Distrust of big tech and a desire for privacy: Understanding the motivations of people who have voluntarily adopted secure email

Warda Usman
Brigham Young University

Jackie Hu
Brigham Young University

McKynlee Wilson
Brigham Young University

Daniel Zappala
Brigham Young University

Abstract

Secure email systems that use end-to-end encryption are the best method we have for ensuring user privacy and security in email communication. However, the adoption of secure email remains low, with previous studies suggesting mainly that secure email is too complex or inconvenient to use. However, the perspectives of those who have, in fact, chosen to use an encrypted email system are largely overlooked. To understand these perspectives, we conducted a semi-structured interview study that aims to provide a comprehensive understanding of the mindsets underlying adoption and use of secure email services. Our participants come from a variety of countries and vary in the amount of time they have been using secure email, how often they use it, and whether they use it as their primary account. Our results uncover that a defining reason for adopting a secure email system is to avoid surveillance from big tech companies. However, regardless of the complexity and accuracy of a person's mental model, our participants rarely send and receive encrypted emails, thus not making full use of the privacy they could obtain. These findings indicate that secure email systems could potentially find greater adoption by appealing to their privacy advantages, but privacy gains will be limited until a critical mass are able to join these systems and easily send encrypted emails to each other.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

1 Introduction

There are over 319 billion[1] emails sent every day. These emails are transmitted and stored primarily in plaintext, and are therefore subject to a wide variety of threats, including surveillance, modification, commercial analysis, and theft. Emails sent and received by larger providers are often encrypted when they are sent between email servers, but this is not universally deployed, can be circumvented, and still leaves emails vulnerable to attacks where they are stored [9]. This insecure communication creates a variety of security and privacy threats for users.

To protect the privacy and security of messages, experts have been suggesting end-to-end encryption (E2EE) and encrypted storage for decades now. Despite these efforts, the use of E2EE for email has remained relatively scarce [45].

The research community has generally focused on improving the usability of secure email systems, believing that this was the primary obstacle to adoption. This work began with a seminal paper by Whitten and Tyger [49], showing that users made mistakes when interacting with key pairs. These problems continued to plague systems based on PGP for years [36, 40], but recent work has shown how to provide usable secure email systems by automating user interactions with keys and certificates as much as possible [14,37,38]. Current web-based systems, such as Proton Mail and Tutanota, utilize automation and have interfaces that are largely similar to popular email sites like Gmail, so usability is unlikely to remain a significant obstacle to adoption.

A growing body of work has demonstrated that a variety of factors beyond usability affect adoption of secure email. In a broad look at secure communication tools [1], the primary obstacles were found to be fragmented user bases, lack of interoperability, and low quality of service. Lack of advertising is also an issue; a large number of people are still unaware of the existence of any secure email services [45]. Further, users

[1] From the Email Statics Report, 2021-2025, by The Radicati Group, https://www.radicati.com/wp/wp-content/uploads/2020/12/Email-Statistics-Report-2021-2025-Executive-Summary.pdf

resist adopting secure email due to their incomplete threat models, misaligned incentives, and due to lack of understanding about the secure email architecture [34]. Other factors which go beyond an individual user also contribute [4]. For example, secure email requires global interoperability among heterogeneous clients and systems to be useful. Additionally, many stakeholders of secure email do not agree on what properties to provide, which hinders development of a ubiquitous protocol for secure email. Another factor is that encrypted storage of email makes search of encrypted archives and scanning for spam and malware more difficult, which might cause some users to stick with traditional unencrypted methods.

Today millions of people do use secure web-based email systems and some businesses use S/MIME integrated into email clients such as Outlook. This is a significant improvement over past decades, but still well short of the billions using standard email and the billions using secure messaging apps such as WhatsApp. However, many of the lessons learned from the adoption of secure messaging do not provide similar pathways for adoption of secure email systems. First, users with no interest in the security or privacy features of secure messaging apps have primarily adopted one because their regular communication partners used it [1]. This is easier to do with secure messaging applications, since they are walled gardens, which means that users can only communicate with those using the same provider. Secure email, on the other hand, must remain interoperable with a wide variety of non-secure email systems and clients in order to be useful; a friend using secure email doesn't require you to join that same system in order to communicate. Another factor motivating adoption of secure messaging apps is that they enable users to avoid texting fees for international messaging. This also doesn't apply to email since it is generally a free service.

Our goal in this work is to better understand those relatively unusual people who choose to use a secure email service such as Proton Mail or Tutanota. While prior work has focused on the *lack* of adoption, these people have made the choice to use a system offering privacy and security benefits when free, less secure, and less private tools are readily available. Moreover, these users must operate in a world where the vast majority of their emails are likely going to other people who do *not* use a secure system, in contrast to the walled garden offered by a secure messaging app. Talking to users who have made this choice can help us to understand their motivations and provide insight into whether more people could follow their path.

We identified the following research questions:

1. Why do people voluntarily adopt secure email systems?

2. What threat models do people have, meaning their conception of attackers and the harms they can impose, and what steps do they take to mitigate these harms?

3. What mental models do people have of secure email systems and their capabilities? We particularly want to understand perceptions of what security and privacy means within the context of email and how secure email systems provide security and privacy.

4. Do people use the secure email services effectively and what obstacles they encounter in trying to do so?

To answer these questions, we conducted an interview study among users of secure email systems, primarily Proton Mail. We interviewed 25 participants who currently use Proton Mail, from 12 different countries. Our interview focused on answering the four questions listed above, thus discussing their reasons for adoption, their mental models, their threat models, and their usage of secure email. We analyzed the interviews using a mix of inductive and deductive coding, depending on which applied best to a given research question.

Our findings indicate that motivations to adopt a secure email system include a combination of distrust of big tech companies, aversion to targeted advertising, various notions of privacy, affordances, trust in companies that offer privacy, and a desire to align decisions with companies that share their values. Privacy resonates strongly with the participants, with Proton Mail seen as one way they can avoid big tech companies or obtain a particular privacy benefit. Participants recognized that major harms could come from government surveillance or hackers stealing their email, but were motivated by threats they felt were more likely, such as the general surveillance economy. These feelings were consistent both among those who had only a limited understanding of how a secure email system works and those who had accurate, detailed mental models of how encrypted email provides privacy guarantees. Despite the dominant theme of privacy, all participants primarily used Proton Mail to send *unencrypted* email to contacts on other email systems, leading to rather limited privacy gains.

The contributions of our paper include (a) a rich, qualitative data from a set of people who have actively chosen to use a secure email system; (b) analysis of the data that illustrates motivations to use a secure email system, mental models, threat models, and usage patterns; and (c) reflections on how researchers and industry can capitalize on the desire for privacy to realize stronger privacy gains for users.

2 Related Work

Because our work focuses on adoption, we reference several prominent theories from research on technology adoption. The Technology Acceptance Model (TAM) [8] identifies perceived usefulness and perceived ease-of-use as factors influencing behavioral intention to use a technology. The Unified Theory of Acceptance and Use of Technology (UTAUT) [46] extends TAM by considering additional factors such as social influence, voluntariness, and facilitating conditions. Protection Motivation Theory (PMT) [26,35] addresses the cognitive processes involved in behavior change when faced with a threat, including assessing threat likelihood and severity, evaluating mitigating action efficacy and cost, and considering self-efficacy.

2.1 Adoption of Secure Technology

Recent work by Zou et al. [55] examined adoption and abandonment of a wide range of security and privacy practices, finding that security practices were more widely adopted than privacy practices. Abu-Salma et al. [1] studied the obstacles to adoption of secure communication tools, discovering that majority of participants did not understand E2EE and primarily adopted them for social reasons rather than security benefits. Story et al. [44] measured the usage of and perceptions about private browsing, VPNs, Tor Browser, ad blockers, and antivirus software. They identified several misconceptions and suggested that interventions surrounding these tools should target well-defined threats and address obstacles to user threat models. Kang et al. [23] interviewed individuals regarding privacy and security risks, identifying that people don't take privacy-protective actions due to lack of concern, actions being costly or difficult, and limited knowledge. Other studies have focused on the adoption of individual tools, such as private browsing [13,18] and VPNs [10,29], suggesting similar results.

Prior research has also looked into the adoption of 2FA and password managers, finding that usability issues are an obstacle [6,7], and that stories encouraged people to be willing to adopt 2FA [12]. Other studies have also found evidence that perceived usability issues may not be as significant as misconceptions surrounding 2FA [5].

Regarding password managers (PMs), prior work has found lack of awareness to be a strong reason for non-adoption [2], and that users of built-in PMs are driven by convenience, whereas users of separately installed password managers prioritize security [31]. Mayer et al. [28] discovered that PM adoption in a university setting is largely driven by perceived ease-of-use.

Two studies have examined adoption of secure email. Gaw et al. [16] found that the perception of encryption behaviour by others influenced a person's decision to adopt encrypted email. Renaud et al. [34] found that misaligned incentives, lack of understanding of the email architecture, and fragmented threat models cause the non-adoption of E2E-encrypted email.

2.2 Privacy Frameworks

One of the motivations we found for people adopting secure email was a desire for privacy. Accordingly, we review the variety of theoretical approaches that researchers have used to explain how people conceptualize and treat privacy.

Westin's taxonomy of privacy classifies individuals based on their varying levels of privacy concerns [21,48]. However, this classification is far from modern real-world scenarios [51] and does not take into account the wider range of privacy management strategies by users [25,50]. Malhotra et al.'s information privacy concern scale looks at privacy from the perspective of the collection, control and awareness of information [27]. Prior research has also highlighted privacy calculus, in which individuals weigh the costs and benefits of disclosing their personal information [20,24]. Another prominent privacy framework is contextual integrity [30], that takes into account the social and cultural norms of specific contexts and argues that privacy is maintained when information flows align with these norms.

Solove proposed a taxonomy of privacy threats which includes four categories: information collection, information processing, information dissemination, and invasions [43]. Solove also worked on conceptualizing privacy [42], which takes into account that individuals are likely to differ in their perceptions of what privacy constitutes, how privacy can be violated, and which privacy benefits are most important to them. In this work, he characterized privacy as six major conceptions: (1) the right to be left alone, (2) limited access to self, (3) secrecy, (4) control over information, (5) personhood, and (6) intimacy.

Our findings on privacy motivations for adoption do not align with any singular privacy framework; we discuss this in Section 5.1.

3 Methodology

Our study is focused on the unique population that has decided to *voluntarily* adopt a secure email service. We designed and conducted semi-structured interviews with 25 users of Proton Mail and Tutanota, two popular secure email systems that claim to have 70 million users and several million users, respectively. We used a semi-structured interview guide to ensure we covered material relevant to each of our research questions, while also having the freedom to explore topics in more depth as needed.

3.1 Screening Survey

In all recruiting venues we asked participants to take a short screening survey to confirm their eligibility (age 18 or older, able to speak English), provide a list of email services they have accounts with, indicate the amount of time they have had a secure email address, describe the frequency with which they use their secure email account, and answer basic demographic questions.

Based on results from the screening survey, we used purposive sampling to ensure that we recruited participants who used secure email services across a variety of characteristics such as the amount of time they have been the service for, how often they use it and whether they use it as their primary email account.

3.2 Recruitment

After substantial recruiting efforts, we were able to recruit eight participants from Reddit and 17 participants from Prolific. We paid participants from Reddit USD 15 each using Amazon gift cards, and participants from Prolific USD 25 each as a Prolific bonus. We increased the compensation for Prolific participants since they were unwilling to participate in a lengthy interview for only USD 15.

Recruiting was challenging because we wanted to interview people who used secure email systems, and this is a relative minority of the overall population with no easy way to access them. We detail some of these challenges below to aid future researchers with similar problems.

We initially posted the invitation for our study on the official subreddits for Proton Mail[2] and Tutanota[3]. After having mixed success, with most participants being technically savvy, we attempted to diversify our sample. We posted our study on Amazon Mechanical Turk and on several general subreddits that were not related to technology. We did not screen for location as long as the potential participants could communicate in English. We asked a few questions at the beginning of the interview to filter fraudulent attempts at participation by non-users, including asking for their zip code (which would typically not match what they had entered in the screening survey), asking for their Proton Mail email address, sending out a test email, and asking about features of Proton Mail that only a user would know. *None* of the participants from MTurk seemed to be legitimate users. We believe the attempt to participate was largely due to the monetary incentive offered, especially in countries with higher USD value, leading in a disproportionate representation of non-users attempting to participate solely for the reward. We therefore decided to exclude MTurk and general subreddits from our study.

We also placed a Google Ad for our study that appeared in search results for terms related to secure and private email, and experimented with both a USD 25 payment for an interview and a drawing for USD 100 with a 1 in 5 chance of winning. Despite the ad receiving 63.5k impressions and 996 clicks, for a total cost of USD 176, nobody signed up for an interview in this recruitment channel.

Ultimately, we switched our recruiting efforts to Prolific, where we had much better success. To mitigate the issue of having non-users in the study, we excluded countries where the ratio of English speakers was extremely low or the currency difference was especially higher. We did not have to exclude any Prolific participants during screening.

3.3 Demographics

We interviewed 25 users of Proton Mail. Participants were residents of Australia, Canada, Mexico, the Netherlands, Switzerland, Portugal, Poland, Spain, Greece, Japan, the United Kingdom, and the United States. Three of them identified as female and 19 identified as male, two identified as non-binary and one preferred not to answer. Four were between 18–24 years of age, twelve were 25–34, four were 35–44, and five were 45–54. Most users were highly educated: nine had bachelor's degrees, and eleven had graduate or professional degrees. 12 participants had a formal background in technical fields. We provide detailed demographics in Table 1.

3.4 Interviews

We conducted all interviews in English remotely via Zoom, where turning the camera on was optional for the participants. Each interview lasted between 35-45 minutes. We began by asking some ice breaker questions to put them at ease, and we confirmed that the participant currently used Proton Mail or Tutanota. To avoid bias, we made sure to not use the word 'security' or 'privacy' until the participant mentioned it. We then asked questions in four different areas, in order, corresponding to each of our research questions:

- *Adoption*: We asked how they first heard about Proton Mail, how they started using it, why they currently use it, whether they encourage other people to use it, and similar questions.

- *Threat model*: We asked them which entities they feel would access or misuse their email data if they could get it, what the consequences would be of someone reading their email without permission, and how they mitigate any perceived threats.

- *Mental model*: We asked participants how they think Proton Mail works. We then asked them to draw what is involved when one person sends an email to another person, similar to prior work [22, 23, 52]. We encouraged participants to think aloud while drawing to gather additional insights into their reasoning. We asked the participants to send a photo of their drawing to us, or if they had their camera on, we requested them to hold it up to the camera and took a screenshot. We explored both structural properties, which describe how participants view the internals of the working of Proton Mail, as well as functional properties which focus on how these users interact with and use the email system.

- *Usage*: We asked them what they use their Proton Mail account for, how they interact with people who don't have secure email accounts, and what they like and dislike about Proton Mail.

[2] https://www.reddit.com/r/ProtonMail/
[3] https://www.reddit.com/r/Tutanota/

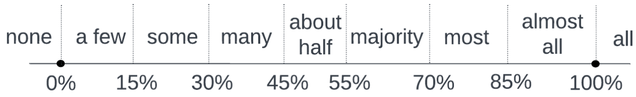

Figure 1: Terminology used to convey relative frequency of themes

3.5 Data Analysis

We recorded the audio from each interview using Zoom. We then transcribed the recordings using an automated transcription service. The first author reviewed all transcripts to ensure consistency with the recordings.

We conducted qualitative coding regularly throughout the interview process. This enabled us to look for saturation and to adjust the interviews as interesting ideas or themes emerged. We used thematic analysis, coding the data corresponding to our research questions. We primarily assigned the codes inductively, but used deductive coding for threat models, where we looked specifically for attackers, harms an attacker can cause, and how the participant explained they would mitigate that harm.

Three researchers coded all the transcripts together and disagreements were resolved through consensus-building as they emerged. We started by coding the data, assigning first-order codes which were closely aligned with the terms used by the interviewees in order to preserve the authenticity of their expressions. We then refined the codes through further iterative rounds of analysis, assigning second-order themes [17]. Similar themes were merged together to identify relationships and patterns in the data.

The primary author conducted a separate analysis of the drawings and the accompanying verbal explanations. In doing so, we grouped similar drawings and mental models together based on a participant's understanding of the inner workings of secure email systems. These categories were then reviewed and discussed among all the authors and any discrepancies were reconciled.

Since our work is qualitative in nature, we avoid using exact numbers. Instead, we use a consistent terminology to convey the relative frequency of major themes, as done by previous studies [11, 19, 53]. Figure 1 presents the terms used to indicate the frequency of occurrence of participants' responses.

3.6 Ethical Considerations

Our study did not create significant potential for harm to participants because we only sought to gather their opinions and experiences. The Institutional Review Board (IRB) at Brigham Young University reviewed and approved our study, and we obtained informed consent from participants. Because participants were from a variety of countries, each potentially with their own privacy laws, we took care to notify all participants of their data privacy rights, using a superset of all rights available in countries whose privacy laws are tracked at the Global Data Privacy & Security Handbook.[4] Specifically, we informed all participants that they had the right to access their own data, correct their data where inaccurate or incomplete, erase their personal data, withdraw consent, etc.

3.7 Limitations

We chose an interview study to gain insights into the attitudes and experiences of a relatively understudied group. As with most qualitative work, our purpose was to surface primary themes that impact adoption, understanding, and use of secure email, rather than to quantify the prevalence of these themes. Our sample is diverse among age, location, and technical expertise, but doesn't capture all possible opinions or experiences.

Despite trying to find users of a variety of secure email systems, with a focus on voluntary adoption rather than mandated corporate use, all of our participants primarily used Proton Mail as a secure email system. Further, we interviewed participants who were fluent in English and resided in countries where the currency exchange rate difference with USD was not dramatically high. Thus our results may not reflect the broader secure email space.

4 Findings

In this section, we present the themes we observed across our interviews for each of the research questions we study: (1) Why do people voluntarily adopt secure email systems? (2) What threat models do people have, meaning their conception of attackers and the harms they can impose, and what steps do they take to mitigate these harms? (3) What mental models do people have of secure email systems and their capabilities? (4) Do people use the secure email services effectively and what obstacles they encounter?

All of our participants were active users of Proton Mail (with a few also using Tutanota), so our findings repeatedly reference their use of this system in particular.

4.1 Adoption Motivations

We found a variety of factors that drive the adoption of Proton Mail for our participants. We describe them here in order of their prevalence and level of emphasis.

Distrust of Big Tech: The decision to adopt Proton Mail was driven heavily by the distrust our participants showed toward technology giants. Majority of the participants expressed

[4] https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security

concerns regarding the continuous monitoring and data collection practices employed by these organizations. Participants mentioned feeling being exploited by big tech companies and feeling uncomfortable with companies knowing everything about them, from their location to their interests to what they are purchasing. They reported these surveillance acts as "creepy" (R5) and these companies as "nasty" (R9).

The participants in the study expressed a significant degree of mistrust in the practices of Google and Facebook in particular, viewing their monitoring activities as intrusive and invasive:

> *"Over the course of the last 20 years working on the internet, I have noticed an increasing amount of activity from business entities like Google, that can only be described as creepy. The fact that Google and Facebook and other big corporations like that are able to put together so much information about us as individuals, and take advantage of that to commercially exploit it, and not even give us a cut of the profits." (R5)*

Participants raised concerns about the integration of Google's products, which they believed gave the company comprehensive access to their personal information and ability to profile and track users. Participants likewise mentioned Facebook and its ability to track and share data outside of their own site.

> *"Whatever it is that you put into your computer or your smartphone, it can be seen and it can be listened to... Facebook used to be fun, and then it destroyed democracy. So later, it stopped being fun at a certain point... And I don't feel very comfortable anymore with these companies." (R9)*

They stated that they abstain from using social media as much as they can, and in some cases, entirely, believing that the cost of disclosing information outweighed the benefits. Yet even this was sometimes considered ineffective, given the tracking that these companies use even on non-users of the site.

Participants overall had a general perception that the big tech companies are not conscientious and ethical. This led to a desire to avoid big tech companies whenever possible and choosing a product that offered them more privacy. As one participant put it,

> *"Over the past few years, I've been trying to wean myself off of Google and other, you know, big tech products, Because they are kind of, I think they're poisoning my mind." (R1)*

Privacy: Privacy is also a significant motivating factor for the adoption of Proton Mail among our participants. We characterize the different models of privacy our participants described according to their conceptualizations, similar to [43]. We found that our participants had different conceptions of privacy which sometimes overlapped. Below, we outline these models and provide examples of how they influence the participants' usage of Proton Mail.

Privacy as a fundamental right: Some participants felt that individuals have an inherent and inalienable right to privacy, and that privacy is not just a preference or a convenience, but is instead a necessity.

> *"I fully believe that privacy should be the default on the internet. It's heinous how we've let that completely fall apart. I'm appreciative of the GDPR and everything that it does... But at least in this country (USA), it's pretty much understood that you're the product if you're using the internet. The internet used to be so cool, and now it's just kind of a garbage fire." (R1)*

Privacy as Anonymity: Some participants believe individuals have the right to use the internet and other digital services without revealing their true identity or personally identifiable information. They adopted Proton Mail because it does not require them to enter their phone number in order to create an account. They can *choose* to provide it for account recovery and two-factor authentication but Proton Mail does not impose this on them. They also use pseudonyms on Proton Mail instead of their real names and like the idea that their communications and activities through that account cannot be traced back to their other email accounts. Participants also reported that they liked the fact that Proton Mail did not log their IP addresses unless they activated this feature.

Privacy as Control: Some participants felt that individuals have the right to control the collection, use, and dissemination of their information. Participants with this model mostly used Proton Mail as a secondary, separate account from their main email address, and used it for a specific task that they wanted to not be associated with their primary online identity. This way, they control the information that is associated with each account, and they are able to ensure that the information they want to keep private is only associated with their secondary email account, which often is an account that uses a pseudonym with no personally identifiable information attached to it.

Privacy as Commodity: Some participants viewed privacy as a commodity that can be bought and sold in the marketplace [41]. Some participants with this conception were particularly uncomfortable with the idea that big tech companies are taking their data and using it to their own benefit without giving any benefit to the individual the data belongs to. Others stated that they were exchanging their privacy for the services they were receiving through these tech giants.

Privacy as Secrecy: Some participants based privacy on the principle of confidentiality. They reported using Proton Mail for its encryption properties that prevent Proton from reading a user's emails.

However, not all our users understood this property. Some of them incorrectly believed that even if the emails are encrypted, it protects them from outside attacks but Proton Mail can still see all their communications. Even with this model, they believed that Proton Mail provided them with a higher level of privacy as opposed to an ordinary service, because their information could be seen only by Proton Mail and was not sold to third parties.

While the overall sentiment our participants shared was that all information deserved to be "safe" and "protected", they repeatedly mentioned that since they were not a high-profile personality and were not doing anything illegal either, they had "nothing to hide". We investigated how the participants defined and characterized sensitive information. The most recurring definition we saw was any personally identifiable information. Our participants particularly resort to Proton Mail when they require anonymity. Other definitions of sensitive information included financial or bank account details, authentication credentials such as PINs and passwords, location, and race.

Affordances: We viewed the different ways in which users interact with secure email through an affordances perspective [15, 39], broadly meaning the possibilities of ways users employed secure email to achieve their goals. We found that sometimes, our participants adopted Proton Mail for one particular reason and used it for that reason only. For example, P10 and P12 use their Proton Mail accounts for only *receiving* emails about their cryptocurrrency trades.

Another participant, R9 stated that he uses a Proton Mail account with a pseudonym and has it associated with a Facebook account. He then uses the Facebook account for selling items on marketplace and contacting potential customers. This way, his original identity is never exposed and is therefore not at risk.

Similarly, P13 uses a Proton Mail account for different micro-tasking websites and uses a pseudonym for it. In his opinion, since the micro-tasking websites do not *need* to know his real name or identity, he likes to use Proton Mail for it and then his data is not associated with his main accounts.

P18 mentioned that he sometimes needs to access his email account from different locations in the world and sometimes shares his email account with someone in a different part of the world. For him, the security measure by Gmail that tracks all IP addresses which access his account is not a desirable feature. He uses Proton Mail because it does not do so if you have your authentication logging off (which it is, by default).

Aversion to Personalized Advertisements: Aversion to personalized advertisements is also emerged as an important reason behind adoption of an encrypted email system. Some participants mentioned that they noticed Gmail scanning their emails for keywords and using that information to display personalized ads related to the content of their emails.

Some participants had experience in careers that exposed them to the kind of information collected about an individual and how that information is shared and used. These participants particularly expressed being uneasy with this practice, leading them to switch to a service like Proton Mail that does not engage in such practices.

Although some participants acknowledged that advertisements are a source of revenue for companies, the majority expressed strong dislike for personalized ads, especially when they originated from unexpected sources. Participants also understood that data was shared to third parties, and that avoiding a given service did not guarantee that the service would have no knowledge of their information. Participants had developed this mental model through personal experiences of seeing targeted ads even when they had not used used a particular service before. A majority of the participants particularly expressed this sentiment with regard to Facebook and Google, stating that anything a person does online is known to these two companies. R1, who is not a Facebook user, mentioned that he uses Proton Mail because he does not want Facebook to know all about his communications even though he does not have a Facebook account.

> *"So I wouldn't want [Facebook] to, you know, somehow manage to sniff my communications. Who doesn't hate advertising? I hate advertising." (R1)*

Trust in Proton: Proton Mail advertises itself as a company that 'protects your privacy'. About half of our participants were unaware of the specific ways their data is protected when using Proton Mail, or ways in which Proton Mail differs from other email providers in terms of its functionality. Despite this lack of understanding, they trusted the company's promise of privacy protection. They either did not know or were not concerned about the encryption of their emails, but rather placed their trust in Proton Mail's commitment to not share or exploit their data. As P14 stated, they trusted the company's reputation for protecting privacy.

> *"I'm assuming that the more privacy focused company wouldn't give away my data." (P14)*

Some participants also expressed trust in Proton Mail due to its location. They had the view that since Proton Mail is founded and based in Switzerland, it provides them a higher level of privacy as they cannot be subjected to surveillance on behalf of US or other intelligence agencies. While Proton Mail claims zero-access encryption, a few participants mistakenly believed that Proton Mail has access to all their email communications. Nevertheless, they felt safe knowing that Proton Mail, being subject to Swiss laws, would not be compelled to release their data to US or EU agencies, even when requested to do so. Similar views were expressed by participants who used Tutanota, which is based in Germany and similarly protected from having to provide data to the US government.

Conscientiousness: Some participants have adopted Proton Mail because they want to support a conscientious company. In a time where data sharing and revenue generation through advertisements and personal data sales are common, they believe that companies like Proton, which prioritize ethical and conscientious practices, should be supported. Our participants stated that users' support for companies that value ethics are important, even at the cost of certain conveniences or functional advantages. Some participants mentioned purchasing the paid plans for Proton Mail instead of using the free version because it makes them feel good about supporting an ethical company.

> *"I purchased a plus subscription to for Proton Mail, because I like supporting conscientious companies like that. So it's partially the privacy and partially it's feeling good about, you know, being a techno vegan." (P16)*

Exposure to Technology and Negative Experiences: Participants with a previous negative experience with technology cited it to be their reason of adoption of an encrypted email service like Proton Mail. Some participants who had not directly had this experience, but had heard about such incidents also felt motivated to use an encrypted email service, as seen by [32, 33] as well.

Further, some participants indicated that exposure to technology served as a driving factor for them to adopt encrypted email services. Their level of awareness about the potential for privacy violations, whether through education or their career, influenced their level of motivation to protect their privacy, since they better understood the likelihood and extent of harm.

4.2 Threat Models

We prompted the participants to think of any entities that could potentially pose a risk to their email communications. They were instructed to perform a think-aloud exercise to identify and articulate the potential threats. Here we describe the categories of attackers and their respective capabilities, as well as any preventative measures participants use to safeguard themselves against these threats.

4.2.1 Adversaries/Attackers

The adversaries our participants mentioned aligned well with the findings of [1] which found that users perceive three types of adversaries: (1) government agencies, (2) service providers, and (3) anonymous hackers. Our participants additionally differentiated between email service providers and other internet-based companies. Further, our participants often clarified that just because an entity has the ability to cause a harm does not necessarily mean that it actually will ever do so. Only one participant (P10) mentioned the risk of someone physically accessing her devices, but dismissed it saying that it is extremely unlikely.

Government and Intelligence agencies: A prevalent potential threat most of our participants perceive is surveillance by governmental agencies. While they mostly think it is unlikely for their government to spy on them and access their emails, they listed it as a possibility nonetheless. Some of our participants mentioned that The Five Eyes Alliance countries (Canada, Australia, New Zealand, the United Kingdom, and the United States) might be more likely to monitor people's email communications. Although the likelihood of such an event happening was deemed negligible, the potential consequences were described as severe. The participants emphasized that governmental entities wield considerable power and could potentially issue directives to email service providers, requiring the surrender of all relevant data. They also believed that governments typically have back doors to encryption algorithms, a sentiment also expressed by interviewees in [1]. The consequences of such an event occurring were perceived as extremely intense and life-threatening such as ethnic cleansing or political assassination.

Anonymous hackers on the internet: According to a majority of our participants, anonymous hackers on the internet pose a credible threat. Nevertheless, the participants held the view that individual attacks on their data are highly unlikely due to the Big Fish model [47] meaning that they are not a significant or "interesting" target (P14) and therefore no one would target them. Rather, the participants expressed concern about the potential for data breaches by these skilled hackers, and getting unauthorized access of corporate databases, since they had often heard such stories. Such breaches were regarded as a serious threat, given the potential to compromise their financial information, which was considered to be the primary motive for such attacks. P17, shared the following experience:

> *"I have seen that there are forums that sell used accounts, for example, for Spotify or PayPal accounts with money on them. So they mostly do it for financial motives." (P17)*

P16 shared a similar experience where their mother's Grammarly account was accessed by an unauthorized individual who obtained the account credentials through a data breach. One participant provided an additional perspective on the potential consequences of hackers gaining access to email addresses, where they could "spam the user to death" (R6) with unsolicited messages until they become overwhelmed and unable to effectively manage their inbox. The participant described this outcome as highly likely, citing personal experience as evidence.

Other Email Service Providers: Participants identified email service providers to be a potential threat to the privacy of their email communications. More than half of our participants acknowledge that while these practices constitute an infringement of privacy, they understand the economic incentives that motivate these companies to scan and read their emails. They stated that the email providers do not have any malicious motivations, but just need to earn a profit. They reported being particularly annoyed with companies that "grab their attention" and "reduce them to a number of their quarterly earning calls" (R1). Overall, participants expressed relatively low levels of concerns about email providers looking at their information. They held this view due to their belief that they do not have any sensitive information in their emails. Even when realizing that their emails contain their financial information which they consider to be sensitive, they stated that they trust the email providers to not misuse that information. They mentioned that the biggest threat through email providers is probably just targeted ads. Some participants believed that Proton Mail has similar abilities and can view and scan all their (encrypted) emails for advertising and profiling. They trusted Proton, however, to not do so.

Online companies: Many participants identified companies and services on the internet as a separate and more significant threat than email service providers. Based on their perception, such entities collect data without users' consent. In contrast to email services, which only have access to email contents, internet-based services can collect additional data across various dimensions, such as location, health information, financial information, race, and interests. Participants viewed this type of data collection as more intrusive and in-depth, hence posing a more severe threat to their privacy as well as security.

4.2.2 Mitigation Strategies

Participants were asked to describe the strategies they employed to mitigate the risks they mentioned. As seen earlier, one of the primary strategies for the threats posed by email service providers and online companies in general was to use Proton Mail. This was seen as a way to remove themselves and their data from big tech, to provide privacy, or to align their choices with companies that share similar values.

When asked about how they would send sensitive information, participants did not mention any strategies related to E2EE systems. Instead, they suggested using offline channels, such as sending the information by post or meeting the communication partner in person. One participant (P11) considered SMS to be a more secure alternative to email and recommended its use as a mitigation strategy to safeguard against information leaks. Although he acknowledged that telephone operators and governments could still access his information through SMS, he felt that it was a relatively safer option compared to the entire internet. Some participants recommended using virtual private networks (VPNs) to safeguard their online activities. In addition, some participants suggested avoiding social media altogether to prevent privacy violations on the internet.

When thinking about protecting themselves from the government, participants mentioned that there is essentially no way to escape that. Some participants expressed some confidence in using Proton Mail, given its location in Switzerland, as a mitigation strategy. However, they perceived that governments always have back doors and can gain access to any information they want, even when one is using an E2EE system, and that in the worst-case scenario, the government could resort to force to obtain their information. Some participants indicated they could protect against government surveillance by being a law-abiding citizen.

> *"If the US government or I mean, heck, even the Pakistani government really wanted to see my emails, they probably, worst comes to worst, beat it out of me." (R2)*

4.3 Mental Models

Since our sample was diverse with respect to the technical background our participants had, their mental models varied drastically depending on their technical knowledge. As we reviewed these models, we grouped them into two broad categories: (1) A Safer, More Trustworthy WebMail System, and (2) A Private, Encrypted Email System. We describe these below.

A Safer, More Trustworthy Email System: Participants with this model did not have a complicated model for what Proton Mail, or any encrypted service for that matter, does when a user tries to send an email to another user. For them, Proton Mail worked just like a regular email provider except it was *somehow* safer. Structurally, they imagined that the processing of email is similar for Proton Mail, Gmail, Outlook, or any other provider.

Participants with this model had at best only a vague understanding that Proton Mail used encryption. Some participants with this model did not know that email in Proton Mail could be encrypted, and had not seen or heard the word encryption. Some thought that all email providers use encryption, but somehow Proton Mail was safer. One participant thought that using the paid version of Proton Mail provides even better encryption than the free version, which in turn is better than using a regular email provider.

> *"But with paid Proton Mail, according to them, they're doing something that if someone tries to*

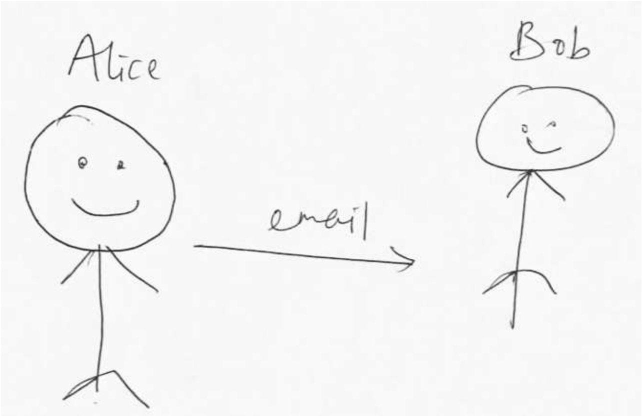

Figure 2: P10's drawing to explain how Alice sends a message to Bob in Proton Mail

> *read the email outside of the system, somehow it's encrypted. I don't know. I don't know how it works. (R6)"*

The common sentiment among participants who held this model is that they do not know Proton Mail works or how it is different than an ordinary email provider, and they probably do not *need* to know the details either. When presented with the diagramming exercise, participants with this model felt at a loss to characterize what goes on in the background when they send an email to their friend. For all they know and care, they send an email and the email is received on the other end *safely*, as Figure 2 shows.

We explored how and why these participants were perceiving Proton Mail to be safer, given that their mental model, both structurally and functionally for Proton Mail and other email providers was essentially identical. We identified that participant perception for Proton Mail originated from the fact that Proton Mail did not collect any personally identifiable information at the time of account creation. While Proton Mail asked them to provide their backup email or phone number for account recovery, this was optional, whereas Gmail and other services they used required those credentials. One participant, P17, mentioned that Proton Mail probably has a better spam filter which makes it safer.

A Private, Encrypted Email System: The other group of participants understood some of the structural properties of Proton Mail and were able to visualize and verbalize the processes involved in sending an email through the system. While some participants made technical errors in describing how encryption works, they generally understood the basic mechanisms.

Participants with this model clearly stated that Proton Mail was different than an ordinary email provider because it is end-to-end encrypted. They also understood that Proton Mail automatically encrypts emails if the sender and receiver are both using Proton Mail, and that emails are encrypted at rest so that Proton can't read them.

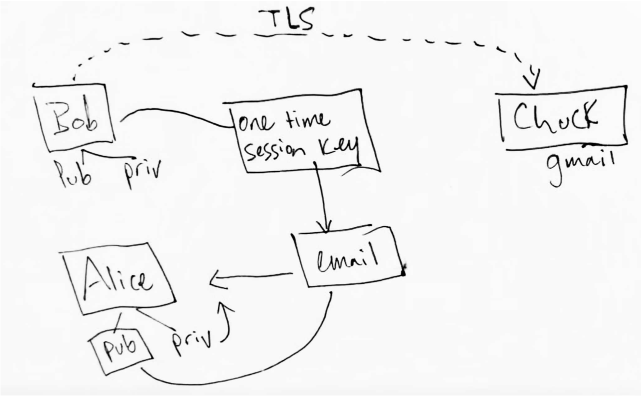

Figure 3: R1's drawing to explain how Bob sends a message to Alice in Proton Mail

Some knew that Proton Mail uses public-key encryption in combination with symmetric encryption. For example as shown in Figure 3, R1 explained this process in detail:

> *"Bob wants to send a message to Alice. If we're talking [about] both Proton Mail users, they both have key pairs. So Bob has a public key and a private key. Alice also has a public key and a private key. And if Bob is the one sending the message, Bob generates a one-time use key. So that's one time, [I] think they call it a session key and uses this key and Alice's public key to encrypt his email. Actually, I should have said, Bob has Alice's public key, [he] uses Alice's public key to encrypt the session key and the one time session key to encrypt the email, which then Alice can decrypt with her private key." (R1)*

Participants with this model clearly distinguished that with ordinary providers, none of these encryption processes are done except that the emails are encrypted in transit through Transport Layer Security protocol (TLS) for security, but that does not protect them from the provider itself because the provider has "all the keys for all the emails". They understood that sending emails from an E2EE email provider to some ordinary provider does not automatically encrypt any emails, whereas encryption automatically happens if both parties use the same E2EE provider. Most participants with this model were aware that Proton Mail provides a password-protected email option that encrypts outgoing emails to someone who is not on Proton Mail. The interviewer hinted at this feature for those who did not mention it themselves. They recalled seeing it but reported almost never using it.

None of the participants with this model mentioned digital signatures, or address verification. They seemed to trust Proton Mail to distribute the correct keys. They had never seen a warning from Proton Mail about any public key changes for their contacts. They also did not mention the *expiration time* feature for emails sent to other providers, which enables a sender to remove access after a predefined period of time.

4.4 Usage

In this section, we report the ways in which our participants employ end-to-end encrypted email.

What they use it for: About half of our participants mentioned using Proton Mail as their primary personal email account, using it to sen med and receive all personal emails through it. A few participants mentioned using their Proton Mail account exclusively for work and communicating with clients since they perceived their nature of work as sensitive, and that using Proton Mail gave a more creditable look and looked more professional. Some participants mentioned using Proton Mail exclusively for all their communications.

> *"Exclusively for both [work and personal] emails, but in terms of how much time I invest, it's probably around about 75% work and 25% personal." (R7)*

Many of the participants stated using their Proton Mail email addresses as separate, disposable accounts. The main reasons for this are that no personally identifiable information is required to set up an account, thereby simplifying the registration process. Additionally, since these accounts are not linked to their primary online identity, they leverage these 'anonymous' accounts to perform tasks they do not want associated with their main email address. Examples of such tasks include gaming, trading cryptocurrency, completing microtasks on websites such as Prolific, and using Proton Mail as a shared account among multiple in different locations, which they perceived easier due to Proton's no-IP logging policy.

Several participants cited an additional use to exclusively receive newsletters and other superfluous email correspondence, which could otherwise inundate their primary email account. Some participants reported adopting several different email addresses as a means of efficiently managing email content and compartmentalizing them according to distinct purposes, for example using Proton Mail for financial communications, Tutanota for shopping websites, Gmail for everyday usage, and Outlook for school and work-related emails (R8).

Sending to non-Proton Mail users: We asked participants about how they sent emails to contacts who were not using Proton Mail, and their responses indicated that they treated it no differently from sending emails to other Proton Mail users. While some participants mentioned being aware of the password-protected email option offered by Proton Mail, they reported rarely or almost never using it. Even when we hinted at this feature to those who did not mention it, they stated that it was not a feature they ever use. Essentially, our participants are sending and receiving unencrypted emails despite using Proton Mail, since most of their communication partners are not using the platform.

5 Discussion

We didn't seek to validate any general theories of technology adoption. However, TAM seems to broadly apply, since users identify strongly with the usefulness of secure email and current web-based systems have usability roughly similar to popular clients like Gmail. Likewise PMT appears to explain adoption well, since participants have identified specific privacy threats that are highly likely to affect them, Proton Mail offers a reasonable way to mitigate those threats, and they are confident in their ability to use the system. Because these are general theories, they don't adequately capture the broader motivations of our participants, particularly those centered on privacy.

Our study leads to the following takeaways.

5.1 Privacy is a key motivation

In reviewing our findings for each research question, we find that a variety of factors lead to adopting secure email, including distrust of big tech and aversion to the surveillance economy, various notions of privacy, affordances, trust in a company offering these products, and a desire to align decisions with companies that share their values. Privacy permeated many of these motivations.

Privacy also played a role in how participants reacted to perceived threats. Participants who regarded government surveillance as a threat viewed it as highly consequential and potentially life-threatening; however, they did not consider themselves likely targets, and therefore, this was not their primary motivation for adopting encrypted email. Conversely, all participants acknowledged the widespread use of personal data by corporations for targeted advertising, which while a significant invasion of privacy, was not life-threatening. Despite its comparatively lower severity, this threat was more compelling to users, motivating them to adopt ProtonMail.

Furthermore, while security was an added benefit of using encrypted email, it was not primarily security that drove these people to use secure email. Some participants indicated they prioritize privacy over security, preferring Proton Mail because it doesn't ask them for an email or phone number for account verification. Privacy was strongly prevalent among participants who had "A Safer, More Trustworthy Email System" mental model, perhaps because they were unaware of the security threats to their communications and were more exposed to privacy threats.

Although our findings align most closely with Solove's conceptualizations of privacy [42], we did not observe all of the conceptualizations they identified in our research. Moreover, we identified some additional conceptualizations that were not accounted for in Solove's framework. Some participants were highly aware of privacy from the perspective of collection and control of information [27], and some expressed weighing costs and benefits of using a free email system [20, 24]. Thus our participants have diverse understandings of privacy which cannot be easily categorized within a singular privacy framework.

5.2 Privacy benefits are broad

Despite the significant desire for privacy, participants appear to largely be sending unencrypted email to contacts outside of the secure email system they are using. Previous literature has identified inaccurate mental models as a barrier to effective usage of secure technologies [3, 49]. Our results show that even when users possess well-formed mental models with respect to both structural and functional properties, they generally use unencrypted email communication. They understand and are aware that their emails remain unencrypted when communicating with non-users of Proton Mail, which is the case the majority of the time.

The reason for this apparent disconnect is partly rooted in differences in the affordances of secure email systems as viewed by some participants when compared to the expectations of security experts. Many participants found value in pseudonymity (having an email disconnected from their usual account), in avoiding big tech companies, in controlling where their data is stored, or in supporting companies that aligned with their values. Thus privacy benefits are viewed rather broadly, and not tied solely to the ability to send or receive encrypted emails.

5.3 Privacy benefits can be expanded

The relatively low use of encrypted emails among participants does present a significant opportunity for research and industry to *increase* the privacy benefits for secure email users. Future research should explore ways to encourage or nudge users toward password-protecting their emails when sending to users outside the system. There is likely some overlap in methods with research seeking to encourage users of password managers to choose strong passwords instead of storing weak passwords in their password manager [54]. For example, a system could display periodic reminders suggesting emails be encrypted or could display a banner indicating the percent of emails sent in the past week were private.

One clear way to provide greater privacy for existing users is to enable interoperability between secure email systems. Currently, Tutanota does not support PGP, instead uses a proprietary system based on AES and RSA. As a result, it does not automatically recognize and allow importing of public keys attached to an outgoing email from Proton Mail. This prevents users from two large secure email systems from communicating with encrypted emails unless they manually set a password. On the other hand, Proton Mail can exchange secure email with the FlowCrypt Gmail extension, provided the user knows how to attach their public key to an outgoing Proton Mail email, which is not done by default and which is hidden in the user interface behind a menu labeled "..." at the bottom of the compose window. Secure email providers could work together to provide both better support for interoperability and better user experiences for sending encrypted emails. A major challenge is helping users decide whether they should trust another user's key. Trust might be increased by having secure email services automatically retrieve a key for a user from their provider, with that key being signed by the user's email provider.

Ultimately, the best way to provide greater privacy is for secure email systems to have greater numbers of users. Email sent between users of the same system are encrypted by default. One possible avenue is to explore the effect of advertising privacy as the primary feature offered by these systems. Typically marketing literature mixes privacy benefits with promotion of security benefits, while using specialized jargon about encryption. For example, Proton Mail's home page uses the tagline "Secure email that protects your privacy", leading with "secure", and also promotes "independently audited end-to-end encryption and zero-access encryption to secure your communications". Later the home page for Proton Mail explains that encryption "protects against data breaches and ensures no one (not even Proton) can access your inbox". At least some of our users did not notice or understand these benefits. How can industry encourage greater understanding of the benefits of secure email? Would greater awareness and understanding yield more users?

6 Conclusion

Among those we interviewed, privacy concerns are a significant motivator for adopting a secure email system. Web-based systems such as Proton Mail are relatively new options in this space, and participants value the ability to use these accounts to achieve a measure of privacy. These benefits are recognized and appreciated even by those without a deep understanding of encryption, in part because those benefits are significantly broader than traditionally recognized by the security community. Additional research is needed to encourage greater use of encryption, to enable interoperability among providers, and to expand awareness and understanding of the benefits offered by privacy technologies.

Acknowledgments

This research is supported in part by the National Science Foundation under Grant No. CNS-1816929.

References

[1] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith. Obstacles to the adoption of secure communication tools. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 137–153, 2017.

[2] Nora Alkaldi and Karen Renaud. Why do people adopt, or reject, smartphone password managers? *1st European Workshop on Usable Security*, pages 1–14, 2016.

[3] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle. A usability study and critique of two password managers. In *15th USENIX Security Symposium (USENIX Security 06)*, Vancouver, B.C. Canada, July 2006. USENIX Association.

[4] Jeremy Clark, Paul C van Oorschot, Scott Ruoti, Kent Seamons, and Daniel Zappala. Sok: Securing email—a stakeholder-based analysis. In *Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part I 25*, pages 360–390. Springer, 2021.

[5] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. "it's not actually that horrible" exploring adoption of two-factor authentication at a university. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2018.

[6] Sanchari Das, Andrew Dingman, and L Jean Camp. Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key. In *Financial Cryptography and Data Security: 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26–March 2, 2018, Revised Selected Papers 22*, pages 160–179. Springer, 2018.

[7] Sanchari Das, Andrew Kim, Ben Jelen, Joshua Streiff, L Jean Camp, and Lesa Huber. Why don't older adults adopt two-factor authentication? In *Proceedings of the 2020 SIGCHI Workshop on Designing Interactions for the Ageing Populations-Addressing Global Challenges*, 2020.

[8] Fred D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3):319–340, 1989.

[9] Zakir Durumeric, David Adrian, Ariana Mirian, James Kasten, Elie Bursztein, Nicolas Lidzborski, Kurt Thomas, Vijay Eranti, Michael Bailey, and J. Alex Halderman. Neither snow nor rain nor mitm...: An empirical analysis of email delivery security. In *Proceedings of the 2015 Internet Measurement Conference*, IMC '15, page 27–39, New York, NY, USA, 2015. Association for Computing Machinery.

[10] Agnieszka Dutkowska-Zuk, Austin Hounsel, Andre Xiong, Molly Roberts, Brandon Stewart, Marshini Chetty, and Nick Feamster. Understanding how and why university students use virtual private networks. *arXiv preprint arXiv:2002.11834*, 2020.

[11] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into iot device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2019.

[12] Chris Fennell and Rick Wash. Do stories help people adopt two-factor authentication? *Studies*, 1(2):3, 2019.

[13] Kevin Gallagher, Sameer Patil, and Nasir Memon. New me: Understanding expert and non-expert perceptions and usage of the tor anonymity network. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 385–398. USENIX Association, 2017.

[14] 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, page 13–24, New York, NY, USA, 2005. Association for Computing Machinery.

[15] William W Gaver. Technology affordances. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 79–84, 1991.

[16] Shirley Gaw, Edward W. Felten, and Patricia 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, page 591–600, New York, NY, USA, 2006. Association for Computing Machinery.

[17] Dennis A Gioia, Kevin G Corley, and Aimee L Hamilton. Seeking qualitative rigor in inductive research: Notes on the gioia methodology. *Organizational research methods*, 16(1):15–31, 2013.

[18] Hana Habib, Jessica Colnago, Vidya Gopalakrishnan, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, and Lorrie Faith Cranor. Away from prying eyes: Analyzing usage and understanding of private browsing. In *Fourteenth symposium on usable*

privacy and security (SOUPS 2018), pages 159–175, 2018.

[19] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. " it's a scavenger hunt": Usability of websites' opt-out and data deletion choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2020.

[20] Il-Horn Hann, Kai-Lung Hui, Tom Lee, and Ivan Png. Online information privacy: Measuring the cost-benefit trade-off. *ICIS 2002 proceedings*, page 1, 2002.

[21] Louis Harris, Alan F Westin, et al. Consumer privacy attitudes: A major shift since 2000 and why, 2003.

[22] David Jonassen and Young Hoan Cho. Externalizing mental models with mindtools. *Understanding models for learning and instruction*, pages 145–159, 2008.

[23] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, pages 39–52. Ottawa, 2015.

[24] Robert S Laufer and Maxine Wolfe. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues*, 33(3):22–42, 1977.

[25] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I Hong. Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings. 2014.

[26] James Maddux and Ronald Rogers. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19:469–479, 09 1983.

[27] Naresh K Malhotra, Sung S Kim, and James Agarwal. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information systems research*, 15(4):336–355, 2004.

[28] Peter Mayer, Collins W Munyendo, Michelle L Mazurek, and Adam J Aviv. Why users (don't) use password managers at a large educational institution. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1849–1866, 2022.

[29] Moses Namara, Daricia Wilkinson, Kelly Caine, and Bart P Knijnenburg. Emotional and practical considerations towards the adoption and abandonment of vpns as a privacy-enhancing technology. *Proceedings on Privacy Enhancing Technologies*, 2020(1):83–102, 2020.

[30] Helen Nissenbaum. Privacy as contextual integrity. *Wash. L. Rev.*, 79:119, 2004.

[31] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, pages 319–338, 2019.

[32] Katharina Pfeffer, Alexandra Mai, Edgar Weippl, Emilee Rader, and Katharina Krombholz. Replication: Stories as informal lessons about security. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 1–18, 2022.

[33] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, pages 1–17, 2012.

[34] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. Why doesn't jane protect her privacy? In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 244–262. Springer, 2014.

[35] Ronald W. Rogers. A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, 91(1):93–114, 1975. PMID: 28136248.

[36] Scott Ruoti, Jeff Andersen, Luke Dickinson, Scott Heidbrink, Tyler Monson, Mark O'neill, Ken Reese, Brad Spendlove, Elham Vaziripour, Justin Wu, Daniel Zappala, and Kent Seamons. A usability study of four secure email tools using paired participants. *ACM Trans. Priv. Secur.*, 22(2), April 2019.

[37] Scott Ruoti, Jeff Andersen, Travis Hendershot, Daniel Zappala, and Kent Seamons. Private webmail 2.0: Simple and easy-to-use secure email. UIST '16, page 461–472, New York, NY, USA, 2016. Association for Computing Machinery.

[38] 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, August 2018. USENIX Association.

[39] Andrea Scarantino. Affordances explained. *Philosophy of Science*, 70(5):949–961, 2003.

[40] Steve Sheng, Levi Broderick, Colleen Alison Koranda, and Jeremy J Hyland. Why johnny still can't encrypt: evaluating the usability of email encryption software. In *Symposium On Usable Privacy and Security*, pages 3–4. ACM, 2006.

[41] H Jeff Smith, Tamara Dinev, and Heng Xu. Information privacy research: an interdisciplinary review. *MIS quarterly*, pages 989–1015, 2011.

[42] Daniel J Solove. Conceptualizing privacy. *California law review*, pages 1087–1155, 2002.

[43] Daniel J Solove. Understanding privacy. 2008.

[44] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. Awareness, adoption, and misconceptions of web privacy tools. *Proceedings on Privacy Enhancing Technologies*, 2021(3):308–333, 2021.

[45] Christian Stransky, Oliver Wiese, Volker Roth, Yasemin Acar, and Sascha Fahl. 27 years and 81 million opportunities later: Investigating the use of email encryption for an entire university. IEEE Computer Society, May 2022.

[46] Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3):425–478, 2003.

[47] Rick Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, pages 1–16, 2010.

[48] Alan F Westin et al. The dimensions of privacy: A national opinion research survey of attitudes toward privacy. 1979.

[49] Alma Whitten and J. D. Tygar. Why johnny can't encrypt: A usability evaluation of PGP 5.0. In *8th USENIX Security Symposium (USENIX Security 99)*, 1999.

[50] Pamela Wisniewski, AKM Islam, Heather Richter Lipford, and David C Wilson. Framing and measuring multi-dimensional interpersonal privacy preferences of social networking site users. *Communications of the Association for information systems*, 38(1):10, 2016.

[51] Allison Woodruff, Vasyl Pihur, Sunny Consolvo, Lauren Schmidt, Laura Brandimarte, and Alessandro Acquisti. Would a privacy fundamentalist sell their dna for $1000... if nothing bad happened as a result? the westin categories, behavioral intentions, and consequences. In *Symposium on Usable Privacy and Security (SOUPS)*, volume 5, page 1, 2014.

[52] Justin Wu and Daniel Zappala. When is a tree really a truck? exploring mental models of encryption. In *SOUPS@ USENIX Security Symposium*, pages 395–409, 2018.

[53] Shikun Zhang, Yuanyuan Feng, Yaxing Yao, Lorrie Faith Cranor, and Norman Sadeh. How usable are ios app privacy labels? *UMBC Faculty Collection*, 2022.

[54] Samira Zibaei, Dinah Rinoa Malapaya, Benjamin Mercier, Amirali Salehi-Abari, and Julie Thorpe. Do password managers nudge secure (random) passwords? In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 581–597, Boston, MA, August 2022. USENIX Association.

[55] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2020.

Appendix

A. Interview Guide

Before we start, I just wanted to say thank you for agreeing to help us with our research project. We really value what you have to say. I also want to be sure you know that there are no right or wrong answers to the questions I'm going to ask. We really just want to hear what you think and feel and hear your opinions. Also, if you're ever confused by a question I'm asking, please let me know, and I'll try to explain or rephrase. I will be recording this interview to transcribe the data. Your video will not be used, and it will be discarded as soon as I get the interview transcribed.

Opening Questions

- Do you have any questions before we start?
- Where do you currently live? How long have you lived there?
- Do you have a CS background? What do you do?
- Verify if they use ProtonMail or Tutanota or not.

Adoption

- How did you first hear about (ProtonMail/Tutanota)?
- Why did you decide to start using (ProtonMail/Tutanota)?
  - Was there a specific event that caused you to use (ProtonMail/Tutanota)?
  - Did you consider using any other encrypted email services?
- Why do you currently use (ProtonMail/Tutanota)?
  - Are there multiple reasons?
  - How would you rank these reasons in order of priority?
  - What kind of information do you regard as "sensitive"? (if applicable)
- What do you particularly like about (ProtonMail/Tutanota)? Dislike about (ProtonMail/Tutanota)?
- Do you use WhatsApp? Signal? Viber? Why or why not?
  - What are the pros of using (ProtonMail/Tutanota) over a more traditional email provider?
  - What are the drawbacks of using (ProtonMail/Tutanota) over a more traditional email provider?
    - Are these sets of pros/cons acceptable?
    - Do any of these contribute to your use of a normal email provider?
- Perception
  - How would you rank yourself on how much you care about security and privacy? On a scale of 1-5?
  - Why is that?
  - How would other people rank you?
- Evangelism
  - Have you ever encouraged your friends to use secure email?
  - Why or why not?
  - What would be the 'talking points' of (ProtonMail/Tutanota) if you were to suggest it to someone?
  - (If yes to above) Do people tell you they are not interested in secure email? What are their reasons? How do you deal with that?
  - Have you ever helped anyone get started with (ProtonMail/Tutanota)? What did they need help with? Tell me about an instance.

Threat model

- Are there entities that you feel would access or misuse your email data if they could get it?
  - Who are they?
  - If you could rank these threats, which are the most likely or most severe?
  - Why do you think they would try to access your information?
- What would be the consequences of someone being able to read your emails?
- What would be the consequences of someone modifying an email you sent?
- What would be the consequences of someone forging an email that was supposedly from you?
- Do you have other accounts that could be compromised if your emails get compromised and read by someone else?

Mental Models

- How do you think (ProtonMail/Tutanota) works?
- Could you draw us a picture of what is involved when a person, Bob, sends an email to another person, Alice, when they are both using (ProtonMail/Tutanota)?
  - How is the email kept secure or private?
- Could you draw another us a picture of what is involved when a person, Bob, sends an email to another person, Alice, but Bob is using (ProtonMail/Tutanota) and Alice is using Gmail?
  - How is the email kept secure or private?
- (ProtonMail/Tutanota) is often advertised as being "secure". What do you think that means?
- (ProtonMail/Tutanota) is also often advertised as offering "privacy"? What do you think that means? How is it different from security?
- Do you feel confident that you know enough about technology to use (ProtonMail/Tutanota) successfully?
- Do you feel a person would need your level of understanding to use (ProtonMail/Tutanota) successfully?

Usage

- What do you use your secure email account for?
  - Do you use it as your primary email account?
  - (if applicable) do you use it for all emails or some emails?
  - If you use a non-secure email account as well, how do you decide which to use and when?
- What features do you wish your secure email service had that are not currently offered?
  - Do you have any difficulties using your secure email service?
  - Can you tell us about one recent instance?
- Do you insist people send you email using a secure email service?
  - If so, how is this received?
- Are there any particular features of (ProtonMail/Tutanota) you really like?
- Can you easily email people who do not use (ProtonMail/Tutanota)?
  - (if not) How much does this affect you on a daily or weekly basis?

  - Would adding this feature be a high priority for you?

- If you need to send sensitive information to someone who is not using (ProtonMail/Tutanota), what do you do?
  - How often does that happen?

- Does it bother you when you have to send emails to non-protonmail users? (because gmail or other service providers still do have access to it)

Ending

- How effective do you think your choice of shifting to secure email has been in protecting your privacy? Especially because most of your friends do not use secure email?

- (if applicable) Don't you think Google can still profile you and see your emails if you send email from ProtonMail to Gmail?

- What other steps do you take to protect your privacy (Other search engines, VPNs, etc?)

B. Participant Demographics

Table 1: Demographics of the interview participants

ID	Age	Country	Gender	Education Level	Tech Background	Using for	Frequency of Usage
R1	35-44	United States	Male	G/PD	Yes	5+ years	Daily
R2	45-54	United States	-	G/PD	Yes	5+ years	Daily
R3	45-54	United States	Male	BA/BS	Yes	5+ years	Weekly
R4	45-54	United States	Male	BA/BS	Yes	5+ years	Weekly
R5	45-54	Australia	Male	G/PD	Yes	5+ years	Daily
R6	45-54	United States	Female	BA/BS	No	5+ years	Daily
R7	25-34	United States	Male	G/PD	No	2-3 years	Weekly
R8	25-34	United States	Male	BA/BS	Yes	5+ years	Monthly
P9	35-44	Canada	Male	G/PD	No	few months	Daily
P10	25-34	Portugal	Female	G/PD	No	1 year	1-2 times a year
P11	18-24	Poland	Male	HS	No	2-3 years	Monthly
P12	35-44	Mexico	Non-Binary	BA/BS	Yes	5+ years	Monthly
P13	25-34	Portugal	Male	BA/BS	No	2-3 years	1-2 times a year
P14	25-34	Netherlands	Male	G/PD	No*	1 year	Weekly
P15	35-44	United Kingdom	Female	G/PD	No	2-3 years	Daily
P16	18-24	Spain	Male	Some college	Yes	1 year	Weekly
P17	25-34	Poland	Male	G/PD	Yes	few months	1-2 times a year
P18	25-34	Mexico	Male	BA/BS	Yes	5+ years	Monthly
P19	25-34	Switzerland	Non-binary	HS	No	5+ years	Daily
P20	25-34	Australia	Male	G/PD	No	5+ years	1-2 times a year
P21	25-34	Greece	Male	G/PD	No	5+ years	Weekly
P22	25-34	Mexico	Male	BA/BS	No	5+ years	Weekly
P23	25-34	Japan	Male	BA/BS	Yes	1 year	Monthly
P24	18-24	Poland	Male	HS	Yes	2-3 years	1-2 times a year
P25	18-24	Poland	Male	Some college	No	1 year	Daily

G/PD = Graduate/Professional Degree
BA/BS = Bachelor's Degree
HS = High School

* P14 mentioned being interested in cybersecurity, but does not have a formal background in it.