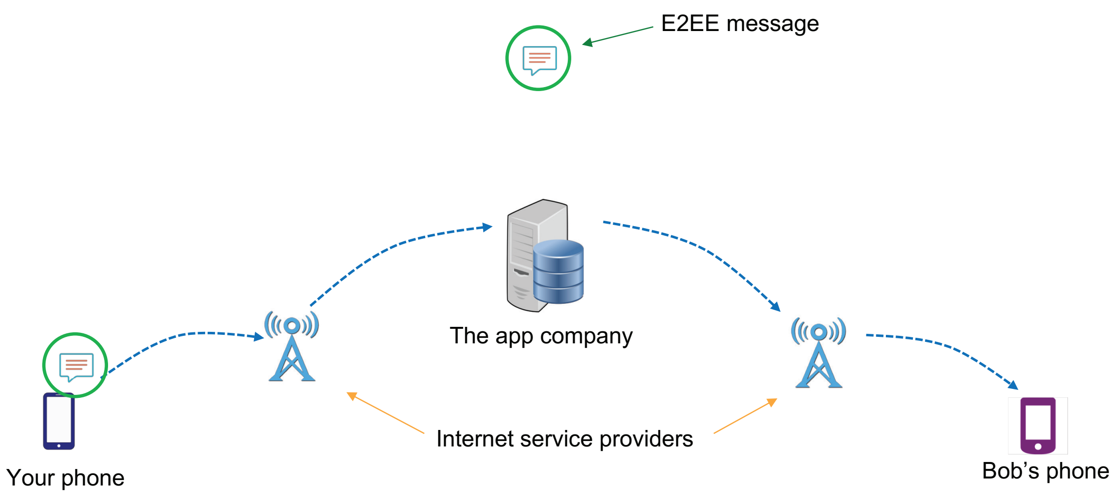


Figure 5.2: Example of visualization used in the tutorial to explain the concept of E2EE, depicting how an E2EE message is sent from "Your Phone" to "Bob's Phone".

(C). Figure 5.2 shows an example slide we used in the tutorial.

5.1.2.1 Overview (O)

The basic overview briefly mentions confidentiality: "with E2EE, only you and your intended recipients can see the messages." We also briefly describe how E2EE protects integrity and authenticity, as well as endpoint weaknesses such as shoulder surfing, message forwarding, and malware on users' phones.

5.1.2.2 Risks (R)

The risk module describes in detail the risks to users when not using E2EE. Prior work has recommended the importance of risk communication with respect to privacy in messaging [8]. We frame these risks by first illustrating, at a high level, how messages transit through ISPs and messaging app companies on their way to the recipient. This illustration aligns with those presented in prior work [6,68], with the addition of ISPs. (As we will see below, the role of ISPs in the messaging process proved surprising to many participants.)

We first highlighted many possible risks of unprotected communication within this ecosystem: interference at endpoints, at the ISP, at the messaging app server, and in transit in between. We then discussed how point-to-point encryption (e.g., webmail over TLS) could mitigate some of these risks, before finally detailing the additional mitigations provided by E2EE.

5.1.2.3 Misconceptions (M)

The misconception module focused on three misconceptions or misunderstandings identified in prior work. First, prior research has identified a belief that encryption is "futile" because no privacy mechanism could be strong enough to protect from powerful attackers like governments or highly skilled hackers, especially if the mechanics of the encryption system are known to the attacker [5,8]. We presented this misconception to participants and then briefly explained the proven strengths of (properly configured) encryption algorithms against even well resourced and knowledgeable attackers.

Prior work has also suggested that many users believe that standard audio calls and SMS messages are more secure than E2EE messaging apps [5, 35]. We clarified to participants that E2EE messaging is the most secure of these options.

Finally, some users mistakenly believe that authenticity and integrity are controlled entirely by username and password security [5]. We explained to participants that even if usernames and passwords are not compromised, without encryption attackers may be able to tamper with messages or impersonate other users.[1]

5.1.2.4 How Cryptography Works (C)

Our final module explains public key encryption using a lock-and-key metaphor adapted from [54]. Participants were told that at app installation, a public lock and private key pair would be created on their phones. All users' public locks would be stored at the app company, referencing the key-directory model commonly used in messaging apps. To send an encrypted message to a friend, the participant's device would request the friend's public lock and use it to lock the message; only the friend, via possession of the matching private key, would be able to read the message. Prior work has obtained mixed results on the utility of explaining the underlying cryptography model [8, 54, 67]. We included this module to investigate both how it would affect users' overall understanding and whether they would find it interesting or important.

5.1.2.5 Tutorial Conditions

To investigate how these different modules affected participants' knowledge retention and sentiment, we created five conditions, each with a different combination

[1] In many E2EE messaging apps, authenticity must be explicitly verified via a ceremony; for simplicity, given the many other concepts we were attempting to convey, we consider details of authentication ceremonies out of scope for this study.

of modules. In an exploratory, lab-based study, obtaining enough participants for a full-factorial design was infeasible; instead, we selected orthogonal combinations to test different hypotheses. All five conditions include the basic overview (to provide a common introduction), plus at most two other modules (to avoid making the tutorial too long). Because we hypothesized (based on prior work) that the cryptography explanation would be least useful, we included it in only one condition. The five conditions, summarized in Table 5.2, include overview only (O); overview + risks (OR); overview + misconceptions (OM); overview + risks + cryptography (ORC); and overview + risks + misconceptions (ORM).

Module	**Condition**				
	O	**OR**	**OM**	**ORC**	**ORM**
Overview (O)	✓	✓	✓	✓	✓
Risks (R)		✓		✓	✓
Misconceptions (M)			✓		✓
Crypto knowledge (C)				✓	

Table 5.2: Tutorial conditions in our study. Each condition is defined by the set of tutorial modules shown to the participants in that conditionl, with five participants per condition.

5.1.3 Recruitment

We recruited participants who were at least 18 years old and use messaging apps at least once a week. We selected participants who did not possess any significant prior cryptographic knowledge, as reported on a prescreening survey. Participants were recruited via flyers placed around a university campus and in surrounding neighborhoods, emails sent to university distribution lists, and advertisements on Craigslist for Washington D.C. area. All interviews took place in person, at University of Maryland, College Park campus, and all sessions were audio recorded (with permission). Participants were compensated with $20 for completing the one-hour study and additionally reimbursed for parking when applicable. The study protocol used was approved by our University of Maryland's Institutional Review Board (IRB).

5.1.4 Data Analysis

All study sessions were audio recorded. Two researchers transcribed three sessions, and the remaining 22 were transcribed by an external transcription service. The majority of our collected data was qualitative. We applied textual microanalysis to analyze these data [93]. Two researchers iteratively developed a codebook using responses from 3 participants to capture themes of participants' responses. The two researchers then independently coded all participants' responses. We use Krippendorff's α to measure the inter-coder reliability [142]. The average α across the codebook is 0.85, which is considered reliable [142]. After calculating reliability, the researchers met to resolve all disagreements.

Because of the limited sample size, we use changes in quiz responses descriptively, to help contextualize participants' qualitative responses to the tutorial. We do not apply hypothesis testing or attempt to make statistical comparisons.

5.1.5 Limitations

Our sample is small, and our participants were younger and more educated than the general population, potentially limiting generalizability. Most participants (see below) had heard of encrypted messaging, but few actively used it, and all had limited knowledge about encryption and related technologies. We therefore believe our study can provide insight about moderately tech-savvy users who might consider adopting encrypted messaging. Results from this exploratory study can be used as a starting point for developing E2EE explanations and validating them with larger samples.

As in any interview study, participants may have answered quickly rather than thoroughly [133]; to mitigate this, we used a variety of tasks and follow-up questions. Demand characteristics suggest that participants might mirror the content of the tutorials back to the interviewer in an effort to tell us what they thought we wanted to hear [143]. In this study, attempts to mirror content demonstrate what the participant has (not) learned and therefore are not a major source of concern.

More broadly, our tutorial necessarily encodes some of the researchers' judgement about what E2EE concepts are most important for users to learn; this may affect participants' information retention and their responses about importance. We attempted to mitigate this by providing a broad range of content for participants to consider and by endeavoring to present all concepts as equally important.

Finally, results from our tutorial, in which participants focused on the material for several minutes, may not translate directly to real-life contexts, such as glancing at instructions or introductory material when using a messaging app. Nonetheless, we believe that insights from our study — particularly which concepts proved most important and surprising — can provide a foundation for future research into shorter educational interventions that users encounter in passing.

5.2 Results

In this section, we first briefly describe our participant pool. We then discuss what participants learned from our tutorial, which mistaken mental models persisted after the tutorial, and which elements of E2EE participants considered most valuable to learn about.

5.2.1 Participants

In total, 62 people completed our prescreening survey. We recruited 26 participants on a rolling basis, eliminating one who withdrew from the study in the middle. The demographics of participants and the tutorial conditions they were assigned can be seen in Table 5.3. Fourteen of 25 participants were female and 21 were between the ages of 18 and 29, so our participants were younger than average. The

ID	Gend.	Age	Eth.	Crit.	Familiarity
O1	F	18-29	Black	1,2	not heard of
O2	M	18-29	Asian	1,5	use frequently*
O3	M	18-29	Asian	2,6	not heard of
O4	M	18-29	Black	3,5	not heard of
O5	F	30-39	Black	4,6	use frequently
OR1	F	18-29	Black	1,4	heard of, do not use
OR2	F	18-29	Asian	2,3	not heard of
OR3	F	18-29	Asian	2,6	use occasionally
OR4	F	18-29	White	4,5	heard of, do not use
OR5	F	30-39	Black	5,6	not heard of
OM1	M	30-39	Black	1,3	use frequently
OM2	F	18-29	Black	1,5	heard of, do not use
OM3	M	18-29	Asian	2,4	use frequently
OM4	F	18-29	Other	3,6	not heard of
OM5	M	18-29	White	4,6	heard of, do not use
ORC1	M	18-29	Black	1,2	use occasionally
ORC2	F	18-29	White	1,6	heard of, do not use
ORC3	F	18-29	Asian	3,4	use frequently*
ORC4	F	18-29	White	3,6	not heard of
ORC5	M	18-29	Asian	4,5	heard of, do not use
ORM1	M	18-29	Asian	1,3	not heard of
ORM2	M	50-59	N/A	1,6	heard of, do not use
ORM3	F	18-29	White	2,5	not heard of
ORM4	F	18-29	Asian	2,5	heard of, do not use
ORM5	M	18-29	Hispanic	3,4	not heard of

Table 5.3: Participant demographics including, gender, age, ethnicity, messages critiqued, and pre-existing familiarity with encrypted or secure mobile instant messaging. The ID indicates the tutorial condition. Two participants who only use WeChat but identified themselves as frequent users of encrypted tools were marked with *.

participants tended to have an educated background, with 19 holding a bachelor's or master's degree.

Only one participant reported having an education in computer security, computer science, computer engineering, or IT and none reported familiarity with cryptographic algorithms. Eighteen participants reported either not having heard of or not having used encrypted or secure messaging, while five reported that they actively use such messaging. However, two out of five participants who thought they were actively using encrypted or secure messaging used WeChat only.

Participants reported using a variety of messaging tools at least once a week. The majority use Facebook Messenger (20) and iMessage (16). Some reported using Snapchat (12), SMS text messaging (12), Google Hangouts (8), and WhatsApp (6). Four participants or fewer reported using each of WeChat, Telegram, KakaoTalk, Google Allo, GroupMe, Instagram Messenger, and Twitter.

5.2.2 Tutorials improved users' mental models, regardless of condition

Participants' understanding of E2EE improved, across all five tutorial versions. This is reflected in changes to their quiz answers after viewing the tutorial, as well as their interview comments.

5.2.2.1 Participants improved their understanding of messages in transit

Our quiz included two adversaries related to threats in transit: hackers who could eavesdrop in the middle and ISPs. Participants learned that E2EE could protect their messages from these two adversaries: 13 and 10 participants lowered their scores (perceiving eavesdropping to be more difficult) in these two questions, with an average score change of 1.1 and 0.7 (out of five points), respectively.

Before reading the tutorial, participants held several misconceptions about these potential adversaries. Seven participants thought these adversaries could not learn message content because these adversaries were not part of the conversation, and four (one overlapping) were surprised to learn that ISPs were involved in the communication. For example, ORM1 said "[ISPs] are even more outside, like, the actors involved in the communication, [they are] not the company making the app and they're not any of the users, it will be very hard for them to open up the message itself." OR3 commented, "I thought this was one to one relations. Even though they provide the service. . . . Like KakaoTalk, I believe that company can access to my messages, but I've never thought that the provider, Verizon [could]. I thought that they just provide the transportation." ORC2 did not realize the recipient's ISP was involved, believe the app company would send the message directly to its recipient.

On the other hand, six participants believed before the tutorial that ISPs could potentially learn any message, since they provide the internet service for phones. As

OR2 said, “I think they have access to everything you send through the network.” After the tutorial, these participants recognized that encryption (point-to-point or end-to-end) could address this issue.

5.2.2.2 Participants learned that E2EE can provide protection from app companies and government agencies

Comparing quiz scores before and after the tutorial, participants understood better that E2EE could protect their messages from app companies and government agencies. The average score of app company was lowered from 3.16 to 1.36, and that of government decreased from 3.64 to 1.76.

Before the tutorial, seventeen participants who thought E2EE messages were vulnerable to these adversaries incorrectly mentioned plaintext messages being stored at the app company, where governments could also request them. Besides, in line with findings from Abu-Salma et al. [5], eleven suggested that these relatively powerful adversaries could simply break the encryption.

After the tutorial, 22 participants recognized that E2EE prevents plaintext messages from being stored at the app company and can defend against even powerful adversaries. OR2 stated, “Using E2EE there will be a shield. . . . The company would know there is a message that exists, but they wouldn’t know what content it contains.” ORM5 similarly commented, “It’s easy for the government to get a copy . . . but with E2EE they won’t be able to break the encryption to see what’s inside of the message.”

5.2.2.3 Participants better recognized E2EE limitations

After the tutorial, 10 participants rated the risk to communications at the endpoints (even when using E2EE) higher than they had initially, and the number of participants who correctly understood that E2EE could not protect them from malware on their phones increased from 16 to 21. Before reading the tutorial, six participants thought encryption could protect against malware at endpoints: "Malware [is] getting access to the activities, but . . . the message is still going to be encrypted" (OM2). Two participants did not understand before the tutorial how malware related to message privacy at all.

OM2 updated his opinion after the tutorial: "If malware's already installed on your phone, then it's not really protected because they have access to the original message before it's even encrypted." This perspective was also new to OM4, who "was surprised to find out that if a hacker installs malware they can take off the encryption." ORM2 was very specific in pointing out that E2EE could protect against "two out of those three risks: the transit ones, and the app company, but not the user phones."

5.2.3 Some concerns and misunderstandings remained; others developed

Although our tutorial improved participants' understanding of E2EE overall, we found that some participants retained existing concerns and misconceptions, and even developed new ones.

5.2.3.1 Confidentiality concerns remain

After the tutorial, eight participants remained unconvinced that E2EE could provide sufficient confidentiality, most often with respect to powerful adversaries. For example, OR5 argued that government agencies have “both the resources and the knowledge base to crack an algorithm.” Similarly, ORC4 continued to believe that the app company would inherently have enough knowledge about the encryption process to access messages: “If the company creates the encryption or whatever, I’m assuming there is some sort of maybe possibility of them decrypting it . . . because I was thinking if Bob gets a lock and a key, creates whatever, . . . then the locks go here [to the company], so the company still has your lock, meaning even if it’s encrypted wouldn’t they be able to at some point decrypt it?” ORC2 suggested that skilled hackers could similarly overcome E2EE: “Because I’m thinking of it literally, although I’m sure it’s not, as a key and lock mechanism, I would imagine that if you work in a locksmith office, if you’re an expert in keys and locks, you might not have somebody’s key but you would be able to get into their house because you are an expert and you know how to manipulate systems.”

5.2.3.2 E2EE is less secure than other communication methods

Four participants ranked one of SMS, email, or direct phone call as the most secure communications method even after the tutorial. Some argued that voice conversations are more transient than written messages: “It’s just talk. That’s most likely to be forgotten” (O4). OR1, on the other hand, preferred phone calls as a means to establish authenticity: “I feel like if I know someone, like if I know my friend or someone in my family, it’s very hard to mimic that voice .... With a phone call, I’d be like, ‘Oh, that’s not you.’ ”

5.2.3.3 Point-to-point encryption is devalued

All modules of our tutorial emphasized the benefits of E2EE. The risks module explicitly distinguishes point-to-point encryption from E2EE, but also mentions that most non-E2EE messaging apps are encrypted point-to-point. This nuance does not seem to have been entirely absorbed. ORC2 recalled from the tutorial that non-E2EE messaging apps “[take] out the first threat even though there are the other threats. So maybe it’s not quite as easy” as with no protection; however, she still ranked such apps behind standard voice calling in the security ranking question. Among the 15 participants who viewed the Risk module, 10 retained their security ranking for these apps (relative to E2EE apps, standard email, SMS and standard phone calls), among whom seven still ranked non-E2EE messaging in fourth or last place. Four other participants reduced their ranking for these apps. This suggests that researchers, designers, and advocates promoting the benefits of E2EE must be careful not to inadvertently push consumers toward least secure options when E2EE is unavailable or undesirable.

5.2.3.4 Integrity and authenticity remain confusing despite some improvement

Prior work has found that users' mental models for encrypted communication do not effectively consider integrity and authenticity [5, 8], and our findings accord with these prior studies. Before the tutorial, most participants did not think integrity (14) or authenticity (18) could easily be violated in E2EE communication; however, many did not relate this difficulty to E2EE, instead believing that such violations would be inherently difficult in any messaging system. Eleven participants believed that these violations would require multiple unlikely steps, and three believed an attacker could never be fast enough to alter a message in transit. OR3 said "They have to read it and they have to manipulate the contents. So it's not very easy. . . . There should be an extra step, I think," and OR4 said, "It would have to happen while the [sender]'s typing, cause like if they get the message instantaneously, then...They'd have only like a second to change it." Eleven participants, meanwhile, believed integrity and authenticity were determined entirely by protection of usernames and passwords, rather than any vulnerability in transit.

After the tutorial, participants were more likely to recognize that E2EE could protect integrity and authenticity. As OR5 explained, messages "have the end-to-end encryption, and if the phone's not stolen, it's going to be difficult." While these participants believed the tutorial's assertion that E2EE can assure integrity and authenticity, exactly how E2EE provides this protection remained blurry to them. Seven continued to confuse integrity with confidentiality. For example, O5 remarked that “there’s really nothing for him (the attacker) to modify because he doesn’t know the contents of the message.” (To be fair, properly designed E2EE tools should protect both confidentiality and integrity without requiring the user to make a distinction.) Further, two participants continued to believe that a limited time window for action would prevent an integrity or authenticity violation, and other participants continued to conflate authenticity with username and password issues. O5 suggested that “E2EE protects against message modification and impersonation. Not even usernames and or passwords can be stolen or guessed.”

Relatedly, the integrity and authenticity discussion in the Misconceptions module was cited by several participants as the least effective section of the tutorial, with three explicitly mentioning that it was unclear or confusing. This may be because these concepts are inherently difficult to explain, because we happened to explain them poorly, or both.

5.2.3.5 E2EE protects against malware

While many participants increased their understanding of endpoint threats after the tutorial, five participants lowered their scores with respect to malware in the quiz, indicating an increased belief that E2EE could protect against malware on their phones. As ORM3 explained, “Even if you put the malware on the phone, it’s not gonna give you access because the data is so well encrypted.” OR4 concurred that “By using E2EE, you decrease the likelihood that someone can hack into your phone.” These results underscore the importance of ensuring that educational interventions do not give users a false sense of security.

5.2.4 What knowledge should we impart?

In this section, we discuss the information that was most salient to our participants, including what they found most important and most surprising as well as what they chose to disseminate to others.

5.2.4.1 Confidentiality is most significant

Unsurprisingly, confidentiality was the most significant information to our participants. It was selected 13 times as the most important information and nine times as the most surprising, which were each more than other themes. O1 said “the inability of other parties to read your messages” was most important because “that actually is the primary purpose of end-to-end encryption.” ORM5 was surprised that “the internet service provider and the app company . . . may still get a copy of the message, that is protected by this wall, that is nearly impossible to break. So they can see you sent a message, but they can’t see what the message says.” OR2 was similarly surprised that with E2EE, even the government could not read the message content: “I thought the government could always read what you have sent because, like, you always heard in the news that some student said something stupid on their phone and they got deported or something. . . . So I always thought that the government can read everything you send. But now today I realize, oh they can’t.”

When asked about what information they would tell others, 17 participants mentioned confidentiality. For example, OM2 would tell a friend "that if you use E2EE on a messaging platform, it is going to be the most secure way that you can send messages. . . . It has kind of like a very, very, strong protective layer around the message so that people can't intercept the message and retrieve its contents. It will only be accessible to the intended recipient."

The importance of confidentiality was also reflected in critiquing existing messages and designing new ones. Almost everyone pointed positively to portions of existing mentions that mention confidentiality, and 20 participants mentioned it in their own messages. O5 wrote in his message that "E2EE is a great way to ensure that your messages will be securely transmitted to the recipient of the message originally intended for. The data is encrypted where no one has directed access to the text contents but the sender and the receiver of the information. Not even the monitoring company, hackers and the government can see the message."

5.2.4.2 Risks are useful to communicate how E2EE and non-E2EE differ

In addition to confidentiality, the risks of non-E2EE messaging were also commonly mentioned. Of 15 participants who saw the Risks module (OR, ORC, ORM), six reported that risks were most important to discuss and five reported risks as most surprising. All six who mentioned risks as important noted that risks were most useful to clearly differentiate E2EE from non-E2EE communications. For instance, ORC4 said “I think, again, knowing the risks of the non-E2EE and then really comparing it to how is this better. So that’s really the most important.” OR1 agreed that “this is all very important as consumers in the United States . . . I think they just want the bottom line, like okay, what is the difference? So, I think the risk factors are probably the biggest takeaway.”

When asked what information they would tell their friends or family about E2EE, overall 10 participants specifically mentioned risks, among whom seven had seen our Risk module. As with importance, these participants used risks specifically to explain why E2EE was better than non-E2EE: ORM3 said he would start by explaining the risks of non-E2EE messaging and then explaining that E2EE “really protects it [your message] while it’s in transit and while it’s at the app company. . . . It can’t be modified or impersonated or whatever. . . . The end-to-end encrypted apps basically protect your message along the entire pathway and it’s the most secure way to send a message.” OR4 agreed that “showing them the benefits of encryption so it’s less likely your information will be hacked would probably be beneficial,” particularly in the context of many data breaches in the news.

The usage of risks to distinguish E2EE from non-E2EE was similarly reflected in participants’ designed messages. OR5 wrote, “Your information is exposed every time you utilize your mobile device. There are three potential exposures, the service providers, the app company, and hackers. In efforts to protect yourself against these parties, please ensure your devices has E2EE protection.” ORM4 began with a detailed message about risks, concluding that “it is essential to find ways to provide more security when communicating over the web,” before going on to explain how

E2EE could address these risks.

5.2.4.3 Explaining weaknesses can be important

We introduced three endpoint weaknesses in the tutorial — shoulder surfing, message forwarding, and malware — but malware primarily drew our participants' attention. Four and five participants reported that this information was the most important and most surprising, respectively. ORC4 explained that "If you're presenting this as a product, I think it's important to [be] realistic and inform people." O3 agreed: "The malware piece is important for me to know if I'm specifically looking at TextLight company and what is not protected . . . because I want to know to what extent is this actually going to be secure?" Similarly, four participants said that if they were to introduce E2EE to other people, they would mention the limitations, and 13 participants acknowledged the limitations straightforwardly in their designed messages. For example, OR4 wrote that "While there are benefits to using E2EE, everyday risks still pose a threat, like a thief stealing your phone, someone looking over your shoulder, or if someone installs malware on an unlocked phone."

Among the messages critiqued by participants, only Msg3 pointed out the possible weaknesses: "But please remember that we cannot protect you from your own mother if she takes your unlocked phone without a passcode. Or from your IT-department if they access your computer at work. Or from any other people that get physical or root access to your phones or computers running TextLight." This information was marked as especially useful by five participants out of eight who saw this message. These participants noted positively both the content of the information and the humorous tone. (However, two participants including ORM5 noted that "root access" was jargon: "I don't know what root access means. What happened?")

5.2.4.4 Cryptography details should be used with caution

We observed mixed reactions to technical details presented in our Crypto Knowledge module and in the existing messages that participants critiqued.

Cryptography details can be interesting or reassuring, but are not necessary Five participants in ORC saw the Crypto Knowledge module. Only one of these participants selected this module as important, because "you cannot tell people this thing is so good, but you don't tell them why" (ORC3). O3, who did not see the Crypto Knowledge module but did critique a message that used the same lock-and-key metaphor (Msg2) remarked that this information "made it a little bit more understanding of what encryption could look like, even though it's not probably how it works."

A few participants who reacted positively to crypto details (in our tutorial or in the critiqued messages) were reassured by the information that a secret key was known only to the user and their devices, as pointed out in Msg4 and Msg6. ORM2, for example, noted that this "eliminates all possibility on service providers that access because it doesn't have the ability to decipher the information. Well, it says they don't have the encryption keys in order to break the codes."

None of the ORC participants mentioned crypto knowledge or the lock and key metaphor when asked what they would tell their friends and family about E2EE. Eight of 25 participants' message designs messages mentioned cryptography, including three that mentioned keys known only to the user and not the app company.

Interestingly, seven participants from conditions other than ORC expressed interest in learning more details about how E2EE works. One participant who did see the Crypto Knowledge module said the module was insufficiently detailed and wished to learn more.

Technical details can create confusion   On the other hand, some participants were confused by technical details. "This [tutorial] is intended for new users, people who don't know anything, like me. This [crypto explanation] is helpful, but I don't need to know exactly how it happens because I can understand what encryption means to some extent" (P1). The same participant similarly found the explanation in Msg4, which referred to "a code that only the recipient's device can translate into plain text," confusing: "I think it's trying to describe the mechanism into encryption, like how it works, but it didn't do a good job." Other participants found specific details confusing: OM5 associated a key with a password and asked, "How do you have a key that you have to put in every time to see a message?" ORM3 was confused by the assertion in Msg5 that "the user is in control over the key exchange," asking, "Do I have to do something? How does that key exchange happen?" Two other participants expressed similar feelings.

Msg2, sourced from WhatsApp, uses the same lock-and-key metaphor we adopted for the Crypto Knowledge module. Seven of eight participants who critiqued this message liked the analogy, and three thought it explained encryption well, but three found the specific language confusing. In particular, O1 thought that the message's reference to a "special key" was "flowery" and "corny." OR2 objected to the message's reference to unique locks and keys for "added protection": "What does it mean by 'added protection?' I don't get it. . . . You already lock it once, why do I have to to lock it twice?"

Msg5 (Threema) explains E2EE as two layers of protection, a "transport layer" and an "end-to-end encryption layer," emphasizing that "the crucial part is that the end-to-end encryption layer passes through the server uninterrupted; the server cannot remove the inner encryption layer." Four of eight participants agreed this explanation increased their confidence in E2EE protection, but five participants worried that it was too technical or even boring to non-experts. OM2 said he couldn't picture what this would look like: "I didn't really understand the difference between them. I didn't understand if it was an inner layer or outer layer, whatever that meant. It was just frustrating . . . I didn't know what it meant by passes through uninterrupted, like does it stop working, or whatever."

Of the eight participant-designed messages that mentioned cryptography, four attempted to apply the lock-and-key metaphor, and three made minor technical errors, including suggesting that the lock and key themselves were encrypted, and providing a symmetric-encryption-like explanation.

5.2.4.5 Other concepts were less important to participants

Other ideas covered in our tutorial and in the critique messages, including integrity and authenticity, comparison with other tools, and algorithm security, did not receive much attention from our participants.

Integrity and authenticity Integrity and authenticity were briefly discussed in the basic Overview module seen by all participants, and then explained in more detail as part of the Misconceptions module seen by 10 participants.

Only a few participants selected integrity and authenticity as important (1) or surprising (2). O1 chose integrity and authenticity as both important and surprising: "I didn't know that there was a system that could prevent that from happening." Three participants mentioned integrity and/or authenticity when choosing information to tell a friend or family member, and six included them in the messages they designed. This unpopularity may relate to the fact that we were relatively unsuccessful explaining these concepts to our participants (Section 5.2.3.4).

Comparison with other tools Ten participants in OM and ORM learned in our Misconceptions module that E2EE messaging is more secure than standard email, phone calls, and SMS. Four participants mentioned this fact as most important, and two mentioned it as most surprising. As ORM4 said the most surprising thing was "probably the misconception that E2EE is more secure than the other methods, 'cause I thought that phone calls was the most secure form since it's using your voice and not actually recorded." Only two participants included a comparison to other communications mechanisms in the messages they designed.

Algorithm security We also included in our Misconceptions module information about algorithm strength; this was intended to combat the finding in prior work that many users assume that an expert who understands the cryptography can always break it [5]. This information did not prove very salient to the 10 participants (OM, ORM) who learned it: only two mentioned it as most important and two as most surprising. ORM3 was most surprised that “it would take like a million years or something . . . ’cause I feel like you always hear about hackers . . . I was surprised just how secure it is.”

Four participants from these conditions mentioned algorithm security in the messages they designed, in all cases as a way to emphasize confidentiality. As ORM1 wrote, “The algorithms that are utilized here are extremely strong and would take third parties an impossible amount of time to crack and decrypt.”

5.2.5 Other feedback about educational interventions

Finally, we report some additional feedback from participants about our tutorial, as well as about the existing texts they critiqued.

5.2.5.1 The tutorial was generally well received

Overall, participants rated the tutorial as easy to understand (mean 4.9 on a five-point Likert scale) and informative (mean 4.5). While these high scores may partially reflect demand effects, participants’ detailed comments suggest that they appreciated the simple language and visualizations in the tutorial. OM2 said "I think it was easy because you used very clear, simple and concise language. Additionally, with the visuals, it was very easy to understand what was happening. The visuals really, I think, facilitated my understanding of what the message was trying to convey." Other participants, such as ORM1, said they gained new knowledge: "It was pretty informative. I learned a lot that I didn't know before, clarifying how messaging apps actually work, the risks and how encryption can help protect you against that." Participants including O1 also said the length was about right: "Since it's a short presentation, I'm sure there was more to learn. However, I don't think anyone needed to know more than that. So I think it was good."

A few participants, however, commented on tutorial elements that were not clear. The majority of these comments referenced integrity and authenticity; as described above, our tutorial did not succeed in explaining these nuanced concepts effectively.

5.2.5.2 Wording should be clear and simple

Participants' critiques of the five existing messages revealed several instances where overly complicated explanations, jargon, and related issues inhibited understanding.

As one example, both Msg2 and Msg5 mention that E2EE is applied automatically (a fact that several participants appreciated). Participants preferred the shorter, clearer wording in Msg5 (five likes, no dislikes) to the longer version in

Msg2 (two likes, three dislikes); O3 disliked that the automation description in Msg2 seemed to be “trying really hard to persuade.” Three participants who viewed these messages went on to mention automation in the messages they designed.

Participants struggled with Msg1’s use of “chat rooms” (O1, ORC1, OR1), which was considered outdated and evoked group rather than one-to-one communication. (We speculate that the use of “chat room” may be more standard in East Asia, where LINE is more popular.) Three out of eight participants who viewed Msg3 (Telegram) struggled with technical terms like ISP, network administrator, and third parties.

The first sentence from Msg2 (WhatsApp) begins “Many messaging apps only encrypt messages between you and them.” Three of eight participants who viewed this text were confused about who “them” referred to. O3 correctly guessed “they” were the messaging apps, but O1 assumed that “they” were message receivers and consequently misunderstood the rest of the sentence.

5.2.5.3 Reaction to ad-targeting prevention was surprisingly mixed

Msg4 (Viber) explains that use of E2EE can prevent data collection that later leads to targeted ads in another setting. Five of eight participants who viewed this add commented on this as a desirable feature, although no one included it in the message they designed. To our surprise, two participants were confused by this, as the messaging apps they were familiar with did not typically contain ads. This misconception is perhaps attributable to poor wording in Msg4 as well as to generally poor understanding of how behavioral advertising and retargeting work [144]. We leave it to future work to explore how secondary privacy benefits such as prevention of ad targeting — when clearly explained — affect users' overall impressions of E2EE.

5.3 Conclusion

In this study, we explored how to improve general users' mental models of end-to-end encryption. We designed a tutorial with four modules: a brief overview, risks associated with non-E2EE communication, corrections to three common misconceptions, and a high-level description of how E2EE technically works. We evaluated what our participants learned, what misconceptions they retained, and which information they found most valuable. We found that overall our tutorials were effective at conveying high-level security properties of E2EE, including potential weaknesses at endpoints. They also corrected certain existing misconceptions about who has access to messages in transit. We found that the risks module effectively conveyed intended ideas about the relative risks of E2EE and non-E2EE communications, but the misconceptions module did not effectively address confusion about integrity and authenticity. The technical description increased understanding somewhat for some participants, but also promoted misunderstanding for others, and was not considered particularly important or useful. The critique activities, meanwhile, revealed several points of confusion within existing messages. Overall, participants' responses suggested that emphasizing confidentiality, clearly conveying the limitations of E2EE protections, and reducing complexity are the most important properties for effective education. We hope that these recommendations can inform the design of interventions that can be integrated more naturally into users' communication workflows, such as those on apps' webpages, in their installation descriptions, or in interstitial screens.

Chapter 6: Discussion

This dissertation investigates the adoption of end-to-end encrypted communication from a variety of user-centered perspective. Based on our studies, we provide some recommendations to the community.

6.1 Choosing Among Key Management Models

In Chapter 3, we conducted the first study examining how non-expert users, briefly introduced to the topic, think about the privacy and convenience tradeoffs that are inherent in the choice of encryption models, rather than about user-interface design tradeoffs.

We found that while participants recognized that the exchange model could provide better overall privacy, they also recognized its potential for self-defeating mistakes. Similarly, our participants acknowledged potential security problems in the registration model, but found it "good enough" for many everyday purposes, especially the option to audit the system and/or split trust among several parties was added. This result is particularly encouraging for approaches like CONIKS and Google's potential end-to-end extension, which spread trust among many potential and actual auditors. It is important to note that understanding the identities and motivations of third-party auditors was important to several of our participants, so making this auditing process as open and transparent as possible may prove important to its success.

We believe our results have important implications for designers of encryption tools as well as researchers, policymakers, journalists, and security commentators. Alarmed denunciations of tools that do not offer perfect privacy may only serve to scare users away from any encryption at all, given that many users already believe encryption is either too much work or unnecessary for their personal communications. Instead, making clear both the marginal benefit and the risk can support better decision making. This also underscores the critical importance of making risks explicit up front, in plain non-technical language; users who are misled into a false sense of security may misjudge tradeoffs to their detriment.

As end-to-end encryption is increasingly widely deployed, designers and companies must make choices about which models to adopt. We believe our results can provide some additional context for making these decisions, relative to the targeted use cases and user population.

6.2 Adding Search to End-to-End Encryption

In Chapter 4, we took the first step in characterizing user-facing tradeoffs inherent in supporting search for an encrypted communication solution. We considered six features, which provide interesting distinction across the space of possible approaches: price, multi-word search ability, partial-word search ability, privacy, local storage occupation, and synchronizing capability.

We found that among the non-monetary features we evaluated, privacy ranked highest overall, with local storage second. However, the value of a secondary privacy improvement — defined in our study as moving from extra to maximum privacy — was slightly less than the value of changing from 500 to 5 MB of local storage. Advanced search features using multiple words and partial-word matching were less valuable overall.

These results have important implications for the design of encrypted communication systems, and in particular for supporting search features. Current encrypted instant-messaging systems rely on a local-index solution, which provides maximum privacy (assuming no endpoint compromise) but also requires additional local storage. Searchable encryption approaches, in contrast, give up some degree of privacy, and limit the flexibility of the searches that can be conducted, but reduce the requirement for local storage.

Our results suggest, then, that at least in the email context, there is a potentially valuable niche for a searchable encryption solution. For some users, the potential reduction in privacy relative to a local index will be worthwhile. In line with prior work, we find that most users do not find significant value in advanced searching capabilities. Overall, this suggests that designers of searchable encryption schemes with email in mind concentrate on privacy and convenience, rather than support for increasingly complex search operations.

Further, our results suggest that searchable encryption may have potential as a reasonable compromise point: more privacy than the current standard, in which email services have plaintext access to all messages, while limiting some inconveniences that may prevent broader adoption of end-to-end encryption.

Our results also show high variation in the relative values of privacy and storage among different participants. We also found that privacy concern and web-use skill are positively correlated with higher valuation of privacy, and particularly higher marginal valuation of additional privacy. This suggests that rather than attempting to develop one suitable solution to enabling end-to-encryption for email, different solutions may be most appropriate for different user groups. Users with more web experience, with higher base levels of privacy concern, and/or with fewer limitations in e.g. local storage may prefer a local-index solution, while others may prefer a searchable-encryption solution. One possible option might be to provide a simple configuration switch offering the user more privacy/more storage or less privacy/less storage, and then implementing either a local index or searchable encryption accordingly. Simple tradeoff language may be appropriate for many users, potentially with a "more information" link to provide details to those who want or need them.

6.3 Helping Users Understand End-to-End Encryption

Throughout our dissertation, helping users understand end-to-end encryption is a key component, which either serves as the necessity to complete the study tasks (Chapters 3 and 4), or acts as the main purpose of the study (Chapter 5).

6.3.1 Users Could Understand End-to-End Encryption

Our results suggest that it may be reasonable to explain in clear language what the high-level risks of a given encryption approach are and trust users to make decisions accordingly. In Chapter 3, our participants could understand at least some high-level security properties of the underlying key management models used in end-to-end encryption, and could coherently trade these properties off against factors like convenience. In Chapter 4, although the purpose of this study was not to design the best way to present information about email service privacy, our participants valued initial privacy improvement more than the secondary privacy improvement when different privacy levels were presented explicitly. In Chapter 5, our participants' understanding of E2EE was overall improved by reading the tutorial designed by us. In general, we observed improvement in understanding how E2EE can protect confidentiality, how it compares to non-E2EE mechanisms, and its limitations. Our participants could better recognize potential adversaries, such as internet service providers, that they had not previously considered as relevant; they also newly recognized that E2EE can provide protection even against powerful adversaries like app companies and governments. Further, the tutorial helped participants recognize that E2EE cannot protect against endpoint threats such as malware.

We do, however, advise some caution. Although most participants understood several aspects of end-to-end encryption at a high level by learning our tutorials, participants still maintained some existing concerns and misunderstandings, and even developed new ones. As an example, our attempt to clarify authenticity and integrity in Chapter 5 — an in particular to disentangle it from password security — was not successful. Further, some participants maintained their belief that standard voice calls are inherently more secure than any text communication, including E2EE messaging.

6.3.2 Helping Users in the Field

Despite years of effort from the security community, effectively communicating the security properties of end-to-end encryption remain difficult. The Electronic Frontier Foundation's *Secure Messaging Scorecard*, which tracks the security properties of encryption tools, provides an valuable start in this direction [66], although it was shown not as effective as expected [5]. In Chapter 5, we took the first study to evaluate existing end-to-end introductory texts drawn from real tools like WhatsApp and Threema. We found that many of these messages contain confusing or misleading wording and technical jargon that could create misunderstandings even for users with time and motivation to carefully read instructions.

However, echoing with prior work that placing information about security up front can lead to users making more security-protective decisions [132], we believe our endeavors presented in this dissertation demonstrate the benefits of continuing to try to help users understand benefits and tradeoffs of end-to-end encrypted communications, which could be crucial to users' ability to make meaningful decisions about their choice of communication channels. Of course, participants in our three studies were directly instructed to read the materials we gave them, either verbally imparted (Chapters 3 and 5), or forced to read online (Chapter 4). In practice, real users often have neither the time nor the motivation to seek out this kind of information. We therefore distill — from our participants' responses to the tutorials, their critiques of existing messages, and their efforts to design new messages — key elements that we hope can translate to shorter educational interventions, such as those on apps' webpages, in their installation descriptions, or in interstitial screens. Our recommendations are as follows:

- **Confidentiality is the primary ingredient**. Our participants placed highest importance on conveying how E2EE can protect users' messages from being read by various adversaries, as shown in all studies in our dissertation. This can be underscored by references to risk, algorithm strength, and the comparative security of different communications methods in Chapter 5. Perhaps most important is to explicitly explain protection against relatively powerful adversaries, as this information was most surprising to many participants.

- **Risks can be used to support comparison.** One way to effectively emphasize confidentiality is to detail the risks that distinguish E2EE from, e.g., point-to-point encryption. This improves users' mental threat models and can provide a stronger sense of security that may help to motivate adoption.

- **Technical details only in small doses.** While understanding how E2EE works seems useful when choosing key management models behind each tool (Chapter 3), and might interest some users (Chapter 5), most of our participants did not find it critical, considering that majority of the popular messaging tools have already adopted the key-directory based model, so that users are not confronted with the choice of key management models when adopting an encrypted communication tool currently. Also, we observed a strong risk of misunderstandings that undermine educational goals. Previous work noted that commonly used metaphors may fail because they are *structural* (what the system looks like) rather than *functional* (what it can do) [67]. In line with this, we observed that technical details were most effective when they were most functional. In particular, emphasizing that the secret stays on one user's device (rather than at the app company, or shared with communicating parties) appears to be a good way to improve users' perception of security without creating new confusion.

- **Clarifying weaknesses is important.** Participants' recognized a lot of value in clarifying what E2EE cannot protect against, as part of a holistic view of its security (Chapters 3 and 5). Commercial companies may be hesitant to call attention to drawbacks of their products, but our evidence suggests this clarity is critical to fixing the broken mental models that can limit adoption.

- **Explaining integrity and authenticity may not be worth it.** Our unsuccessful explanations of integrity and authenticity in Chapter 5, combined with prior related findings, suggest that conveying these nuanced concepts effectively will continue to be challenging. Relatively few participants regarded these concepts as important in themselves; instead, most participants absorbed them into their model of confidentiality, which they did see as important. (This aligns with the approach given in [6] of redefining authenticity in terms of confidentiality.) As such, we recommend against trying to explain integrity and authenticity independently.

- **Strive for simplicity** Various comments from our critique session in Chapter 5 demonstrate that jargon words not only obstruct users' understanding, but also annoy them. Relatedly, participants generally frowned on overly complex explanations, whereas simple explanations were both preferred in critiques and more likely to be repeated in the design task. All the texts we examined appear to have been written to be colloquial, but we suggest even further simplification.

We hope that these recommendations can inform the design of interventions that can be integrated more naturally into users' communication workflows. In particular, they must be validated with broader demographics and in situations when learning about E2EE is not the user's primary task. Future work should also examine how to tie these high-level mental models more directly to concrete tasks such as choosing a communication medium, turning on E2EE mode (when not automated), or performing an authentication ceremony. Besides of system designers, our work also magnifies the role of journalists, security commentators, and other opinion-makers whose recommendations users often rely on instead, and we hope our findings from this dissertation could better help them when communicating end-to-end encryption to the general public.

Overall, we believed that continued education from all community, discussions in the media, and more frequent engagement with encryption tools in daily life may all assist in broader adoption and more effective use of communications tools.

Chapter 7: Conclusions and Future Work

7.1 Conclusions

In this dissertation, we investigated the adoption of end-to-end encrypted communication from a variety of user-centered perspectives.

We begin with understanding how general users balance the usability and security tradeoffs for different key management models in end-to-end encryption. We found that users could understand at least some high-level security properties and could coherently trade these properties off against factors like convenience. We found that while participants recognized that the exchange model could provide better overall privacy, they also recognized its potential for self-defeating mistakes. Similarly, our participants acknowledged potential security problems in the registration model, but found it "good enough" for many everyday purposes, especially when offered the option to audit the system and/or split trust among several parties. Therefore, trying to convince average users to exclusively use more complicated schemes, when they often don't see a need for the added protection, may instead keep them away from using any encryption at all. Rather than spreading undue alarm about the risks of key-directory based models, or forcing users into only exchange models, we recommend that policymakers and designers present tradeoffs clearly and encourage adoption of usable but imperfect security for the many scenarios where it may be appropriate.

We then explored users' tradeoffs for search in encrypted communications. We found that privacy was the most important non-price feature to our participants, and minimizing the use of local storage was almost as highly valued. These findings suggested that in the email context, although local indexing may largely be suitable, there might also be a niche for searchable encryption. For some users, the potential reduction in privacy relative to a local index will be worthwhile, in order to save on storage space. In particular, searchable encryption may have potential as a compromise: more privacy than the current standard, in which email services have plaintext access to all messages, while limiting some inconveniences that may prevent broader adoption of end-to-end encryption.

Finally, we explored how to improve general users' mental models of end-to-end encryption. We designed a tutorial with four modules: a brief overview, risks associated with non-E2EE communication, corrections to three common misconceptions, and a high-level description of how E2EE works technically. We evaluated what our participants learned, what misconceptions they retained, and which information they found most valuable. We found that overall our tutorials were effective at conveying high-level security properties of E2EE, including potential weaknesses at endpoints. They also corrected certain existing misconceptions about who has access to messages in transit. We found that the risks module effectively conveyed intended ideas about the relative risks of E2EE and non-E2EE communications, but the misconceptions module did not effectively address confusion about integrity and authenticity. The technical description increased understanding somewhat for some participants, but also promoted misunderstanding for others, and was not considered particularly important or useful. The critique activities, meanwhile, revealed several points of confusion within existing messages. Overall, participants' responses suggested that emphasizing confidentiality, clearly conveying the limitations of E2EE protections, and reducing complexity are the most important properties for effective education. We hope that these recommendations can inform the design of interventions that can be integrated more naturally into users' communication workflows, such as those on apps' webpages, in their installation descriptions, or in interstitial screens.

7.2 Future Directions

Extending evaluation of searchable encrypted communication. In Chapter 4, we explored only a small subset of possible tradeoffs inherent in supporting search for end-to-end encryption. Future work could apply similar approaches to test a broader array of features (for example, latency) or to test more options for each feature (a larger range of possible prices, more storage size options, or more detailed breakdowns of privacy models).

Besides, our work didn't ask or measure our participants' current email behaviors, such as how they performed search in their daily life, how many emails they had, and how often they checked their emails both in laptops/PCs and mobile phones. Future work could try to get these "ground truth" before asking participants the choice questions, and compare how their perceptions extracted from conjoint analysis differ.

Also, we acknowledged that expressed preferences, even in a conjoint analysis study designed to operationalize relative value, do not always match real-world behavior. As such, it would be useful to design a follow-up field study, in which participants live with the consequences of the tradeoffs they select for days or weeks, to see how this changes their opinions.

Designing effective educational materials. All of our work, either part or the whole chapter, emphasized the importance to user education about end-to-end encryption so that users could make better informed decisions when adopting and using encrypted communication tools. In Chapters 3 and 5, we designed the educational materials about end-to-end encryption in PowerPoint slides, and conducted the study in a tutorial-style scenario. In practice, of course, most users will not have the time or interest to complete the tutorial like this. Therefore, based on the key elements distilled from our study, future directions could derive more concise, understandable and attractive educational materials, both in terms of content and intervention, which can be integrated more naturally into users' communication workflows. This also applies to our work in Chapter 4 especially when presenting the privacy levels to users. In particular, the new designed educational materials should be validated with broader demographics and in situations when learning about E2EE is not the user's primary task.

Also, future work could examine how to tie these high-level mental models more directly to concrete tasks such as choosing a communication medium, turning on E2EE mode (when not automated), or performing an authentication ceremony, so that the community will have better insights about how improved mental models can potentially enable more adoption and effective use of end-to-end encrypted communication tools.

Including authentication ceremony as part of the evaluation. As the first step, our studies didn't consider authentication ceremonies when evaluating users' perceptions of and attitudes toward end-to-end encrypted communication. Therefore, users' opinions of usability and the sense of security might change if they are exposed to performing authentication ceremonies within such tools. There are several studies focusing on helping users complete the authentication ceremony in these tools [6, 36, 37, 61]. However, these work either solely considered the usability of ceremonies, or explained the reasons of performing this action very briefly to participants. Thus, future work could consider including authentication ceremonies on the basis of our studies, when evaluating the usability and security of encrypted communication tools, and/or designing educational materials.

Evaluating the tradeoffs between end-to-end encryption and other concerns. This dissertation focuses on how end-to-end encrypted communication could help protect users' online privacy. There are other possible tradeoffs we didn't evaluate, which future work can examine more closely. For example, there is still ongoing debate about whether the benefits of adopting end-to-end encryption will be outweighed by the threats to the national security [145]; whether the daily use of end-to-end encryption is considered illicit, immoral or "paranoid", except for protecting privacy; and whether end-to-end encryption will get in the way of efficient spam and malware detection within email and messaging tools. Better understanding those tradeoffs will give the whole community a holistic view.

Appendix A: Key Management Lab Study

This appendix contains the full survey and instructional instrument used in our research.

- Section A.1 introduces the task and role-play to the participant.
- Section A.2 contains the introduction and explanation of the Exchange Model.
- Section A.3 contains the introduction and explanation of the Registration Model.
- Section A.4 contains the post-task survey instrument.
- Section A.5 contains the demographic questionnaire.

A.1 Overall Introduction

Welcome to our experiment. Today you will use two systems. These systems are developed to encrypt your emails so that your emails can be protected from being read by email providers (such as Google and Yahoo!), governments (e.g. NSA), as well as malicious attackers.

In this experiment, **pretend you are Henry**, and you want to send and receive encrypted emails to some people. Below are email addresses you may use in this experiment.

- Henry: researchmessage@gmail.com
- Henry2: researchmessage2@gmail.com
- Alice: alice.recipient@gmail.com
- Bob: bobby.recipient@gmail.com
- Carl: carl.recipient@gmail.com

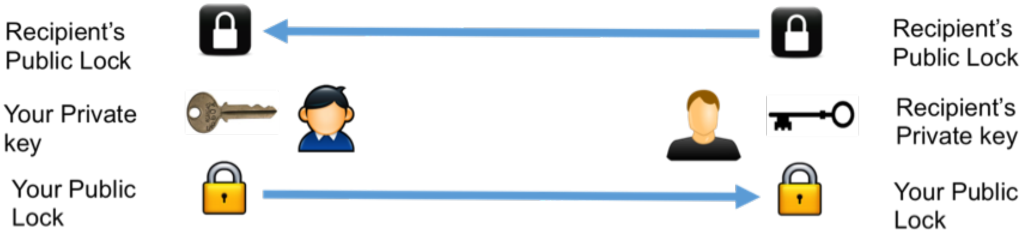
A.2 Exchange Model

Below is how *Lock Exchange System* works.

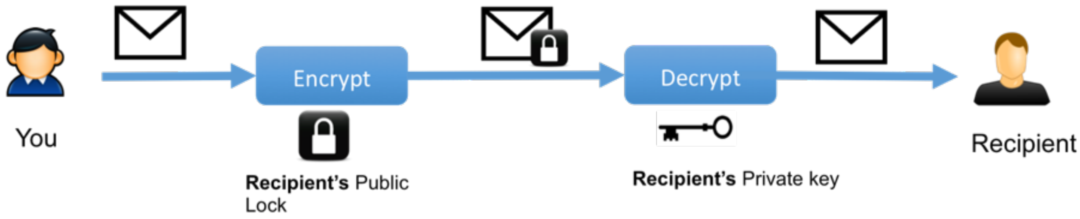
1. Every user can get a public lock and a private key.

Your Public Lock
Your Private key
Recipient's Public Lock
Recipient's Private key

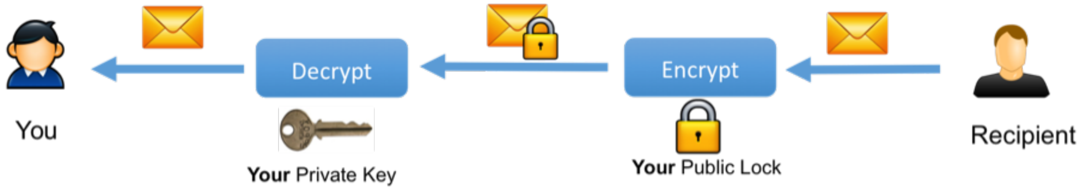
2. Users have to exchange their public locks in some way.



3. You can send encrypted emails with others' public locks, so that others' can read the emails with their private keys.

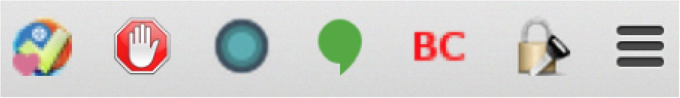


4. Similarly, you can also read any encrypted emails that are encrypted to you using your private key.

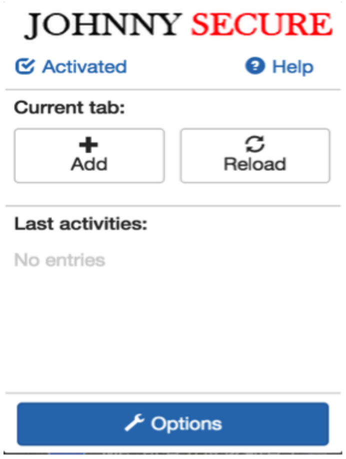


Task Instructions:

- Click the extension on upper right corner on tool bar in Chrome.



- Click "Options" for configuration.



1. Generate a public lock/private key pair.

   Go to “Generate Lock and Key” to generate a **public lock/ private key pair**.

   Note: The password is only for this study, and is NOT your email password. **DON’T** use your real passwords associated with any of your account in real life.

2. Exchange Public Locks with Alice.

   (a) Go to “Display Lock/Key Pair” and click the lock/key pair you just generated. Then export your public lock to Alice.

   The public lock will **start with** “-----BEGIN PGP PUBLIC LOCK BLOCK-----”, and **end with** “-----END PGP PUBLIC LOCK BLOCK-----” (Note: there are FIVE “-” in the beginning and in the end).

   You can send your public lock by one or combination of ways that we **provide** you.

   (b) Then you will receive Alice’s public lock.

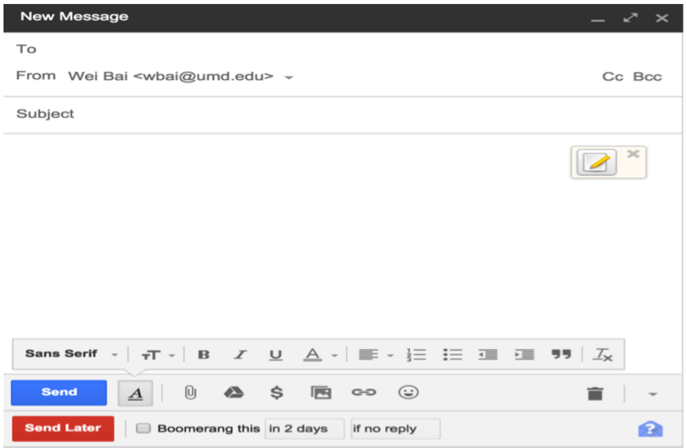
   (c) Import Alice’s public lock into the extension.

3. Send an encrypted email to Alice

   In the email interface, first click the encryption icon to write “What is your favorite color” to Alice. If the icon doesn’t show up, please refresh the website.

   Note: you need to encrypt for Alice.

4. Decrypt the received email from Alice.



From Wei Bai <wbai@umd.edu>

Move your mouse to the email body. When a lock icon appears, click on the icon. You need your password (you created in step 3) to decrypt email.

Next you will send encrypted email to two recipients Bob and Carl.

5. Exchange Public Locks with Bob and Carl.

   You can use the same way or different way provided in step 4 to exchange public locks with Bob and Carl.

6. Send encrypted email to Bob and Carl.

   Imagine that you are a financial secretary in your department, and you want to send the payroll reports to Bob and Carl by encrypted email. For simplicity, you can simply write "Here is your biweekly payroll summary: Salary is $888.88, Tax is $88.88. Your subtotal: $800.00." in the email body. You can refer to previous steps to send encrypted email.

7. Decrypt the received email from Bob and Carl.

8. Imagine that you are still the financial secretary in your department, and you

will send the payroll reports to 10 people by encrypted email, what will you do? Please specify the steps.

9. Misconfiguration

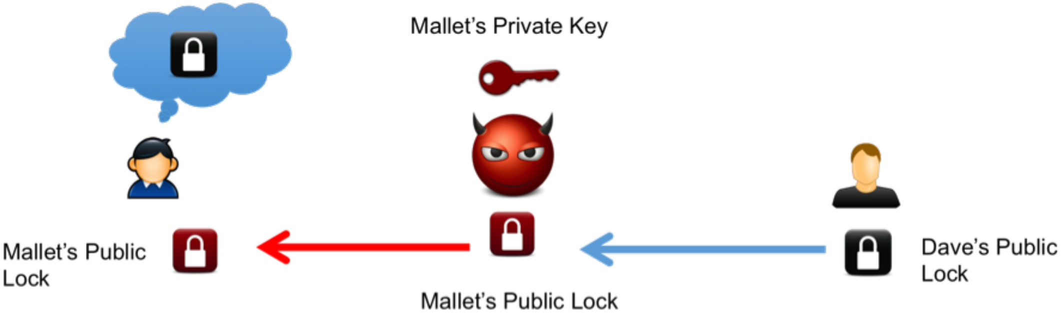
   (a) If you accidentally delete or lose Alice's public lock, what will you do if you want to send/receive encrypted email to/from Alice?

   (b) If you accidentally delete or lose your own private key, what will you do if you want to send/receive encrypted email to/from other recipients?

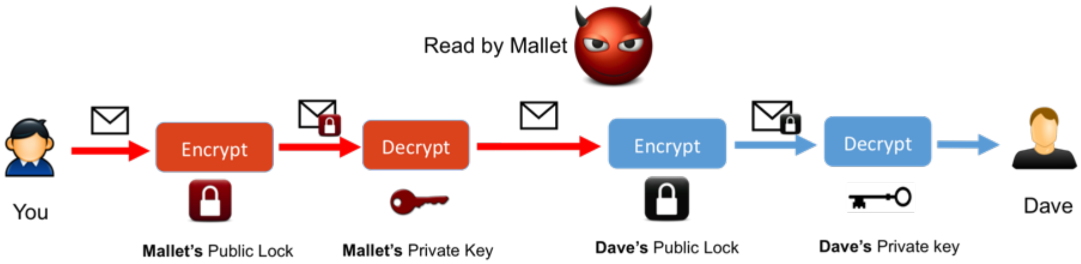
   (c) If you accidentally publicize your own private key, what will you do if you want to send/receive encrypted email to/from other recipients?

Possible Threats for *Lock Exchange System*:

These systems are developed to encrypt your emails so that your emails can be protected from being read by email providers (such as Google and Yahoo!), governments (e.g. NSA), as well as malicious attackers.



The threat may happen when you exchange public locks with others. When you try to get the public lock from Dave, Mallet (can be any type of attacker from above) secretly switches the public lock to his own. You think you get Dave's public lock, but in fact you get Mallet's.



Then when you send encrypted email to Dave, you actually use Mallet's public lock. As a result, Mallet can read your email. Mallet will consequently use Dave's public lock and send the encrypted email to Dave, so that both you and Dave don't realize the email has been read.

This threat doesn't happen usually, because it requires Mallet to have much power and resources to achieve this.

Please give your feedback about *Lock Exchange System:*

Note: We are evaluating these systems. We are not testing you. These systems are not developed by us. Please leave your feedback as honestly as you can. Your honest feedback, positive or negative, will help with our research.

For the first two questions, please note the difference between difficulty and cumbersomeness. Difficult tasks are intellectually challenging and need effort or skills to accomplish. Cumbersome tasks are tedious and need an unnecessarily long time to accomplish.

Please rate your agreement with the following statements.

1. The following tasks were difficult.

   (a) Generate the public lock and private key pair

   (b) Exchange public lock with Alice

(c) Send encrypted email to Alice

(d) Decrypt email from Alice

(e) Exchange public locks with Bob and Carl

(f) Send encrypted email to Bob and Carl

(g) Decrypt email from Bob and Carl

(h) Send and receive encrypted emails to 10 people

2. The following tasks were cumbersome.

   (a) Generate the public lock and private key pair

   (b) Exchange public locks with Alice

   (c) Send encrypted email to Alice

   (d) Decrypt email from Alice

   (e) Exchange public locks with Bob and Carl

   (f) Send encrypted email to Bob and Carl

   (g) Decrypt email from Bob and Carl

   (h) Send and receive encrypted emails to 10 people

3. This system effectively protected my privacy.

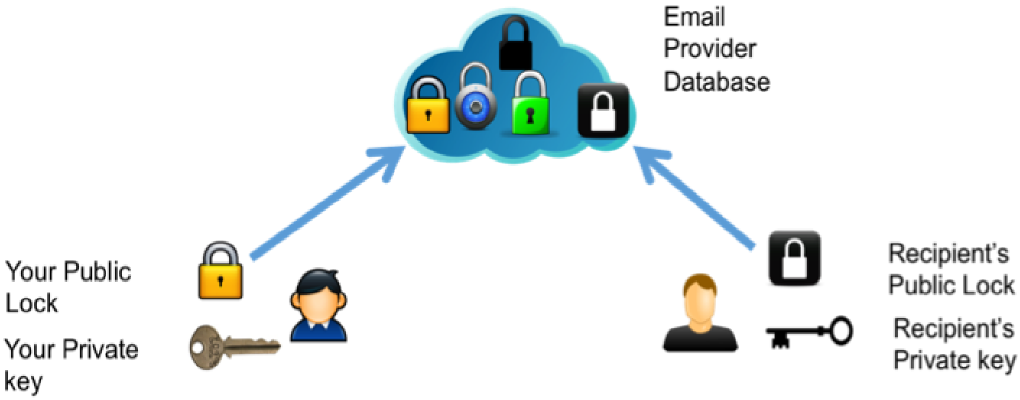
A.3 Registration Model

Instruction: Below is how *Registration System* works.

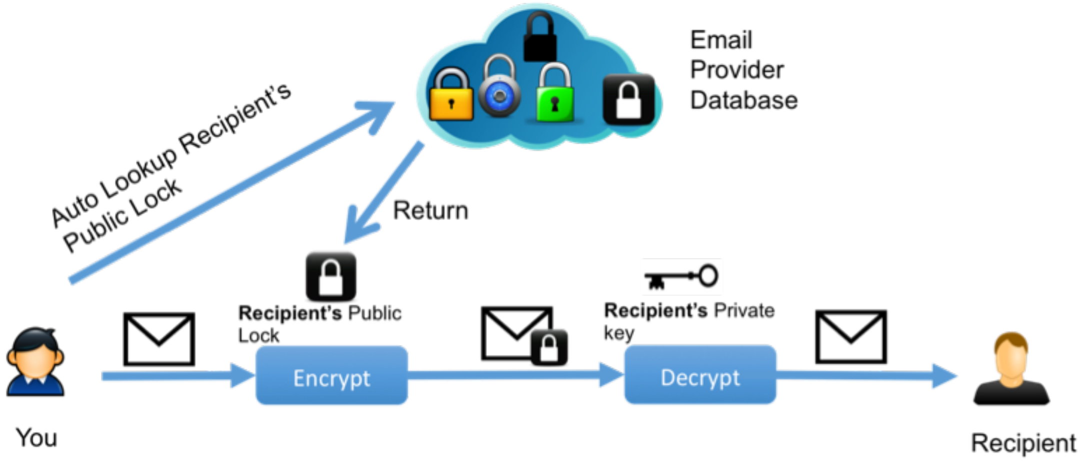
1. Every user can get a public lock and a private key when you register.

Your Public Lock
Your Private key
Recipient's Public Lock
Recipient's Private key

2. Every user's public lock will be automatically stored in a cloud database that is run by the email provider.

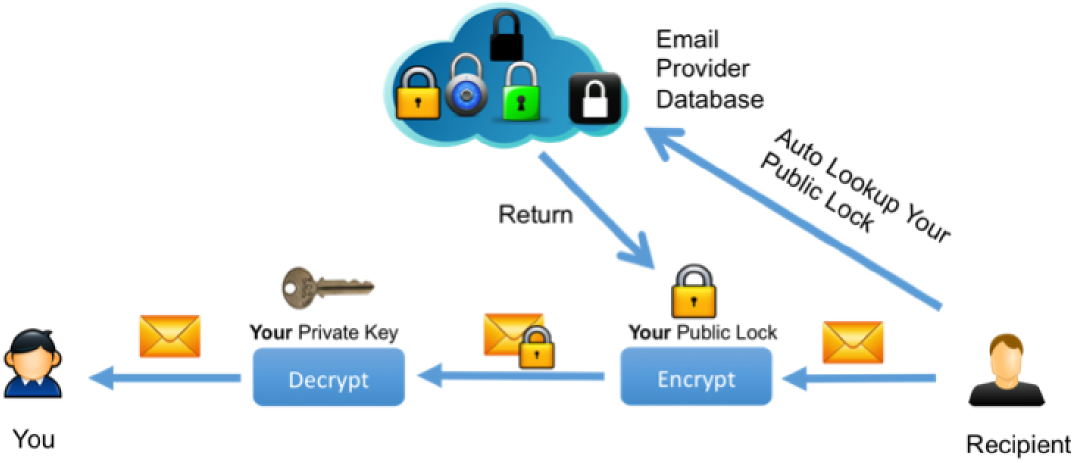


3. You can send encrypted emails with others' public locks, so that others' can read the emails with their private keys. The cloud database will return others' public locks for you.



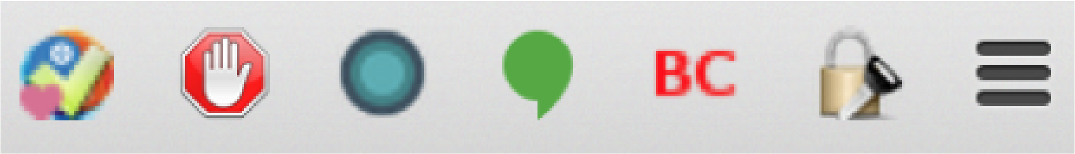
4. Similarly, you can also read any encrypted emails that are encrypted to you

using your private key.

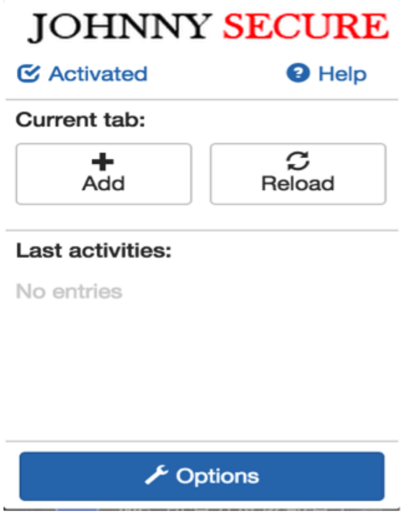


Task Instructions:

- Click the extension on the upper right corner on the tool bar in Chrome.



- Click "Options" for configuration.



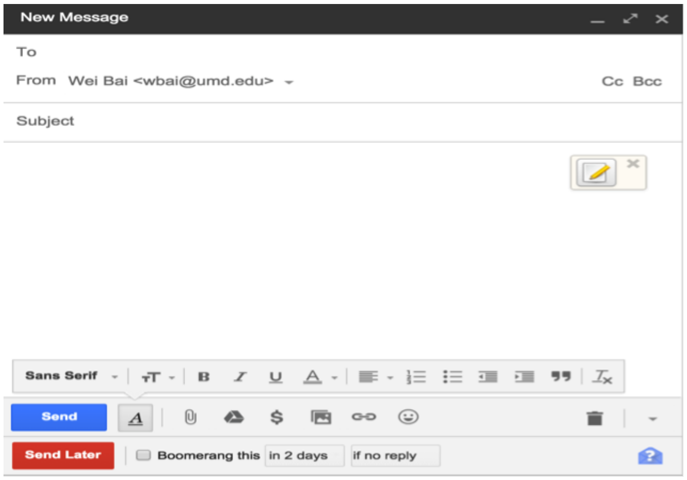
1. Register

Go to “Register” to register your email account to the email provider server. The registration will give you a public lock and a private key.

2. Send an encrypted email to Alice

   In the email interface, first click the encryption icon to write “What is your favorite color” to Alice. If the icon doesn’t show up, please refresh the website.

   Note: you need to encrypt for Alice.



From Wei Bai <wbai@umd.edu>

3. Decrypt the received email from Alice

   You need your password (you created in step 3) to decrypt email.

   Next you will send encrypted email to two recipients Bob and Carl.

4. Send encrypted email to Bob and Carl.

   Imagine that you are a financial secretary in your department, and you want to send the payroll reports to Bob and Carl by encrypted email. For simplicity, you can simply write “Here is your biweekly payroll summary: Salary is

$888.88, Tax is $88.88. Your subtotal: $800.00." in the email body. You can refer to previous steps to send encrypted email.

5. Decrypt the received email from Bob and Carl

6. Imagine that you are still the financial secretary in your department, and you will send the payroll reports to 10 people by encrypted email, what will you do? Please specify the steps.

7. Misconfiguration

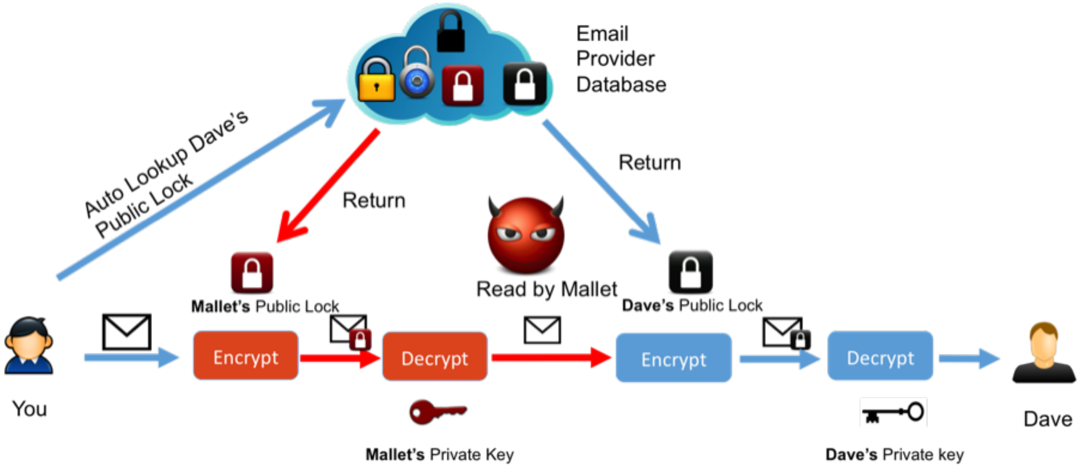
   (a) If you accidentally delete or lose your own private key, what will you do if you want to send/receive encrypted email to/from other recipients?

   (b) If you accidentally publicize your own private key, what will you do if you want to send/receive encrypted email to/from other recipients?

Possible Threats for *Registration System*:

These systems are developed to encrypt your emails so that your emails can be protected from being read by email providers (such as Google and Yahoo!), governments (e.g. NSA), as well as malicious attackers.

There are two prototypes for *Registration System.* For the first prototype (Model 1), the possible threats are as follows.



The threat may happen when you send encrypted emails to others. For example, when you try to send encrypted emails to Dave, you think the email provider database will return Dave's public lock to you. But in fact it returns Mallet's, so that Mallet can read your email. Therefore, you need to trust the email provider in this system.

In the second prototype (Model 2), there is a third-party service (not the email provider) as an intermediary. In this prototype, neither the third-party service nor your email provider can read your email themselves. However, if your email provider and the third-party service collaborate, they can both read your email. Therefore, you need to trust that the two services are not collaborating.

Please give your feedback about *Registration System*:

Note: We are evaluating these systems. We are not testing you. These systems are not developed by us. Please leave your feedback as honestly as you can. Your honest feedback, positive or negative, will help with our research.

For the first two questions, please note the difference between difficulty and cumbersomeness. Difficult tasks are intellectually challenging and need some effort or skills to accomplish. Cumbersome tasks are tedious and need an unnecessarily long time to accomplish.

Rate your agreement with the following statements.

1. The following tasks were difficult.

   (a) Register

   (b) Send encrypted email to Alice

   (c) Decrypt email from Alice

   (d) Send encrypted email to Bob and Carl

   (e) Decrypt email from Bob and Carl

   (f) Send and receive encrypted emails to 10 people

2. The following tasks were cumbersome.

   (a) Register

   (b) Send encrypted email to Alice

   (c) Decrypt email from Alice

   (d) Send encrypted email to Bob and Carl

   (e) Decrypt email from Bob and Carl

   (f) Send and receive encrypted emails to 10 people

3. This system effectively protected my privacy.

A.4 Overall Feedback

Please give your overall feedback about these two systems:

Note: Again, please give your honest feedback to help with our research.

1. Please rate your willingness to use these two systems in the future.

   (a) I would like to use *Lock Exchange System*.

   (b) I would like to use *Registration System* with Model 1.

   (c) I would like to use *Registration System* with Model 2.

2. Below please rate your willingness to recommend these systems to others.

   (a) I would like to recommend *Lock Exchange System* to others.

   (b) I would like to recommend *Registration System* with Model 1 to others.

   (c) I would like to recommend *Registration System* with Model 2 to others.

3. Please rate your agreement with the following statements.

   (a) I think that I would need the support of a technical person to be able to use Lock Exchange System.

   (b) I think that I would need the support of a technical person to be able to use Registration System.

   (c) I would imagine that most people would learn to use Lock Exchange System very quickly.

(d) I would imagine that most people would learn to use Registration System very quickly.

(e) I would need to learn a lot of things before I could get going with Lock Exchange System.

(f) I would need to learn a lot of things before I could get going with Registration System.

4. What do you like or dislike for each system? Why?

In Model 3, the email provider will still store all users' public locks, just like Model 1. But there are other parties (auditors) who audit the email provider, to ensure that the email provider is giving out correct public locks. These auditors may include other email providers, public interest groups, and software on your devices. If the email provider gives you a public lock that doesn't belong to the recipient, or gives someone else the wrong public lock for you, these parties will notify you. You (or someone else) may use the wrong lock temporarily (for an hour or a day) before you are notified.

In this model, you don't need to trust any email provider, but you need to trust the auditors and/or the software on your device. Because there are several auditors, even if one auditor does not alert you another one probably will.

A.5 Demographics

1. Which of the following best describes your current occupation?

   (a) Healthcare Practitioners and Technical Occupations

   (b) Office and Administrative Support Occupations

   (c) Production Occupations

   (d) Farming, Fishing, and Forestry Occupations

   (e) Computer and Mathematical Occupations

   (f) Community and Social Service Occupations

   (g) Life, Physical, and Social Science Occupations

   (h) Management Occupations

   (i) Legal Occupations

   (j) Installation, Maintenance, and Repair Occupations

   (k) Food Preparation and Serving Related Occupations

   (l) Architecture and Engineering Occupations

   (m) Arts, Design, Entertainment, Sports, and Media Occupations

   (n) Building and Grounds Cleaning and Maintenance Occupations

   (o) Healthcare Support Occupations

   (p) Construction and Extraction Occupations

(q) Education, Training, and Library Occupations

(r) Protective Service Occupations

(s) Sales and Related Occupations

(t) Business and Financial Operations Occupations

(u) Transportation and Materials Moving Occupations

(v) Other (please specify)

2. Where did you grow up (primarily)?

(a) United States

(b) Other North America

(c) South or Central America

(d) Western Europe

(e) Eastern Europe

(f) Africa

(g) South Asia (India, Bangladesh, Pakistan, etc.)

(h) East Asia (China, Japan, Korea, etc.)

(i) Central Asia

(j) The Middle East

(k) Australia / Oceania

(l) Other: [please specify]

(m) I prefer not to answer

3. What is your age?

   (a) 18-20

   (b) 21-24

   (c) 25-34

   (d) 35-44

   (e) 45-54

   (f) Above 54

   (g) I prefer not to answer

4. What is your gender?

   (a) Male

   (b) Female

   (c) I prefer not to answer

5. Please tell us whether you have the following experiences (yes or no).

   (a) I have attended a computer security conference in the past year.

   (b) I have taken or taught a course in computer security before.

   (c) Computer security is one of my primary job responsibilities.

   (d) I have used SSH before.

(e) I have configured a firewall before.

(f) I have a degree in an IT-related field (e.g. information technology, computer science, electrical engineering, etc.)?

(g) I have an up-to-date virus scanner on my computer.

Appendix B: Email Preference Study

Features	**Feature Descriptions**	**Options**
Price	One-time fee for signing up for the service	**$0.00** **$1.99**
Multi-word Search	Can you search using multiple words, for example, "home depot"?	**Yes** **No**
Partial-word Search	Can you search with a partial word instead of a complete word, e.g., "amaz" vs "amazon"?	**Yes** **No**
Privacy	What can your email provider learn about your email?	**No privacy**: Your email provider can read the contents of all email and search queries. This is how most email services currently work (Gmail, Yahoo! Mail, Outlook, etc.). **Some privacy**: Your email provider can read the contents of certain emails and search queries, but not all. The provider can choose specific topics of high interest to learn about. **Maximum privacy**: Your email provider cannot read the contents of any emails or search queries.
Local storage	How much local storage the service will use (on your computer or phone)	**Requires 5MB**: equivalent to about 2-3 HD photos **Requires 500 MB**: equivalent to about 200 HD photos or 20 mobile apps
Syncing old email to a new device	After using this email service on one device (a phone or laptop) for several months, you buy a new device. You set up the email service on your new device. Can you read and search old emails on your new device?)	**Yes**: read and search all email using the new device both before and after its activation. **No**: read and search only email after you configured the new device. You can?t read and search old emails on your new device.

Table B.1: Details of feature description in email preference study

B.1 Survey Questionnaire

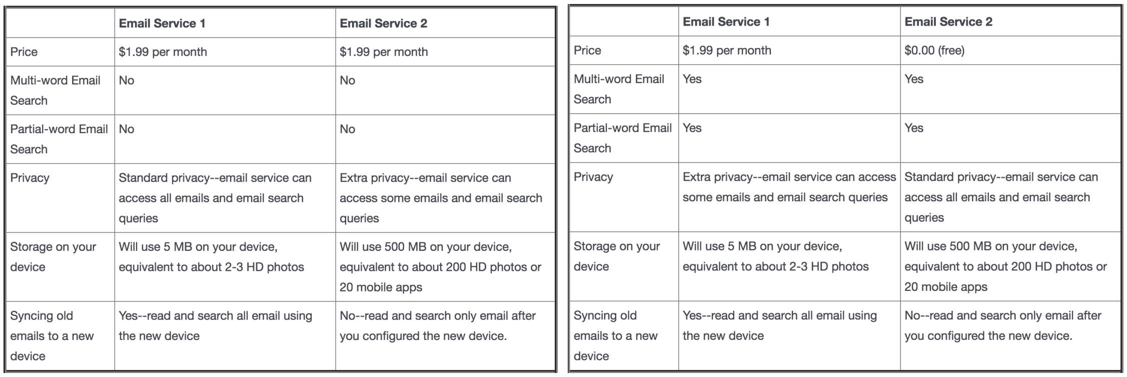
In this section, please imagine that you have been asked to recommend an email service to a friend. In each of the following 16 questions, you will be provided with descriptions of two different email services, which may differ in several features. We will ask you to choose **which email service you would recommend**.

Some of the email services you are going to see are not currently available, but we'd like you to **imagine that they were available today**. It is important that you answer in the way you would if you were **actually recommending email services**.

The details of feature description are shown in Table B.

B.2 Screenshots of Email Preference

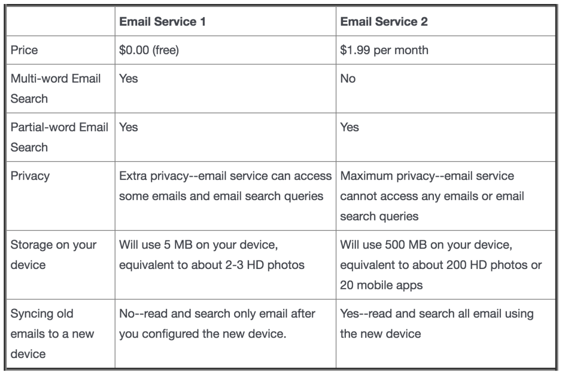
This section contains the full 16 email service choice questions in our study. During the survey, the sequence of questions was randomized for each participant.



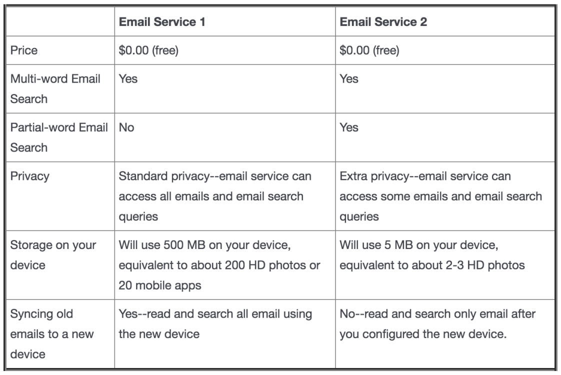
	Email Service 1	Email Service 2
Price	$1.99 per month	$1.99 per month
Multi-word Email Search	No	No
Partial-word Email Search	No	No
Privacy	Standard privacy--email service can access all emails and email search queries	Extra privacy--email service can access some emails and email search queries
Storage on your device	Will use 5 MB on your device, equivalent to about 2-3 HD photos	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps
Syncing old emails to a new device	Yes--read and search all email using the new device	No--read and search only email after you configured the new device.

	Email Service 1	Email Service 2
Price	$1.99 per month	$0.00 (free)
Multi-word Email Search	Yes	Yes
Partial-word Email Search	Yes	Yes
Privacy	Extra privacy--email service can access some emails and email search queries	Standard privacy--email service can access all emails and email search queries
Storage on your device	Will use 5 MB on your device, equivalent to about 2-3 HD photos	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps
Syncing old emails to a new device	Yes--read and search all email using the new device	No--read and search only email after you configured the new device.

Figure B.2.1: Question 1 (left) and Question 2 (right)

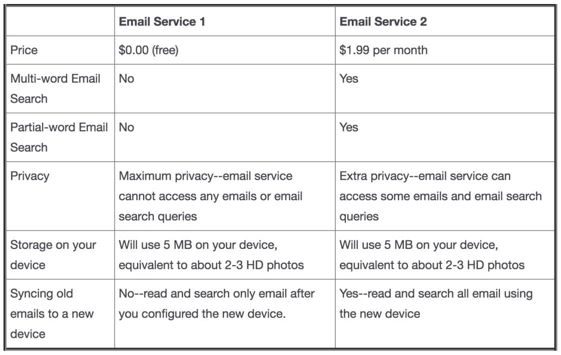


	Email Service 1	Email Service 2
Price	$0.00 (free)	$1.99 per month
Multi-word Email Search	Yes	No
Partial-word Email Search	Yes	Yes
Privacy	Extra privacy--email service can access some emails and email search queries	Maximum privacy--email service cannot access any emails or email search queries
Storage on your device	Will use 5 MB on your device, equivalent to about 2-3 HD photos	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps
Syncing old emails to a new device	No--read and search only email after you configured the new device.	Yes--read and search all email using the new device

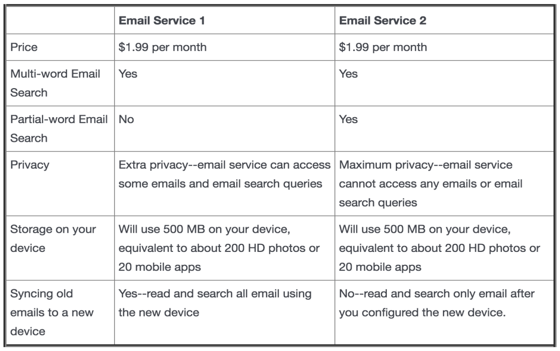


	Email Service 1	Email Service 2
Price	$0.00 (free)	$0.00 (free)
Multi-word Email Search	Yes	Yes
Partial-word Email Search	No	Yes
Privacy	Standard privacy--email service can access all emails and email search queries	Extra privacy--email service can access some emails and email search queries
Storage on your device	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps	Will use 5 MB on your device, equivalent to about 2-3 HD photos
Syncing old emails to a new device	Yes--read and search all email using the new device	No--read and search only email after you configured the new device.

Figure B.2.2: Question 3 (left) and Question 4 (right)

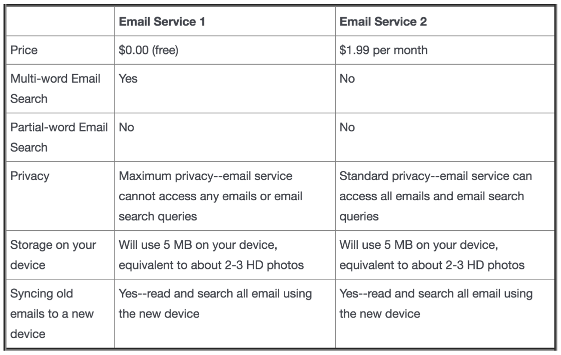


	Email Service 1	Email Service 2
Price	$0.00 (free)	$1.99 per month
Multi-word Email Search	No	Yes
Partial-word Email Search	No	Yes
Privacy	Maximum privacy--email service cannot access any emails or email search queries	Extra privacy--email service can access some emails and email search queries
Storage on your device	Will use 5 MB on your device, equivalent to about 2-3 HD photos	Will use 5 MB on your device, equivalent to about 2-3 HD photos
Syncing old emails to a new device	No--read and search only email after you configured the new device.	Yes--read and search all email using the new device

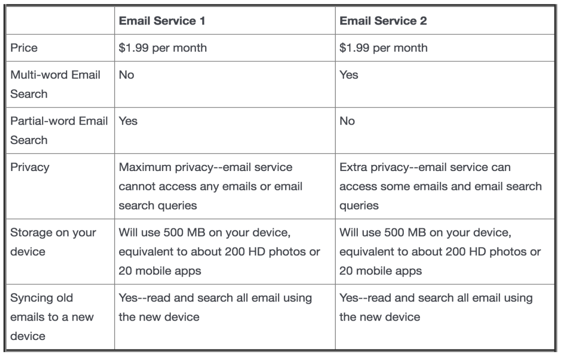


	Email Service 1	Email Service 2
Price	$1.99 per month	$1.99 per month
Multi-word Email Search	Yes	Yes
Partial-word Email Search	No	Yes
Privacy	Extra privacy--email service can access some emails and email search queries	Maximum privacy--email service cannot access any emails or email search queries
Storage on your device	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps
Syncing old emails to a new device	Yes--read and search all email using the new device	No--read and search only email after you configured the new device.

Figure B.2.3: Question 5 (left) and Question 6 (right)

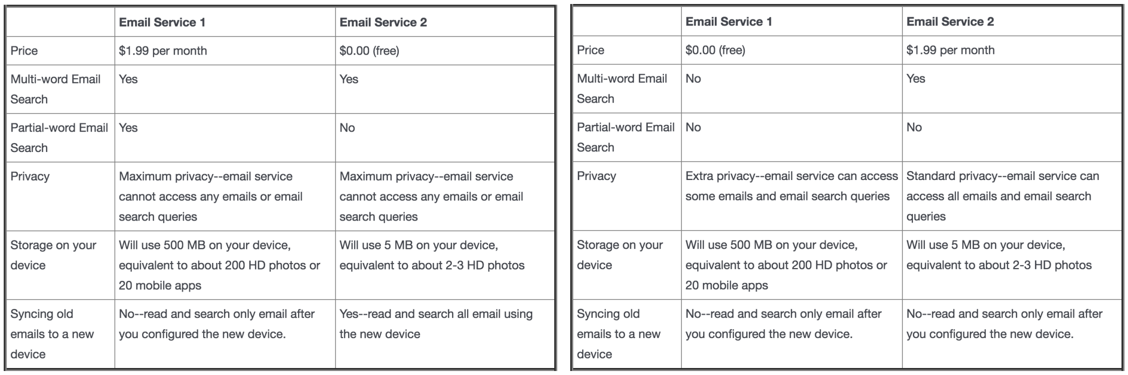


	Email Service 1	Email Service 2
Price	$0.00 (free)	$1.99 per month
Multi-word Email Search	Yes	No
Partial-word Email Search	No	No
Privacy	Maximum privacy--email service cannot access any emails or email search queries	Standard privacy--email service can access all emails and email search queries
Storage on your device	Will use 5 MB on your device, equivalent to about 2-3 HD photos	Will use 5 MB on your device, equivalent to about 2-3 HD photos
Syncing old emails to a new device	Yes--read and search all email using the new device	Yes--read and search all email using the new device



	Email Service 1	Email Service 2
Price	$1.99 per month	$1.99 per month
Multi-word Email Search	No	Yes
Partial-word Email Search	Yes	No
Privacy	Maximum privacy--email service cannot access any emails or email search queries	Extra privacy--email service can access some emails and email search queries
Storage on your device	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps
Syncing old emails to a new device	Yes--read and search all email using the new device	Yes--read and search all email using the new device

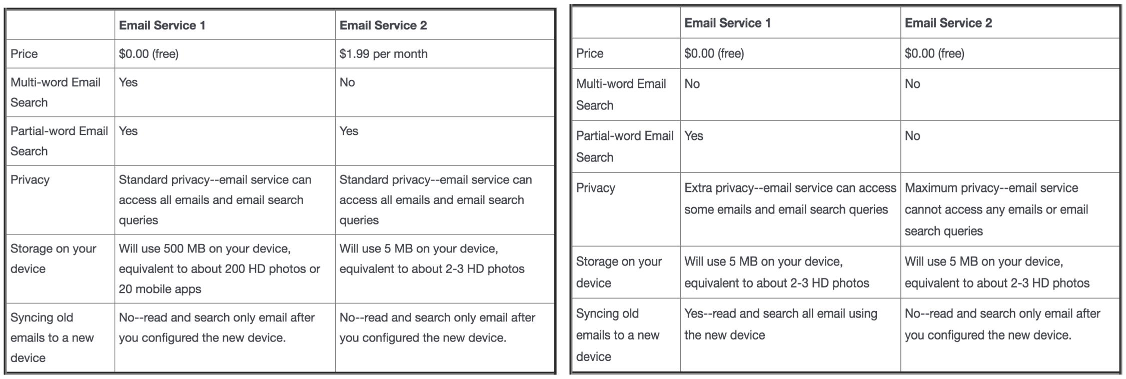
Figure B.2.4: Question 7 (left) and Question 8 (right)



	Email Service 1	Email Service 2
Price	$1.99 per month	$0.00 (free)
Multi-word Email Search	Yes	Yes
Partial-word Email Search	Yes	No
Privacy	Maximum privacy--email service cannot access any emails or email search queries	Maximum privacy--email service cannot access any emails or email search queries
Storage on your device	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps	Will use 5 MB on your device, equivalent to about 2-3 HD photos
Syncing old emails to a new device	No--read and search only email after you configured the new device.	Yes--read and search all email using the new device

	Email Service 1	Email Service 2
Price	$0.00 (free)	$1.99 per month
Multi-word Email Search	No	Yes
Partial-word Email Search	No	No
Privacy	Extra privacy--email service can access some emails and email search queries	Standard privacy--email service can access all emails and email search queries
Storage on your device	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps	Will use 5 MB on your device, equivalent to about 2-3 HD photos
Syncing old emails to a new device	No--read and search only email after you configured the new device.	No--read and search only email after you configured the new device.

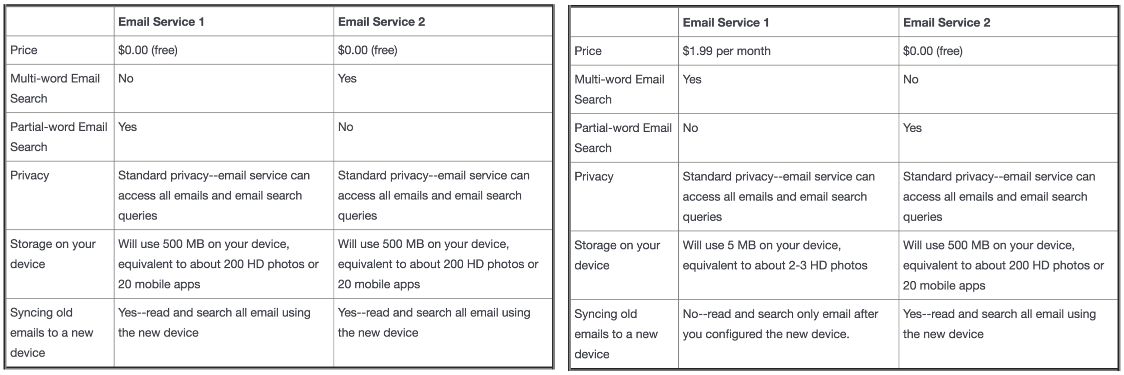
Figure B.2.5: Question 9 (left) and Question 10 (right)



	Email Service 1	Email Service 2
Price	$0.00 (free)	$1.99 per month
Multi-word Email Search	Yes	No
Partial-word Email Search	Yes	Yes
Privacy	Standard privacy--email service can access all emails and email search queries	Standard privacy--email service can access all emails and email search queries
Storage on your device	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps	Will use 5 MB on your device, equivalent to about 2-3 HD photos
Syncing old emails to a new device	No--read and search only email after you configured the new device.	No--read and search only email after you configured the new device.

	Email Service 1	Email Service 2
Price	$0.00 (free)	$0.00 (free)
Multi-word Email Search	No	No
Partial-word Email Search	Yes	No
Privacy	Extra privacy--email service can access some emails and email search queries	Maximum privacy--email service cannot access any emails or email search queries
Storage on your device	Will use 5 MB on your device, equivalent to about 2-3 HD photos	Will use 5 MB on your device, equivalent to about 2-3 HD photos
Syncing old emails to a new device	Yes--read and search all email using the new device	No--read and search only email after you configured the new device.

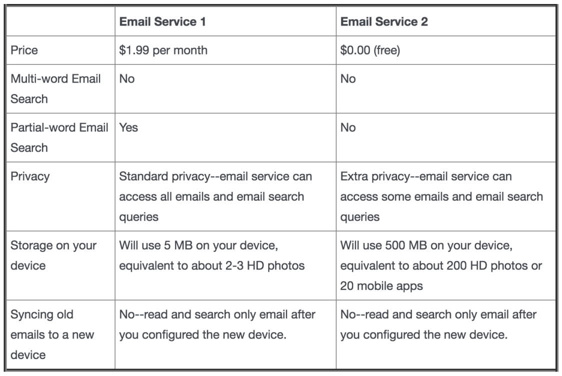
Figure B.2.6: Question 11 (left) and Question 12 (right)



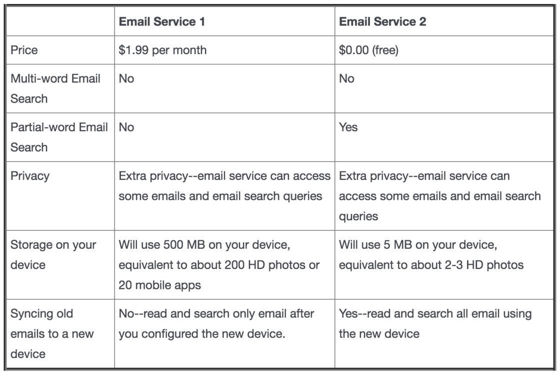
	Email Service 1	Email Service 2
Price	$0.00 (free)	$0.00 (free)
Multi-word Email Search	No	Yes
Partial-word Email Search	Yes	No
Privacy	Standard privacy--email service can access all emails and email search queries	Standard privacy--email service can access all emails and email search queries
Storage on your device	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps
Syncing old emails to a new device	Yes--read and search all email using the new device	Yes--read and search all email using the new device

	Email Service 1	Email Service 2
Price	$1.99 per month	$0.00 (free)
Multi-word Email Search	Yes	No
Partial-word Email Search	No	Yes
Privacy	Standard privacy--email service can access all emails and email search queries	Standard privacy--email service can access all emails and email search queries
Storage on your device	Will use 5 MB on your device, equivalent to about 2-3 HD photos	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps
Syncing old emails to a new device	No--read and search only email after you configured the new device.	Yes--read and search all email using the new device

Figure B.2.7: Question 13 (left) and Question 14 (right)



	Email Service 1	Email Service 2
Price	$1.99 per month	$0.00 (free)
Multi-word Email Search	No	No
Partial-word Email Search	Yes	No
Privacy	Standard privacy--email service can access all emails and email search queries	Extra privacy--email service can access some emails and email search queries
Storage on your device	Will use 5 MB on your device, equivalent to about 2-3 HD photos	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps
Syncing old emails to a new device	No--read and search only email after you configured the new device.	No--read and search only email after you configured the new device.



	Email Service 1	Email Service 2
Price	$1.99 per month	$0.00 (free)
Multi-word Email Search	No	No
Partial-word Email Search	No	Yes
Privacy	Extra privacy--email service can access some emails and email search queries	Extra privacy--email service can access some emails and email search queries
Storage on your device	Will use 500 MB on your device, equivalent to about 200 HD photos or 20 mobile apps	Will use 5 MB on your device, equivalent to about 2-3 HD photos
Syncing old emails to a new device	No--read and search only email after you configured the new device.	Yes--read and search all email using the new device

Figure B.2.8: Question 15 (left) and Question 16 (right)

B.3 Web-Skill Scale and Privacy Perception

1. Web-Skill Scale

   In this section, please tell us how familiar you are with the following computer and Internet-related items. Please choose a number between 1 and 5, where 1 represents no understanding and 5 represents full understanding of the item.

   (a) Advanced Search

   (b) PDF

   (c) Spyware

   (d) Wiki

   (e) Cache

   (f) Phishing

2. Privacy Perception

   In this section, please tell us how much you agree with the following statements. Please choose a number between 1 and 7, where 1 represents "strongly disagree" and 7 represents "strongly agree".

(a) Consumer online privacy is really a matter of consumers? right to exercise control and autonomy over decisions about how their information is collected, used, and shared.

(b) Consumer control of personal information lies at the heart of consumer privacy.

(c) I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.

(d) Companies seeking information online should disclose the way the data are collected, processed, and used.

(e) A good consumer online privacy policy should have a clear and conspicuous disclosure.

(f) It is very important to me that I am aware and knowledgeable about how my personal information will be used.

(g) It usually bothers me when online companies ask me for personal information.

(h) When online companies ask me for personal information, I sometimes think twice before providing it.

(i) It bothers me to give personal information to so many online companies.

(j) I'm concerned that online companies are collecting too much personal information about me.

B.4 Demographics

There are 6 questions about your demographics.

1. Please specify the gender with which you most closely identify.

   (a) Male

   (b) Female

   (c) Other

   (d) Prefer not to answer

2. Please specify your age? ______________ (number)

3. Please specify your ethnicity.

   (a) Hispanic or Latino

   (b) Black or African American

   (c) White

   (d) American Indian or Alaska Native

   (e) Asian, Native Hawaiian, or Pacific Islander

   (f) Other

   (g) Prefer not to answer.

4. Please specify the highest degree or level of school you have completed.

(a) Some high school credit, no diploma or equivalent

(b) High school graduate, diploma or the equivalent (for example: GED)

(c) Some college credit, no degree

(d) Trade/technical/vocational training

(e) Associate degree

(f) Bachelor's degree

(g) Master's degree

(h) Professional degree

(i) Doctorate degree

(j) Prefer not to answer.

5. Which of the following best describes your educational background or job field?

   (a) I have an education in, or work in, the field of computer science, computer engineering or IT.

   (b) I DO NOT have an education in, nor do I work in, the field of computer science, computer engineering or IT.

   (c) Prefer not to answer.

6. Please specify the range which most closely matches your total, pre-tax, household income in 2016.

   (a) <$29,999

   (b) $30,000 - $49,999

(c) \$50,000 - \$74,999

(d) \$75,000 - \$99,999

(e) \$100,000 - \$124,999

(f) \$125,000 - \$149,999

(g) \$150,000 - \$199,999

(h) \$200,000 or more

(i) Prefer not to answer.

Appendix C: End-to-End Encryption Education Study

C.1 Quiz Questions

Suppose TextLight is a messaging app which has end-to-end encryption (E2EE). You send a message to your friend, Bob, using TextLight, to invite him to watch the movie *Star Wars* tonight. Please answer the following questions based on your understanding of end-to-end encryption (E2EE). [Note: all questions except Q9 were five-point Likert-scale choice questions: “Very difficult,” “Somewhat difficult,” “Neutral,” “Somewhat easy,” “Very easy.”]

1. Suppose Dave could observe the communication between your phone and the TextLight company, how difficult would it be for Dave to learn the contents of your invitation message?

2. How difficult would it be for the TextLight company to learn the contents of your invitation message?

3. Consider your Internet or mobile service provider, such as Comcast, Verizon, AT&T, Sprint, etc. How difficult would it be for these service providers to learn the contents of your invitation message?

4. If a hacker, Chuck successfully steals data that is stored in the computers

at the TextLight company, how difficult would it be for Chuck to learn the contents of your invitation message?

5. Some government intelligence or national security agencies (e.g. NSA) request the TextLight company to hand over stored user messages to them. How difficult would it be for these agencies to learn the contents of your invitation message?

6. Suppose George has previously installed some malware on your phone which could record your activities, how difficult would it be for George to learn the contents of your invitation message?

7. How difficult would it be for someone (for example, a hacker) to modify messages between you and Bob during your conversation, so that Bob will receive an invitation to watch the movie *Jurassic Park*, instead of *Star Wars*?

8. Suppose both your and Bob's Textlight usernames and passwords are **not** hacked/stolen/guessed by other people. How difficult would it be for someone (for example, a hacker) to impersonate Bob in order to respond your invitation message? For example, you receive a response message that seems to be from Bob, but was actually sent by Frank.

9. Please sort the following tools based on how secure you feel using them, with the most secure tool at the top.

   (a) Sending messages using SMS text messaging app

   (b) Making a direct landline/mobile phone call

(c) Sending Email

(d) Sending messages in instant messaging apps with E2EE

(e) Sending messages in instant messaging apps without E2EE

C.2 Interview Questions

Now we will ask you some questions about how you feel about these slides.

1. Could you briefly recall what you have learned from our tutorial?

2. How difficult or easy to understand was our tutorial? [Very difficult, difficult, neutral, Easy, Very easy]

3. How informative was our tutorial? [Very non-informative, non-informative, neutral, informative, very informative]

4. What piece of the tutorial you think is most important to you to help you learn E2EE? Why? What about non-important parts?

5. What part of the tutorial you think is most surprising to you? Least surprising? Why?

6. Suppose you want to teach E2EE to your family or friends who don?t know E2EE before, what part of the tutorial do you want them to learn, or should they know? Why?

7. What part of the tutorial you like or dislike, think (not) clear, or (not) well-articulated?

C.3 App Message Critique

Nowadays, some messaging apps also have E2EE. They also try to write some short introductions to their users. Here are some of the examples. Please take some time to read them. We anonymized these app names, and name them all as TextLight [1].

C.3.1 App Messages

APP 1 - Line

Letter Sealing is a feature that provides end-to-end encryption (E2EE) for chat room messages. E2EE is a communication system designed so that messages saved on our servers are encrypted and cannot be read by anyone except the sender and receiver of the message. Letter Sealing uses unique, user-specific encryption keys which allow users to safely and securely send messages to one another.

APP 2 - WhatsApp

Many messaging apps only encrypt messages between you and them, but TextLight's end-to-end encryption ensures only you and the person you're communicating with can read what is sent, and nobody in between, not even TextLight. This is because your messages are secured with a lock, and only the recipient and you have the special key needed to unlock and read them. For added protection, every mes-

[1] We replaced the names of all the apps with Textlight to mitigate effects of seeing certain brand names.

sage you send has its own unique lock and key. All of this happens automatically: no need to turn on settings or set up special secret chats to secure your messages.

APP 3 - Telegram

All messages use end-to-end encryption. This means only you and the recipient can read those messages – nobody else can decipher them, including us here at TextLight. TextLight can help when it comes to data transfer and secure communication. This means that all messages that you send and receive via TextLight cannot be deciphered when intercepted by your ISP, network administrator or other third parties. But please remember that we cannot protect you from your own mother if she takes your unlocked phone without a passcode. Or from your IT-department if they access your computer at work. Or from any other people that get physical or root access to your phones or computers running TextLight.

APP 4 - Viber

On TextLight, end-to-end encryption is always turned on. Encryption keys exist on user devices and nowhere else. So no one but you and the people you're communicating with can see your messages or hear your calls, not even TextLight. The messages you send make their way from your device to the recipient in the form of a code that only the recipient's device can translate to plain text.

When your chats are protected by end-to-end encryption, no one has access to them. Perhaps most importantly, TextLight doesn't have access to them – which means nothing you share can be used to target you later. TextLight can't share what it doesn't have and, since TextLight doesn't have access to the content of your conversations, it can't share it with third. So, you can be sure you won't mysteriously start seeing ads related to something you were just talking about with a friend on TextLight.

APP 5 - Threema

TextLight end-to-end encrypts all your messages. All encryption and decryption happen directly on the device, and the user is in control over the key exchange. This guarantees that no third party – not even the server operators – can decrypt the content of the messages and calls. Only the intended recipient, can read your messages.

TextLight uses two different encryption layers to protect messages between the sender and the recipient.

- End-to-end encryption layer: this layer is between the sender and the recipient.
- Transport layer: each end-to-end encrypted message is encrypted again for transport between the client and the server, in order to protect the header information.

The crucial part is that the end-to-end encryption layer passes through the server uninterrupted; the server cannot remove the inner encryption layer.

APP 6 - ProtonMail

In TextLight, your data is encrypted in a way that makes it inaccessible to us. Data is encrypted on the client side using an encryption key that we do not have access to. This means we don't have the technical ability to decrypt your messages, and as a result, we are unable to hand your data over to third parties. With TextLight, privacy isn't just a promise, it is mathematically ensured.

When you use E2EE to send a message to someone, no one monitoring the network can see the content of your message – not hackers, not the government, and not even the company (e.g. TextLight) that facilitates your communication.

This differs from the encryption that most companies already use, which only protects the data in transit between your device and the company's servers. For example, when you send and receive a message using a service that does not provide E2EE, the company has the ability to access the content of your messages because they also hold the encryption keys. E2EE eliminates this possibility because the service provider does not actually possess the decryption key. Because of this, E2EE is much stronger than standard encryption.

C.3.2 Interview Questions

1. Generally speaking, what do you think of these introductions? [Followup: Do you think these introductions can help general users understand E2EE better?]

2. Please use the green pen to mark the parts you think the introductions are good, and use the red pen to mark the parts you think are not good. [Followup: Why do you think these parts are (not) good?]

3. What else you might like these introductions to tell you?

4. Please choose the best one from these introductions.

C.4 Message Design

Now you have learned our tutorial about E2EE, and have read some tutorials used by some messaging apps. Could you design a short introduction if you want to teach other people about end-to-end encryption? We don't expect you to come up with a long document describing every aspect of E2EE. Instead, please pick the most important pieces you want to convey. Try to come up with the introduction within 200 words.

C.4.1 Participants' Designed Messages

1. **O1:** End-to-end encryption (E2EE) is a process that protects your messages from third parties including but not limited to an individual, your app company or internet service provider. As a result, only the sender and intended recipient of a message can view its contents. E2EE also protects messages from being duplicated, impersonated or modified by third parties. Although E2EE is a step forward in protecting user information, app companies are still researching ways to secure user information when Malware software is detected.

2. **O2:** E2EE is a tech that can protect your messages from any other third party by controlling E2EE process happening directly on the device, so that only the intended recipient can read your messages.

3. **O3:** End-to-end encryption, or E2EE, protects messages in that it only allows

you (the user) and your intended audience to read the message. Data is protected on the user side using an encryption that the messaging app company - or any other third party (including hacker, the government, impersonators, etc.) - have access to, therefore no one else can see the content of the message. E2EE does not, however, protect receivers if malware has been installed in their phone.

4. **O4:** Hey everyone, I want to share some important news about the safe and secure software that can protect you, and your information you pass to another. This software is called E2EE it provides end to end encryption protection with messages and calls are exchanged and not even the providers can see it. However if anyone is looking over your shoulder that the only possible way your information can be shared. Overall this software is definitely something to look into if you have privacy difficulties.

5. **O5:** E2EE is a great way to ensure that your messages will be securely transmitted to the recipient of the message originally intended for. The data is encrypted where no one has directed access to the text contents but the sender and the receiver of the information. Not even the monitoring company, hackers and the government can see the message being sent in the secure way. On particular E2EE apps the encryption is always turned on the be coded and will decode once the message has been fully received by the recipient. This E2EE protects against message modification and impersonation. Not even usernames and or passwords can be stolen or guessed.

6. **OR1:** E2EE is a very useful and secure way of assuring its user's that the contents of their messages cannot be viewed or manipulated in any way, throughout the transit and retrieval of the message. Unlike messaging apps that choose not to use end-to-end encryption, messages with E2EE cannot even be accessed by the app company themselves. As amazing as it may seem, the only possible way for a hacker to access the encrypted information would be if they had the ability to install malware on one's phone.

7. **OR2:** The end-to-end encryption(E2EE) means only you and your intended recipients can read the content of messages. Under non-E2EE situation, there are risks in which your message can be subject to deciphering, interception and modification. The internet service providers can get access to the content of your messages during transit, the app company can can read your messages and hand them to government agency when required. Moreover, a hacker can easily intercept and modify your messages. Using E2EE can eliminate the possibility of leaking the contents of your messages in situations mentioned before by adding a shield to your message so that only you and the recipient can open that shield. More importantly, no message modification and impersonation will take place. However, E2EE can't protect you from shoulder surfing, an unreliable recipient or malware installed on your phone.

8. **OR3:** In TextLight, your data is protected with end-to-end encryption in a way that no one except you and the person you are communicated with can read your messages. This is because each message you send has its own

encrypted lock and key so that not only us (the company) but also the internet service providers and even the government CANNOT decrypt your messages and hand over to third parties. Also, the encryption works automatically and hence there is no need to turn on settings or set up special secrets chats.

9. **OR4:** There are more benefits than risks to using E2EE, or End-to-End Encryption. E2EE mitigates some of the risks message senders are exposed to in every day life while texting their friends, sending invitations through Whatsapp, or communicating in other ways via instant messaging.

   By using E2EE, this process creates a lock and key for your messages. When you send a message using E2EE, the message travels from your Internet Provider, through the messaging app servers, through the recipient's Internet Provider, and to the recipient. The lock prevents hackers, rogue employees, and the app company/IP company themselves from viewing the messages, and only the recipient has the key to unlock these messages. By using E2EE, you decrease the likelihood that someone can hack into your phone. While there are benefits to using E2EE, every day risks still pose a threat, like a thief stealing your phone, someone looking over your shoulder, or if someone installs malware on an unlocked phone.

10. **OR5:** E2EE is exceptionally important in protecting your information. Your information is exposed every time you utilize your mobile device. There are three potential exposures, the service providers, the app company, and hackers. In efforts to protect yourself against these parties please ensure your devices

has E2EE protection. This protection allows you information to remain secure not even the company itself has an encryption key to decode, grant access to other and leave your personal information unsecured. Additionally, one must take precautions against those who shoulder surf and readily giving information/ access to others (giving passwords or forwarding information). E2EE is the best method of protection and all who utilize text messaging services should utilize its services.

11. **OM1:** E2EE is an encryption used for securing your messaging. It sends an signal through your internet, sends to whom your messaging. With a decrypted message only they can see and open.

12. **OM2:** E2EE is a system which will allow for the safe and secure transmission of messages. This will make it such that the message can only be viewed by the sender and the intended recipient.

13. **OM3:** End to end encryption is the most secure platform to convey your messages to the other user.It does not even let the network providers and the company itself to access to our messages. We have a few misconceptions about E2EE like we think that our information can be hacked or used by other agencies be it government or non-government but it cannot. Along with this, we think that mailing is the best and most secure method for communication but what I have found is that apps with E2EE are more secure that E-mails, phone messengers and phone calls. We just need to take care about the malwares installed in our phone and if any other person can have access to our phone.

14. **OM4:** When you use E2EE to send a message to someone, E2EE encrypts the data in a way that makes it inaccessible to third parties, as the message is being delivered. This means that the app company, internet service providers (such as comcast or verizon), government agencies, and even hackers do not have the ability to decrypt your messages. Additionally, the app is unable to hand your data over to third parties. No one monitoring the network can see the contents of your message.

15. **OM5:** End-to-end encryption means that each user has a key which only their phone has. When travelling between service providers and the app company, the message is encrypted and cannot be read until the key unlocks the message. With normal message services, they hold the unencrypted messages which could be read at any time, and third parties such as hackers or the government could see the contents. The encryption algorithms are also very strong (so that no hacker can break it), so the only way for somebody besides the intended recipient to view the message contents is if their username or password is stolen/revealed.

16. **ORC1:** I learned that E2EE is an end-to-end encryption that secure messages between you and others. E2EE secures each messages with a key that you have with each message sending out. Non E2EE is more vulnerable to hackers that can intercept, edit, & view your outgoing messages. Government officials can legally obtain messages from the app company or service provider no matter how secure the encryption is. Sometimes message can also be lost in transit.

17. **ORC2:** E2EE enables a more secure form of communication, making users less vulnerable to security threats. Therefore, when a user is incentivized to have secure communication, apps using E2EE should be utilized over non-E2EE apps. While this is a general principle, it's worth noting that messages sent over E2EE are still vulnerable in some regards (just fewer parts than when not using E2EE).

18. **ORC3:** All messages use end-to-end encryption. This means only you and the recipient can read those messages - nobody else can decipher them, not even TextLight. All messages that you send and receive via TextLight cannot be deciphered when intercepted by your ISP, network administrator or any other third parties. Unless your usernames and passwords are stolen or guessed, there is no way that your messages could be modificated by a third person, nor the impersonation could happen. Nothing you share can be used to target you later. But please note that end to end encryption cannot protect your messages from any other people that get physical or root access to your phones or computers running TextLight.

19. **ORC4:** Do you ever wonder who may get access to your private messages/texts? Nowadays, it is very easy for hackers to get your private information, but NOT if you use TexLight app! TexLight is a specially-encrypted app that ensures that only you and your intended recipient can view the messages. This encryption is so secure that even the TexLight company cannot decrypt the messages, so you can feel secure in your communication. Try out yourself by

downloading the app here.

20. **ORC5:** The advantage of using end-to-end encryption (E2EE) is that it prevents your messages from being read when they are in transit and when they are stored by the app company. Non-E2EE approaches can prevent messages in transit from being compromised, but they are still at the risk of being exposed to third parties if the app company itself compromised. For example, non-E2EE cannot prevent the message from being exposed to:

    (a) Rogue employees

    (b) Requests by government agencies

    (c) Hackers who find a way to access the app company's servers

    However, the downside is that both E2EE and non-E2EE apps are still at risk when it comes to the user's phone. Such cases include when malware is installed or another person looks over the user's shoulder as they type in their passwords.

21. **ORM1:** End-to-end encryption is an encryption technique that utilizes user-specific encryption keys that only the sender and receiver of messages have access to. This encryption technique ensures that messages from one party to another are secure during transit between parties and when the company that stores the data for these messages is compromised. The algorithms that are utilized here are extremely strong and would take third parties an impossible amount of time to crack and decrypt. End-to-end encryption is an

essential tool to protect users' privacy in the modern age, whether it be from the government or private hackers.

22. **ORM2:** E2EE is a user friendly feature which protects both the sender and receive, as a result of method the data is encrypted stored. The positive capabilities eliminates the possibilities of a hacker intercepting messages or restrict the company's service provider's from executing decryption keys to decipher content. With TextLight, the software makes it vertically impossible for unauthorized outsider to gain access since there's no monitoring of the network by the company or third parties.

23. **ORM3:** With other, non-encrypted messaging apps, your messages might be vulnerable to hacking before reaching your recipient. With TextLight, your message is automatically encrypted with a unique lock and key, ensuring only you and your recipient can read what is sent. We use two layers of encryption so that no one else– not even server operators or TextLight employees– can access your message.

24. **ORM4:** Many apps, text messages, and even phone calls are not secure these days. The government, hackers, and even phone companies can have access to the content of your messages. People can even modify messages that you send in between you and your friend. Thus, it is essential to find ways to provide more security when communicating over the web. One way people do this is through E2EE. It is a secure messaging app that makes it almost IMPOSSIBLE for people to gain access to the content of your message. For example, a

messaging app that is E2EE may know that you have sent a message but they do not know what the content is. This also eliminates risk of hackers. Even if a hacker were to hack the company, they would not be able to alter or gain access to your content. It is actually more secure than other platforms such as text messages, imessage, emails, or even phone calls. It eliminates a lot of risk. However, there are still some risks that can not be eliminated such as someone looking over your shoulder while you're texting. However, overall, it is a more secure way for people to communicate via the web.

25. **ORM5:** End-to-end encryption otherwise as E2EE is a way to protect messages, phone calls, data transfers, and other similar things from being obtained. E2EE does this by essentially putting a shell that is impenetrable around the information being sent. This means that it is nearly impossible for someone to break the shell and get the information that the shell is protecting. The shell protects against everything such as the text messaging company, hackers who try to intercept the message, or internet service providers. The only time E2EE does not work is when a virus has already been placed on your phone/computer, someone gets into your phone/computer, or whoever you are sending the information shares it.

Bibliography

[1] A. Whitten and J. D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, SSYM'99, pages 14–14, 1999.

[2] S. Sheng, L. Broderick, C. A. Koranda, and J. J. Hyland. Why Johnny still Can't Encrypt: Evaluating the Usability of Email Encryption Software. In *Proceedings of the Second Symposium on Usable Privacy and Security*, SOUPS '06, 2006.

[3] Simson L. Garfinkel and Robert C. Miller. Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, SOUPS '05, pages 13–24. ACM, 2005.

[4] Scott Ruoti, Nathan Kim, Ben Burgon, Timothy van der Horst, and Kent Seamons. Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes. In *Proceedings of the Ninth Symposium on Usable Privacy and Securit*, pages 5:1–5:12. ACM, 2013.

[5] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the Adoption of Secure Communication Tools. In *Proc. of IEEE Security and Privacy*, pages 137–153, May 2017.

[6] Elham Vaziripour, Justin Wu, Mark O'Neill, Jordan Whitehead, Scott Heidbrink, Kent Seamons, and Daniel Zappala. Is that you, Alice? A Usability Study of the Authentication Ceremony of Secure Messaging Applications. In *Proc. of SOUPS '17*, pages 29–47, Santa Clara, CA, 2017. USENIX Association.

[7] Elham Vaziripour, Justin Wu, Mark O'Neill, Daniel Metro, Josh Cockrell, Timothy Moffett, Jordan Whitehead, Nick Bonner, Kent Seamons, and Daniel

Zappala. Action Needed! Helping Users Find and Complete the Authentication Ceremony in Signal. In *Proc. of SOUPS '18*, pages 47–62, Baltimore, MD, 2018. USENIX Association.

[8] Justin Wu and Daniel Zappala. When is a Tree Really a Truck? Exploring Mental Models of Encryption. In *Proc. of SOUPS '18*, pages 395–409, Baltimore, MD, 2018. USENIX Association.

[9] G. Kumparak. Apple Explains Exactly How Secure iMessage really is. *TechCrunch*, February 2014. `http://techcrunch.com/2014/02/27/apple-explains-exactly-how-secure-imessage-really-is/`.

[10] Apple. The Most Personal Technology Must Also Be the Most Private. `https://www.apple.com/privacy/approach-to-privacy/`, March 2016.

[11] C. Cattiaux and gg. iMessage Privacy. `http://blog.quarkslab.com/imessage-privacy.html`, October 2013.

[12] N. Weaver. iPhones, the FBI, and Going Dark. *Lawfare*, August 2015. `https://www.lawfareblog.com/iphones-fbi-and-going-dark`.

[13] Natasha Lomas. WhatsApp Completes End-to-End Encryption Rollout. `http://techcrunch.com/2016/04/05/whatsapp-completes-end-to-end-encryption-rollout/`, April 2016.

[14] S. Somogyi. Making End-to-End Encryption Easier to Use. *Google online security blog*, June 2014. `http://googleonlinesecurity.blogspot.com/2014/06/making-end-to-end-encryption-easier-to.html`.

[15] I. Paul. Yahoo Mail to Support End-to-End PGP Encryption by 2015. *PCWorld*, August 2015. `http://www.pcworld.com/article/2462852/yahoo-mail-to-support-end-to-end-pgp-encryption-by-2015.html`.

[16] Google. Google End-To-End wiki. `https://github.com/google/end-to-end/wiki`, December 2014.

[17] Susan E McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. Investigating the Computer Security Practices and Needs of Journalists. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 399–414. USENIX Association, 2015.

[18] S. Gaw, E. W. Felten, and P. Fernandez-Kelly. Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted Email. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, pages 591–600, New York, NY, USA, 2006. ACM.

[19] M. S. Melara, A. Blankstein, J. Bonneau, E. W. Felten, and M. J. Freedman. CONIKS: Bringing Key Transparency to End Users. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 383–398. USENIX Association, August 2015.

[20] Marta E. Cecchinato, Abigail Sellen, Milad Shokouhi, and Gavin Smyth. Finding Email in a Multi-Account, Multi-Device World. In *Proc. of CHI '16*, pages 1200–1210. ACM, 2016.

[21] Qingyao Ai, Susan T. Dumais, Nick Craswell, and Dan Liebling. Characterizing Email Search Using Large-scale Behavioral Logs and Surveys. In *Proc. of WWW '17*, pages 1511–1520, 2017.

[22] David Carmel, Liane Lewin-Eytan, Alex Libov, Yoelle Maarek, and Ariel Raviv. The Demographics of Mail Search and Their Application to Query Suggestion. In *Proc. of WWW '17*, pages 1541–1549, 2017.

[23] Dawn Xiaoding Song, D. Wagner, and A. Perrig. Practical Techniques for Searches on Encrypted Data. In *Proc. of IEEE Security and Privacy*, pages 44–55, 2000.

[24] Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions. In *Proc. of CCS '06*, pages 79–88. ACM, 2006.

[25] Seny Kamara, Charalampos Papamanthou, and Tom Roeder. Dynamic Searchable Symmetric Encryption. In *Proc. of CCS '12*, pages 965–976. ACM, 2012.

[26] Seny Kamara and Charalampos Papamanthou. *Parallel and Dynamic Searchable Symmetric Encryption*, pages 258–274. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[27] Emil Stefanov, Charalampos Papamanthou, and Elaine Shi. Practical Dynamic Searchable Encryption with Small Leakage. In *NDSS '14*. Internet Society, 2014.

[28] Raphael Bost. $\Sigma O \Phi O \varsigma$: Forward Secure Searchable Encryption. In *Proc. of CCS '16*, pages 1143–1154, 2016.

[29] Paul E. Green and V. Srinivasan. Conjoint Analysis in Marketing: New Developments with Implications for Research and Practice. *Journal of Marketing*, 54(4):3–19, 1990.

[30] Henrik Sattler and Adriane Hartmann. *Commercial Use of Conjoint Analysis*, pages 103–119. Gabler, Wiesbaden, 2008.

[31] Marco Vriens. Solving Marketing Problems with Conjoint Analysis. *Journal of Marketing Management*, 10(1-3):37–55, 1994.

[32] Yu Pu and Jens Grossklags. Towards a Model on the Factors Influencing Social App Users' Valuation of Interdependent Privacy. In *Proc. of PETS '16*, pages 61–81, 2016.

[33] Hanna Krasnova, Thomas Hildebrand, and Oliver Guenther. Investigating the Value of Privacy in Online Social Networks: Conjoint Analysis. In *ICIS '09 Proc.*, 2009.

[34] Daniel Burda and Frank Teuteberg. Understanding the Benefit Structure of Cloud Storage as a Means of Personal Archiving - a Choice-Based Conjoint Analysis. In *ECIS '14*, 2014.

[35] Alexander De Luca, Sauvik Das, Martin Ortlieb, Iulia Ion, and Ben Laurie. Expert and Non-Expert Attitudes towards (Secure) Instant Messaging. In *Proc. of SOUPS '16*, pages 147–157, Denver, CO, 2016.

[36] Svenja Schröder, Markus Huber, David Wind, and Christoph Rottermanner. When Signal Hits the Fan On the Usability and Security of State-of-the-Art Secure Mobile Messaging. In *Proc. of EuroUSEC*. Internet Society, 2016.

[37] Joshua Tan, Lujo Bauer, Joseph Bonneau, Lorrie Faith Cranor, Jeremy Thomas, and Blase Ur. Can Unicorns Help Users Compare Crypto Key Fingerprints? In *Proc. of CHI '17*, pages 3787–3798. ACM, 2017.

[38] W. Diffie and M. E. Hellman. New Directions in Cryptography. *Information Theory, IEEE Transactions on*, 22(6):644–654, Nov 1976.

[39] R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.

[40] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer. Openpgp message format. RFC 4880, RFC Editor, November 2007.

[41] Philip Zimmermann. Why I Wrote PGP. https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html, 1991.

[42] P. Zimmermann. PGP Version 2.6.2 User's Guide. `ftp://ftp.pgpi.org/pub/pgp/2.x/doc/pgpdoc1.txt`, October 1994.

[43] GPGTools. GPGTools. `https://gpgtools.org/`.

[44] Mailvelope. `https://www.mailvelope.com/en/`.

[45] B. Ramsdell. S/MIME Version 3 Message Specification. RFC 2633, RFC Editor, June 1999.

[46] P. Gutmann. Why isn't the Internet Secure Yet, Dammit. In *AusCERT Asia Pacific Information Technology Security Conference 2004; Computer Security: Are we there yet?* AusCERT Asia Pacific Information Technology Security, May 2004.

[47] Apple. iOS Security Guide, iOS 12.1 or Later. `https://www.apple.com/business/docs/iOS_Security_Guide.pdf`, November 2018.

[48] Christina Garman, Matthew Green, Gabriel Kaptchuk, Ian Miers, and Michael Rushanan. Dancing on the Lip of the Volcano: Chosen Ciphertext Attacks on Apple iMessage, 2016.

[49] B. Laurie, A. Langley, and E. Kasper. Certificate Transparency. RFC 6962, RFC Editor, June 2013.

[50] M. D. Ryan. Enhanced Certificate Transparency and End-to-End Encrypted Mail. In *21st Annual Network and Distributed System Security Symposium, NDSS'14*, 2014.

[51] S. Fahl, M. Harbach, T. Muders, and M. Smith. Confidentiality as a Service – Usable Security for the Cloud. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, pages 153–162, June 2012.

[52] Scott Ruoti, Jeff Andersen, Travis Hendershot, Daniel Zappala, and Kent Seamons. Private Webmail 2.0: Simple and Easy-to-Use Secure Email. In *Proc. of UIST '16*, pages 461–472. ACM, 2016.

[53] Erinn Atwater, Cecylia Bocovich, Urs Hengartner, Ed Lank, and Ian Goldberg. Leading Johnny to Water: Designing for Usability and Trust. In *Proc. of SOUPS '15*, pages 69–88, 2015.

[54] Wenley Tong, Sebastian Gold, Samuel Gichohi, Mihai Roman, and Jonathan Frankle. Why King George III Can Encrypt. `http://randomwalker.info/teaching/spring-2014-privacy-technologies/king-george-iii-encrypt.pdf`, 2014.

[55] Joscha Lausch, Oliver Wiese, and Volker Roth. What is a Secure Email. In *Proc. of EuroUSEC '17*. Internet Society, 2017.

[56] Scott Ruoti, Jeff Andersen, Scott Heidbrink, Mark O'Neill, Elham Vaziripour, Justin Wu, Daniel Zappala, and Kent Seamons. 'We're on the Same Page': A Usability Study of Secure Email Using Pairs of Novice Users. In *Proc. of CHI '16*, pages 4298–4308. ACM, 2016.

[57] Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith, and Uwe Sander. Helping Johnny 2.0 to Encrypt His Facebook Conversations. In *Proc. of SOUPS '12*, pages 11:1–11:17. ACM, 2012.

[58] Wei Bai, Moses Namara, Yichen Qian, Patrick Gage Kelley, Michelle L. Mazurek, and Doowon Kim. An Inconvenient Trust: User Attitudes toward Security and Usability Tradeoffs for Key-Directory Encryption Systems. In *Proc. of SOUPS '16*, pages 113–130, Denver, CO, 2016.

[59] Keybase. `https://keybase.io/`.

[60] A. Lerner, E. Zeng, and F. Roesner. Confidante: Usable Encrypted Email: A Case Study with Lawyers and Journalists. In *Proc. of European Security and Privacy*, pages 385–400, April 2017.

[61] Amir Herzberg and Hemi Leibowitz. Can Johnny Finally Encrypt?: Evaluating E2E-encryption in Popular IM Applications. In *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust*, STAST '16, pages 17–28, New York, NY, USA, 2016. ACM.

[62] Maliheh Shirvanian and Nitesh Saxena. On the Security and Usability of Crypto Phones. In *Proc. of ACSAC '15*, pages 21–30, 2015.

[63] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith. SoK: Secure Messaging. In *Proc. of IEEE Security and Privacy*, pages 232–249, May 2015.

[64] Scott Ruoti, Jeff Andersen, Tyler Monson, Daniel Zappala, and Kent Seamons. A Comparative Usability Study of Key Management in Secure Email. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 375–394, Baltimore, MD, 2018. USENIX Association.

[65] D. J. Solove. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review*, 44:745, 2007.

[66] Electronic Frontier Foundation. Secure Messaging Scorecard, 2016. `https://www.eff.org/node/82654`.

[67] Albese Demjaha, Jonathan Spring, Ingolf Becker, Simon Parkin, and Angela Sasse. Metaphors Considered Harmful? An Exploratory Study of the Effectiveness of Functional Metaphors for End-to-End Encryption. In *Workshop on Usable Security*. Internet Society, 2018.

[68] Nina Gerber, Verena Zimmermann, Birgit Henhapl, Sinem Emeröz, and Melanie Volkamer. Finally Johnny Can Encrypt: But Does This Make Him Feel More Secure? In *International Conference on Availability, Reliability and Security (ARES)*, ARES 2018, pages 11:1–11:10, New York, NY, USA, 2018. ACM.

[69] Billy Lau, Simon Chung, Chengyu Song, Yeongjin Jang, Wenke Lee, and Alexandra Boldyreva. Mimesis Aegis: A Mimicry Privacy Shield–A System's Approach to Data Privacy on Public Cloud. In *USENIX Security '14*, pages 33–48, 2014.

[70] David Cash, Joseph Jaeger, Stanislaw Jarecki, Charanjit Jutla, Hugo Krawczyk, Marcel-Catalin Rosu, and Michael Steiner. Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation. Cryptology ePrint Archive, Report 2014/853, 2014.

[71] Patrick Grofig, Martin Haerterich, Isabelle Hang, Florian Kerschbaum, Mathias Kohler, Andreas Schaad, Axel Schroepfer, and Walter Tighzert. Experiences and Observations on the Industrial Implementation of a System to Search Over Outsourced Encrypted Data. http://subs.emis.de/LNI/Proceedings/Proceedings228/article7.html, 2014.

[72] Bitglass. "http://www.bitglass.com/".

[73] Google. Bigquery. https://github.com/google/encrypted-bigquery-client.

[74] Microsoft. Always Encrypted (database engine). https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine.

[75] Skyhigh Networks. https://www.skyhighnetworks.com.

[76] B. Fuller, M. Varia, A. Yerukhimovich, E. Shen, A. Hamlin, V. Gadepally, R. Shay, J. D. Mitchell, and R. K. Cunningham. SoK: Cryptographically Protected Database Search. In *Prof. of IEEE Security and Privacy*, pages 172–191, May 2017.

[77] T. Midorikawa, A. Tachikawa, and A. Kanaoka. Helping Johnny to Search: Encrypted Search on Webmail System. In *2018 13th Asia Joint Conference on Information Security (AsiaJCIS)*, pages 47–53, Aug 2018.

[78] Susan Dumais, Edward Cutrell, JJ Cadiz, Gavin Jancke, Raman Sarin, and Daniel C. Robbins. Stuff I'Ve Seen: A System for Personal Information Retrieval and Re-use. In *Proc. of SIGIR '03*, pages 72–79. ACM, 2003.

[79] David Elsweiler, David E. Losada, José C. Toucedo, and Ronald T. Fernandez. Seeding Simulated Queries with User-study Data for Personal Search Evaluation. In *Proc. of SIGIR '11*, pages 25–34. ACM, 2011.

[80] Morgan Harvey and David Elsweiler. *Exploring Query Patterns in Email Search*, pages 25–36. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[81] Steve Whittaker, Tara Matthews, Julian Cerruti, Hernan Badenes, and John Tang. Am I Wasting My Time Organizing Email?: A Study of Email Refinding. In *Proc. of CHI '11*, pages 3449–3458. ACM, 2011.

[82] Adestra. Top 10 Email Clients in March 2019. https://www.adestra.com/resources/top-10-email-clients/, March 2019.

[83] Fluent. The Inbox Report, Consumer Perceptions of Email. https://www.fluentco.com/resources/the-inbox-report/, 2018.

[84] Yu Pu and Jens Grossklags. Valuating Friends' Privacy: Does Anonymity of Sharing Personal Data Matter? In *Proc. of SOUPS '17)*, pages 339–355, 2017.

[85] Richard E. Mayer and Richard B. Anderson. The Instructive Animation: Helping Students Build Connections Between Words and Pictures in Multimedia Learning. *Journal of Educational Psychology*, 84(4):444–452, 1992.

[86] Richard E. Mayer. *Multimedia Learning.* Cambridge University Press, New York, NY, USA, 2nd edition, 2009.

[87] National Research Council. *How People Learn: Bridging Research and Practice.* The National Academies Press, 1999.

[88] John Robert Anderson. *Rules of the Mind.* Lawrence Erlbaum Associates, Inc., Hillsdale, NJ, US, 1993.

[89] K. Elliott and T. Rupar. Six Months of Revelations on NSA. *Washington Post*, June 2013. `http://www.washingtonpost.com/wp-srv/special/national/nsa-timeline/m/` (Last accessed on 05/16/2016).

[90] D. Bisson. A Timeline of the Apple-FBI iPhone Controversy. *The State of Security*, March 2016. `http://www.tripwire.com/state-of-security/government/a-timeline-of-the-apple-fbi-iphone-controversy/` (Last accessed on 05/16/2016).

[91] D. Hedeker. Mixed Models for Longitudinal Ordinal and Nominal Outcomes, 2012. `http://www.uic.edu/classes/bstt/bstt513/OrdNomLS.pdf` (Last accessed on 05/16/2016).

[92] K. P. Burnham and D. R. Anderson. Multimodel Inference: Understanding AIC and BIC in Model Selection. *Sociological Methods & Research*, 33(2):261–304, November 2004.

[93] Anselm L. Strauss and Juliet M. Corbin. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory.* Sage Publications, Inc, Thousand Oaks, CA, USA, 1998.

[94] M. Viswanathan. *Measurement Error and Research Design.* Sage Publications, 2005.

[95] W. Bai, D. Kim, M. Namara, Y. Qian, P. G. Kelley, and M. L. Mazurek. Balancing Security and Usability in Encrypted Email. *IEEE Internet Computing*, 21(3):30–38, May 2017.

[96] L. J. Camp, T. Kelley, and P. Rajivan. Instrument for Measuring Computing and Security Expertise. Technical Report TR715, Indiana University, February 2015.

[97] Oded Goldreich and Rafail Ostrovsky. Software Protection and Simulation on Oblivious RAMs. *J. ACM*, 43(3):431–473, May 1996.

[98] Tarik Moataz and Abdullatif Shikfa. Boolean Symmetric Searchable Encryption. In *Proc. of ASIA CCS '13*, pages 265–276. ACM, 2013.

[99] Eric Chen, Ismael Gomes, Brian Saavedra, and Jonatan Yucra. Cocoon: Encrypted Substring Search, 2015. `https://courses.csail.mit.edu/6.857/2016/files/29.pdf`.

[100] Chase Melissa and Shen Emily. Substring-Searchable Symmetric Encryption. *Proc. on Privacy Enhancing Technologies*, 2015:263, Apr. 2015.

[101] Xianrui Meng, Seny Kamara, Kobbi Nissim, and George Kollios. GRECS: Graph Encryption for Approximate Shortest Distance Queries. In *Proc. of CCS '15*, pages 504–517. ACM, 2015.

[102] Tarik Moataz and Erik-Oliver Blass. Oblivious Substring Search with Updates. *IACR Cryptology ePrint Archive*, 2015:722, 2015.

[103] Yuval Ishai, Eyal Kushilevitz, Steve Lu, and Rafail Ostrovsky. *Private Large-Scale Databases with Distributed Searchable Symmetric Encryption*, pages 90–107. Springer International Publishing, Cham, 2016.

[104] Antti Oulasvirta and Lauri Sumari. Mobile Kits and Laptop Trays: Managing Multiple Devices in Mobile Information Work. In *Proc. of CHI '07*, pages 1127–1136. ACM, 2007.

[105] ProtonMail. `https://protonmail.com/`.

[106] Threema. `https://threema.ch/en`.

[107] Google. How Gmail Ads Work. `https://support.google.com/mail/answer/6603?hl=en`, 2017.

[108] Vasilis Pappas, Fernando Krell, Binh Vo, Vladimir Kolesnikov, Tal Malkin, Seung Geol Choi, Wesley George, Angelos Keromytis, and Steve Bellovin. Blind Seer: A Scalable Private DBMS. In *Proc. of IEEE Security and Privacy*, pages 359–374, 2014.

[109] B. A. Fisch, B. Vo, F. Krell, A. Kumarasubramanian, V. Kolesnikov, T. Malkin, and S. M. Bellovin. Malicious-Client Security in Blind Seer: A Scalable Private DBMS. In *Proc. of IEEE Security & Privacy*, pages 395–410, May 2015.

[110] David Pouliot and Charles V. Wright. The Shadow Nemesis: Inference Attacks on Efficiently Deployable, Efficiently Searchable Encryption. In *Proc. of CCS '16*, pages 1341–1352, 2016.

[111] Yupeng Zhang, Jonathan Katz, and Charalampos Papamanthou. All Your Queries Are Belong to Us: The Power of File-Injection Attacks on Searchable Encryption. In *USENIX Security '16*, pages 707–720, Austin, TX, 2016.

[112] Muhammad Naveed. The Fallacy of Composition of Oblivious RAM and Searchable Encryption. Cryptology ePrint Archive, Report 2015/668, 2015. `http://eprint.iacr.org/2015/668`.

[113] Paul E. Green and Vithala R. Rao. Conjoint Measurement for Quantifying Judgmental Data. *Journal of Marketing Research*, 8(3):355–363, 1971.

[114] Paul E. Green and V. Srinivasan. Conjoint Analysis in Consumer Research: Issues and Outlook. *Journal of Consumer Research*, 5(2):103–123, 1978.

[115] Wayne S. Desarbo, Venkatram Ramaswamy, and Steven H. Cohen. Market Segmentation with Choice-Based Conjoint Analysis. *Marketing Letters*, 6(2):137–147, 1995.

[116] G.E.P. Box, J.S. Hunter, and W.G. Hunter. *Statistics for Experimenters: Design, Innovation, and Discovery*. Wiley series in probability and statistics. Wiley-Interscience, 2005.

[117] Mickael Bech, Trine Kjaer, and Jrgen Lauridsen. Does the Number of Choice Sets Matter? Results from a Web Survey Applying a Discrete Choice Experiment. *Health Economics*, 20(3):273–286, 2011.

[118] Hideo Aizaki and Kazushi Nishimura. Design and Analysis of Choice Experiments Using R: A Brief Introduction. *Agricultural Information Research*, 17(2):86–94, 2008.

[119] Amazon Mechanical Turk. `https://www.mturk.com/mturk/welcome`.

[120] Eyal Peer, Joachim Vosgerau, and Alessandro Acquisti. Reputation as a sufficient condition for data quality on Amazon Mechanical Turk. *Behavior Research Methods*, 46(4):1023–1031, 2014.

[121] Eszter Hargittai and Yuli Patrick Hsieh. Succinct Survey Measures of Web-Use Skills. *Soc. Sci. Comput. Rev.*, 30(1):95–107, February 2012.

[122] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Info. Sys. Research*, 15(4):336–355, December 2004.

[123] Sören Preibusch. Guide to Measuring Privacy Concern: Review of Survey and Observational Instruments. *Int. J. Hum.-Comput. Stud.*, 71(12):1133–1143, December 2013.

[124] Peter E. Rossi and Greg M. Allenby. Bayesian Statistics and Marketing. *Marketing Science*, 22(3):304–328, September 2003.

[125] Peter Rossi. *bayesm: Bayesian Inference for Marketing/Micro-Econometrics*, 2015. R package version 3.0-2.

[126] Mickael Bech and Dorte Gyrd-Hansen. Effects Coding in Discrete Choice Experiments. *Health Economics*, 14(10):1079–1083, 2005.

[127] Ming Yuan and Yi Lin. Model Selection and Estimation in Regression with Grouped Variables. *Journal of the Royal Statistical Society, series B*, 68:49–67, 2006.

[128] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. Privacy attitudes of mechanical turk workers and the u.s. public. In *Proc. of SOUPS '14*, pages 37–49, 2014.

[129] Rudolf Vetschera and Guenther Kainz. Do Self-Reported Strategies Match Actual Behavior in a Social Preference Experiment? *Group Decision and Negotiation*, 22(5):823–849, 2013.

[130] Eszter Hargittai and Alice Marwick. "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication*, 10(0), 2016.

[131] Ana Nuno and Freya A.V. St. John. How to Ask Sensitive Questions in Conservation: A Review of Specialized Questioning Techniques. *Biological Conservation*, 189:5–15, 2015.

[132] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. Privacy As Part of the App Decision-making Process. In *Proc. of CHI '13*, pages 3393–3402. ACM, 2013.

[133] Scott Barge and Hunter Gehlbach. Using the Theory of Satisficing to Evaluate the Quality of Survey Data. *Research in Higher Education*, 53(2):182–200, 2012.

[134] Wei Bai, Ciara Lynton, Michelle. L Mazurek, and Charalampos Papamanthou. Understanding User Tradeoffs for Search in Encrypted Communication. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2018.

[135] Kenneth Train. *Discrete Choice Methods with Simulation*. SUNY-Oswego, Department of Economics, 2003.

[136] Rinus Haaijer, Wagner Kamakura, and Michel Wedel. The 'no-choice' Alternative in Conjoint Choice Experiments. *International Journal of Market Research*, 43, 2001.

[137] Alessandro Acquisti and Jens Grossklags. An Online Survey Experiment on Ambiguity and Privacy. *Communications & Strategies*, 88:19–39, 2012.

[138] Janice Y. Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. In *ICIS '07 Proc.*, 2007.

[139] WhatsApp. https://www.whatsapp.com/.

[140] Facebook Inc. Facebook Messenger. https://www.messenger.com/.

[141] Telegram. MTProto Mobile Protocol. https://core.telegram.org/mtproto.

[142] Klaus Krippendorff. *Content Analysis: An Introduction to Its Methodology.* Sage Publications, Inc., 2004.

[143] R. Rosenthal, R.L. Rosnow, and A.E. Kazdin. *Artifacts in Behavioral Research: Robert Rosenthal and Ralph L. Rosnow's Classic Books.* Oxford University Press, 2009.

[144] Jeffrey Warshaw, Nina Taft, and Allison Woodruff. Intuitions, Analytics, and Killing Ants: Inference Literacy of High School-Educated Adults in the US. In *Proc. of SOUPS*, 2016.

[145] Reuters. UK Minister Says Encryption on Messaging Services is Unacceptable. https://www.reuters.com/article/us-britain-security-rudd/uk-minister-says-encryption-on-messaging-services-is-unacceptable-idUSKBN16X 2017.