"You do understand that people don't trust technology?": Explaining Trusted Execution Environments to Non-Experts

McKenna McCall*†
Colorado State University
mckenna.mccall@colostate.edu

Carolina Carreira*
Carnegie Mellon University and IST University of Lisbon, INESC-ID
cdacunha@andrew.cmu.edu

Miguel Flores
Carnegie Mellon University
miguelfl@andrew.cmu.edu

Lorrie Faith Cranor
Carnegie Mellon University
lorrie@cmu.edu

Abstract

Trusted Execution Environments (TEEs) protect confidentiality and integrity of trusted applications by creating an isolated environment for executing code. Prior work has shown that users may feel more comfortable sharing data when they know it will be protected by a TEE—especially if they understand what a TEE is. In this study, we evaluated text-based explanations introducing TEEs to non-experts. We analyzed existing TEE explanations to develop candidate explanations and evaluated them via vignette scenarios with 966 crowdworkers. The explanations that enhanced understanding most were *non-technical* ones that highlighted specific threats that can be *prevented* by a TEE. Surprisingly, even the explanations that enhanced understanding had little effect on willingness to use the TEE-enhanced technology. These results provide insights into ways to communicate technical security concepts more effectively but also suggest that explaining security technology might not be enough to address users' privacy concerns.

Keywords

Usable Security, Trusted Execution Environments

1 Introduction

While the demand for users to share their data grows, consumers are expressing concern and confusion about how their information is used [40]. Confidential computing [21] seeks to protect users by restricting computations on sensitive data to Trusted Execution Environments (TEEs). These environments guarantee the authenticity of the executed code, the integrity of the runtime states, and the confidentiality of the code and data [48]. Confidential computing and TEEs have applications in AI and machine learning [20, 42, 60], IoT [13], and blockchain smart contracts [61].

TEEs are not only being explored for their technical strengths. Prior work also suggests that when users are made aware of cloud-based TEEs in home IoT devices, they may feel more comfortable with their data being collected [43]—especially when they understand what a TEE is. However, this work did not investigate how technologists should explain TEEs to end-users, which is itself a challenge. Unlike some security concepts like passwords, most people are not familiar with TEEs, or even the technologies they rely on. While fully explaining TEEs to a non-technical audience may not be feasible, understanding all of the technical details may not be necessary to understand enough of the security benefits they offer to help users feel secure. Indeed, the original study investigating the impact of TEEs on comfort evaluated understanding based on just three high-level TEE concepts [43].

In this study, we evaluate strategies for explaining TEEs to enhance both *understanding* of the capabilities of a TEE as well as *comfort* using TEE-enhanced technologies. Ideally, an explanation would be nuanced enough to communicate what guarantees TEEs offer—without over-promising or being overly pessimistic about risks, which could discourage people from using technology. We based our explanations on common themes we found in existing TEE explanations from technical websites, forums, research papers, and popular media. We evaluated candidate explanations through a series of True/False questions via two online surveys of 966 Prolific crowd workers. We used vignettes in our surveys to evaluate explanations across different scenarios where TEEs might be used. We include home IoT scenarios, AI, and medical research applications, as they have been identified as potential use cases for TEEs [29].

Our first survey addresses two research questions:

- **RQ1:** Which explanations improve TEE *understandability* for non-experts? Is there a best overall explanation or do different scenarios benefit from different explanations?
- **RQ2:** Which explanations enhance *willingness* to use the TEE-enhanced technology? Which ones promote the feeling that data will be *safe*?

Based on the results of our first survey, we developed an FAQ to supplement our explanations by answering real questions asked by our participants. We also asked follow-up questions to better understand what contributes to the perception of safety. In the second survey, we answer the following research questions:

- **RQ3:** Does an FAQ further improve understandability? Does it increase willingness to use TEE-enhanced technology or the feeling of safety?
- **RQ4:** Which aspects of TEE scenarios contribute to the belief that data would be safe/unsafe?

To the best of our knowledge, ours is the first study to investigate strategies for explaining TEEs to non-experts. While we found that many existing explanations use technical jargon and focus on broad security guarantees (e.g., attestation, confidentiality, and integrity), what performed best in our experiments were *non-technical* explanations that highlighted specific attacks *prevented* by a TEE. We also

*Both authors contributed equally to this research.
†This work was completed while McKenna was at Carnegie Mellon University.

found that people generally answered comprehension questions correctly when we provided information directly in our explanations or FAQs, but struggled to answer questions that required them to make inferences based on our explanations.

Surprisingly, in contrast with prior work [43], we found that our explanations had little effect on willingness to use TEE-enhanced technology or feelings of safety. We believe that this is due to methodological differences between ours and the previous study (namely that we focus on high-level feelings of comfort and safety, while they focused on specific data-sharing conditions) and, importantly, our observation that TEEs cannot address all of the privacy concerns raised by our participants. These results provide insights into ways to communicate technical security concepts more effectively but also suggest that explaining security technology, while useful for improving transparency, might not be enough to address users' privacy concerns.

The paper is organized as follows: Section 2 covers background and related work; Section 3 explains our methods for collecting and analyzing existing TEE explanations to identify themes for testing via our surveys; Section 4 describes our survey methods; Sections 5 and 6 present the results of our two surveys; Section 7 includes additional discussion; finally, Section 8 concludes.

2 Background and Related Work

In this section, we describe background on TEEs. Next, we outline some related work on the importance of communicating with users about security. Finally, we summarize work that has attempted to explain technical security concepts to end-users.

2.1 Trusted Execution Environments

TEEs are combinations of several security processes, including hardware security extensions, cryptographic modules, secure distributed systems protocols, and more. According to Sabt et al. [48], a TEE can be defined as a tamper-resistant processing environment that guarantees the *confidentiality* and *integrity* of the executed code and data (preventing unauthorized reading and modification, respectively). A TEE also provides remote *attestation*, a process where the TEE proves to a remote verifier (such as a server) that it is operating securely and that the integrity of its code and data has not been compromised.

TEEs can be found in many Android phones. Authentication in Android is typically handled by code residing in a TEE based on ARM TrustZone [9], a set of security extensions that enable ARM processors to run in two distinct modes—secure and non-secure. Most Androids also use TEEs to process mobile payments, secure banking, device reset protection, and detect malware [8].

Another type of TEE, Intel SGX, allows applications to create protected areas in memory in some Intel CPUs [35] and also has applications in smart home devices. Ayoade et al. [13] propose using Intel SGX for decentralized data management in smart home applications. There are several other TEE technologies in the realm of confidential computing that target cloud computing, such as AMD SEV-SNP [7], Intel TDX [36], and ARM CCA [11].

Confidential computing is particularly relevant in the medical domain, because patient data, such as data from clinical trials, has some of the strongest legal protections in the US [1, 31]. Data aggregation enabled by confidential computing gives healthcare providers the ability to improve patient or research outcomes while safeguarding patient privacy [6]. TEEs could be used to protect machine learning for medical applications and ensure compliance with medical regulations [20].

2.2 Importance of Understanding Security Technology Basics

While technical expertise may be required to understand the details of security technology, even a basic understanding can help users make informed decisions and better protect themselves, while misconceptions and poor usability can lead to worse outcomes. An early example of opaque security technology hindering users can be found in the seminal paper by Whitten et al., which provides empirical evidence that users who lack understanding about how public key encryption works behave in ways that undermine the security and privacy of their encrypted email. The authors conclude that an unusable or incomprehensible security mechanism will not be used effectively and thus not provide security [62].

Misunderstanding the use and limitations of security tools can lead to a false sense of security [3, 32]. This overconfidence may lead them to engage in riskier behaviors under the mistaken belief that they are protected. For instance, Bravo-Lillo et al. [15] showed that misconceptions about web browser security warnings can give users an illusion of safety. In addition, interview [58] and survey studies [57] have investigated users' misconceptions about how attackers steal passwords, finding that misconceptions led users to believe vulnerable passwords were secure.

Misconceptions about security tools and design choices can also hinder their adoption [44]. Users may also face usability challenges with cookie banners due to their design [14]. Similarly, users struggle to comprehend iOS privacy labels because of jargon and unfamiliar terminology [64, 66]. On the other hand, informing users about security technology can have a positive impact. For example, Furnell et al. [28] find that more information can motivate users to choose strong passwords. When security- and privacy-enhancing technologies are mentioned to users as part of the consent process, users need a basic understanding of what protections these tools can and cannot offer if they are to make an informed decision. The European Union's GDPR [27] requires that organizations must provide clear and accessible information to ensure users understand how their data is used. Similarly, in the US, HIPAA [1] mandates that healthcare providers give patients clear information about their privacy rights and how their medical information is shared.

While most of the work in this space focused on technologies users employ to protect themselves, explaining TEEs is a fundamentally different task since they are hidden from users. Our goal in explaining TEEs is more to improve transparency and comfort than to change user behavior.

2.3 Explaining Technical Concepts

Our study builds upon prior work on short explanations to communicate technical concepts and evaluate them using online surveys [4, 24, 51]. Prior work on explaining security concepts mostly focused on perceived security [24, 53] and did not address comprehension or focus on non-TEE related contexts [4, 4, 16, 51].

Several research studies have proposed and tested explanations of other technical security concepts with end-users. Research on formal verification has also emphasized the importance of communicating technical concepts to non-technical audiences and identified it as a priority and a challenge for future work [18].

Xiong et al. [65] attempted to explain differential privacy with experiments to investigate the effects of different communication approaches. They found that, despite the positive effect of the explanations, participants struggled with understanding some of the more technical jargon. Karegar et al. [37] studied a possible solution by addressing the impact of metaphor-based explanations of differential privacy. They found that metaphors can aid understanding but may lead to misconceptions. Cummings et al. [23] attempted to design better explanations about differential privacy but highlighted the difficulty of crafting explanations that satisfy user interest and preserve the integrity of the technical content.

Similar to our work, Akgul et al. [4] investigated whether text-based explanations improve users' mental models of encryption. They found that changing pre-existing mental models can be challenging, but educational interventions can work. Interestingly, they concluded that their explanations may have slightly oversold the capabilities of encryption. Shen et al. investigated users' understanding of smartphone permissions and observed that short explanations within user interfaces led to better comprehension. The authors found that adding information to permissions dialogues made it more clear to users how their choice affected the way that their location would be tracked [51]. When it comes to explaining encryption, not all authors agree. Distler et al. [24] attempted to explain encryption and concluded that explaining encryption does not necessarily maximize perceived security. They focused primarily on the feeling of security and did not study users' comprehension of encryption. This is also the case for Stransky et al. [53], but their results suggest that using text disclosures about encryption makes users feel more secure seem more effective than iconography.

OS and browser security warnings are designed to provide actionable security information to non-technical users [16, 50]. Wu et at. [63] show that warning notifications in Signal can improve comprehension of the purpose of security mechanisms and promote favorable privacy outcomes. Well-designed password meters can be an effective communication tool to inform users about their password complexity and are a good way to provide actionable feedback about password strength [56]. Privacy and security "nutrition" labels are designed to provide succinct information to users that can inform their decision-making [26, 39].

To our knowledge, the only other attempt to communicate about TEEs to end-users is from Musale et al. [43], who investigated the impact of TEEs on data-sharing preferences. They also looked at the impact of understanding TEEs, finding that people who understood TEEs were more likely to be comfortable sharing their data. For example, they found that participants who understood TEEs were significantly more comfortable with their data being collected if they were "notified" of the data collection than those who did not understand TEEs. To assess TEE comprehension, the authors asked three True/False questions about secure storage, secure computing, and remote attestation. In one question, they ask whether the statement "non-authorized persons can modify/change the nature of the algorithm being used or gain access to the image database" is true or false. While their study focused on understanding the impact of TEEs on existing privacy norms, ours focuses on how to effectively explain TEEs. For this reason, we conduct a broader assessment of 10-12 questions that address different aspects of a TEE. We also focus on high-level feelings of comfort and safety instead of specific data-sharing conditions. While their work did attempt to explain TEEs to their participants, the goals and methodologies of that study were fundamentally different from ours.

3 Developing Candidate TEE Explanations

In this section, we describe our approach for developing candidate TEE explanations, which is based on a technique from prior work on differential privacy [23] and other guidelines for writing effective explanations [24, 49]. First, we describe how we analyzed existing TEE explanations from technical websites, forums, research papers, and popular media to identify common themes. Next, we explain how we used these themes to develop explanations for evaluating in our study.

3.1 Identifying Existing TEE Explanations

We conducted a Google search using the term "Trusted Execution Environment" and restricted results to the last five years. The first five pages of results included 42 unique URLs that had 32 TEE explanations. These results came from diverse sources, mostly aimed at an audience of technical experts. We obtained eight additional explanations through searches targeting well-known, general audience platforms like the New York Times, Medium, and Forbes.

We removed 12 sources from the initial 50 that did not include substantive TEE explanations (i.e., the source mentioned TEEs, but did not provide any explanation about what they are). We removed two others because their explanations were incorrect or misleading. We analyzed the explanations from the 36 remaining sources to identify themes to test in our experiments. 19 sources came from technology-focused websites from companies that provide TEEs (e.g. Intel, NVIDIA, AWS). Media sources, including general audience magazines and news websites, accounted for 6 explanations. The remainder came from a mix of scientific publications, forums, social media websites, governmental websites, and Wikipedia (see supplementary materials [2] for all explanations and sources). This diversity of sources ensured a broad spectrum of explanations to reflect the variety of information available to the public.

Two authors independently reviewed the explanations to identify themes and assigned a code for each theme. The number of codes per explanation largely depended on the size and complexity of the text. We ended up assigning eight codes to the most complex explanation. The coding process began with a few initial codes based on our prior knowledge of TEEs. Codes were added based on themes that emerged during the analysis. After reviewing all explanations, the coders discussed the themes to develop a shared codebook. They repeated the process of reviewing explanations, coding, discussing all disagreements, and refining the codebook twice more until they reached 100% agreement. The final codebook has 14 codes. Here we list the codes that appeared in at least five explanations with the number of explanations in which they appeared in parentheses: *Isolation* (23), *Hardware* (23), *Confidentiality* (21), *Prevents* (17), *Integrity* (16), *Technical* (11), *Cryptography* (10).

Code	Description	Frequency
Reputation	Leverages pre-existing trust/reputation of recognizable companies	2
Verified	Application running in the TEE is verified	2
Attestation	Process to check that the software supporting the TEE is the code we expect	4
Trust	Explanation mentions the word "trust"	5
Unsubstantial	Generic/un-detailed description	8
Threat	TEE protects against untrusted OS/peripherals	8
Techniques	Describes particular TEE (e.g., Intel SGX, Arm TrustZone)	10
Cryptography	Mentions cryptographic concepts	10
Technical	Explanation uses technical terminology (e.g., "confidentiality," "attestation")	11
Integrity	TEE prevents unauthorized modification	16
Prevents	TEE prevents some undesirable behavior	17
Secrecy	TEE prevents unauthorized access	21
Isolation	TEE ensures isolation from the rest of the system	23
Hardware	Mentions that a TEE is *hardware*-supported	23

Table 1: Codebook for explanations found in the wild and how frequently each code was identified in the explanations. Each explanation could have up to 7 different codes.

Techniques (10), *Threat* (8), *Unsubstantial* (8), and *Trust* (5). The complete codebook, including a description of each code, can be found in Table 1.

3.2 Designing Candidate TEE Explanations

We developed new explanations that used key themes found in existing explanations and iterated on their wording through pilot testing. We designed our explanations to be composable so that we could separately test each component in controlled experiments. We identified *Confidentiality*, *Isolation*, and *Integrity* as themes that seemed fundamental to a TEE explanation and should be included in every candidate explanation using either *Technical* or *Non-technical* language. In addition, we identified *Hardware*, *Trust*, and *Prevents* as themes that might aid understanding. We decided to test explanations that included *Hardware*, *Trust*, or an *Unsubstantial* explanation, as well as explanations that either explained what a TEE *Prevents* or includes *No Prevents* clause. In order to keep the number of treatments in our survey manageable, we did not evaluate the less common themes.

As shown in Figure 1, the structure of each explanation is: (1) a high-level sentence introducing the concept of a TEE as a security mechanism (one of the following themes: *Hardware*, *Trust*, or *Unsubstantial*), followed by (2) a sentence introducing the concepts of isolation, confidentiality, and integrity in either technical or non-technical language (one of the following themes: *Technical* or *Non-technical*), and, only for some explanations, (3) a third sentence introducing a specific threat that a TEE can prevent (theme: *Prevents* or *No Prevents*). Our candidate TEE explanations are the set of all 12 possible combinations of themes that follow the structure above. Complete TEE explanations are shown in Appendix B.

4 Survey Methods

To evaluate our candidate TEE explanations, we conducted two surveys. The Survey 1 focused on evaluating our explanations (**RQ1-2**), while Survey 2 tested some follow-up research questions (**RQ3-4**) based on the results of Survey 1. In this section, we describe the methods we used to conduct and analyze data from both surveys.

4.1 Survey 1: Evaluating TEE Explanations

The purpose of Survey 1 was to evaluate our candidate TEE explanations to identify which themes, adopted from existing explanations, are best at enhancing understanding (**RQ1**), willingness to use TEE-enhanced technology, and feelings of safety (**RQ2**). We constructed four scenarios to use in our surveys. Each scenario describes a situation where personally identifiable data is collected for some purpose. The data collected in each scenario is the same, but the *setting* and *purpose* of collection depends on the scenario.

We choose medical research and smart home settings because they are both promising TEE use cases [6, 7, 11, 13, 20, 36]. We chose not to use a smartphone scenario, despite it being another TEE use case [8, 9] because we wanted to focus on emerging TEE applications. The fact that most people already have smartphones [46] could also have biased our results. In the medical research setting, we ask participants to imagine there is a medical research study that involves collecting personal information if they choose to participate. In the smart home setting, we ask them to imagine shopping for a smart device that will collect personal information about them if they choose to purchase it.

We also have two variations of each scenario, one where the purpose of the data collection is to develop technology involving AI and one not involving AI. We included AI in our scenarios because the adoption of AI has been growing in both medical research [38] and the smart home context (e.g., Google Home [30] and Alexa [5]) and there is evidence that people are wary of AI [40], which could factor into their willingness to use the technology.

Each participant receives one medical research scenario and one smart home scenario randomly. They are also randomly assigned the technology with AI or without AI in each scenario.For example, one participant may receive the "medical research with AI" scenario followed by the "smart home with AI" scenario while another may receive the "smart home without AI" scenario followed by the "medical research with AI" scenario. For each scenario, participants are told that the data is stored in the cloud and protected by a TEE. The complete scenario text for all four scenarios is shown in the supplementary materials [2]. The scenario text is followed by a random candidate TEE explanation (from the set of 12 explanations), and they receive the same explanation for both scenarios.

In the first part of the survey, we introduce the scenario and confirm participants are paying attention by asking them to select the purpose of the medical research study or what device they're shopping for. If they answer incorrectly, they are asked to re-read the scenario text and try again.[1]

Next, we asked participants to rate their willingness to participate in the medical research study (for the medical research scenarios) or willingness to purchase the smart home device (for the smart

[1]Eight participants answered incorrectly the first time, but four succeeded after we gave them a second chance at the attention check.

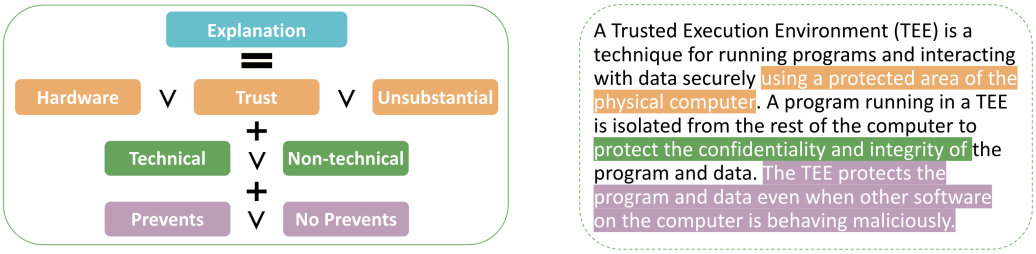


Figure 1: Diagram illustrating the design of the initial TEE explanations and an example candidate TEE explanation.

home scenarios), and how safe they believe their data would be, each on a 3-point Likert scale. We then evaluated comprehension via 10 True/False questions and allowed participants to ask us any lingering questions they had about TEEs. We ended the survey by collecting demographic data. The complete survey instrument can be found in the supplementary materials [2]. We solicited feedback from TEE experts outside of our team on the technical accuracy of our explanations, scenarios, and comprehension questions. We refined the survey questions through multiple pilots.

4.2 Survey 2: FAQs and Understanding Aspects of Feeling Safe

Survey 2 was similar to Survey 1 other than the introduction of an FAQ to answer some of the most frequently asked questions participants had in Survey 1 (**RQ3**) and asked additional questions to understand which *aspects* of the scenarios led to the belief that data shared with the TEE-enhanced technology would be safe or unsafe (**RQ4**). We developed this FAQ based on direct feedback from participants. However, given its considerably more technical nature, we kept it apart from the explanations.

Participants were randomly assigned to one of three FAQ conditions: one where they were *Shown* the FAQ on its own page after the first scenario was introduced (which they could not click past for 60 seconds) *and* as expandable text on subsequent pages; one where the FAQ was *Hidden* by default and *only* offered as expandable text; and one where they were not given an FAQ (*None* condition). To keep the number of survey conditions reasonably small, we did not re-test all of the TEE explanations from Survey 1. Since the *Technical* and *No Prevents* themes generally led to worse comprehension scores, we used the *Non-Technical* and *Prevents* themes in all of the explanations. Thus, we had 3 explanation conditions (*Hardware*, *Trust*, and *Unsubstantial*), plus we added a fourth no-explanation condition (*None* condition) to serve as a baseline for the questions about aspects of safety.

Because some participants mentioned in Survey 1 that they do not believe data could ever be "Completely safe," when we asked participants how safe they believe their data would be in Survey 2, we used a 4-point Likert scale, adding "Mostly safe" to the 3-point scale (Completely safe, Somewhat safe, Not at all safe) from Survey 1. We also asked participants to rate how much different aspects of the scenarios contributed to the belief that their data would be safe/unsafe on a 5-point Likert scale and to expand on "anything else" that contributes to those feelings in a free-response field. Finally, we added 2 True/False questions about the topics covered in the FAQ.

Constructing the FAQ. Our FAQ is based on the questions participants asked in Survey 1. Our FAQ answers three questions: (1) How do TEEs work? (2) How do we know the TEE is working correctly? (3) How are TEEs used in real life? The answer to the first question includes additional technical details about how TEEs work, specifically Arm TrustZone [12] and Intel SGX [35]. To answer the second question, we described attestation and mentioned that researchers are continuing to develop ways to ensure the applications running in the TEE work as expected. Finally, we used authentication in Android [9, 10] as an example of a real TEE use case in the answer to the third question. The complete FAQ text may be found in the supplementary material [2]. We also provided links to the resources cited in this paragraph (plus general information about confidential computing [22]) at the end of the survey. We did not keep track of whether participants clicked the links.

4.3 Recruitment

We used the same recruitment process for both surveys. We recruited 469 Prolific participants for Survey 1 and 501 for the second using quotas [47] to ensure approximately equal numbers of men and women.[2] People who participated in Survey 1 were not allowed to participate in Survey 2. Our participants are adults located in the US who are fluent in English. We determined compensation rates by piloting our study to estimate survey completion time and our intended hourly rate ($15 per hour). We paid participants $2.50 for Survey 1 ($15 per hour, median completion time approx. 10 minutes) and $2.75 for Survey 2 ($12.35 per hour, median completion time approx. 13 minutes).

We reviewed results for low-effort or nonsensical free-text responses (none in either survey) and removed responses for participants who failed both attention checks (none in Survey 1, 4 in Survey 2). We were left with 469 responses for Survey 1 and 497 for Survey 2.

Table 2 shows the participant demographics, which are similar for both surveys. Participants were balanced across gender, generally young (73.4% under 45 in Survey 1 and 73.8% in the second), and college-educated (63.3% in Survey 1 and 61.6% in the second). Few participants were familiar with TEEs before taking our survey (around 7% for both surveys) or have a career or formal education

[2]Sample sizes were determined by a rule-of-thumb estimate for the logistic regressions we planned for our analysis [59].

	Initial Survey		Follow-up	
	n	%	*n*	%
Gender				
Male	229	48.8%	245	49.3%
Female	228	48.6%	242	48.7%
Non-binary / third gender	11	2.3%	8	1.6%
Prefer not to say	1	0.2%	2	0.4%
Age				
18-24	74	15.8%	82	16.5%
25-34	151	32.2%	164	33.0%
35-44	119	25.4%	121	24.3%
45-54	63	13.4%	81	16.3%
55+	62	13.2%	48	9.7%
Prefer not to say	0	0.0%	1	0.2%
Highest Education Achieved				
Less than high school	9	1.9%	5	1.0%
High school or equivalent	161	34.3%	184	37.0%
Bachelor or associate degree	207	44.1%	225	45.3%
Graduate degree	90	19.2%	81	16.3%
Prefer not to say	2	0.4%	2	0.4%
Familiar with TEEs?				
Yes	35	7.5%	36	7.2%
No	434	92.5%	461	92.8%
Experience in Computing?				
Yes	95	20.3%	107	21.5%
No	374	79.7%	390	78.5%
Experience With Smart Homes?				
Yes	382	81.4%	429	86.3%
No	87	18.6%	68	13.7%
Experience with Medical Research/Work?				
Yes	113	24.1%	142	28.6%
No	356	75.9%	355	71.4%
Total	469	100%	497	100%

Table 2: Demographics of participants for both surveys.

in a computing field (16.4% in Survey 1 and 21.5% in the second). Our participants tend to have some experience with smart home devices (81.4% in Survey 1 and 86.3% in the second) but not with medical research/work in the medical field (23.2% and 28.6%).

4.4 Qualitative data analysis

Our study has two open-ended questions. In the first open-ended question, we ask participants if they have any questions about TEEs.In the second, we ask about aspects of the scenario that contribute to their belief that their data would be safe or unsafe (this question is only in Survey 2). In this section, we describe how we analyzed these questions. Codebooks, including descriptions of the codes, can be found in supplementary materials [2].

Questions about TEEs. The questions asked by participants in Survey 1 were coded by two of the authors. Initially, one coder reviewed the participants' answers, constructed the codebook using thematic coding, then trained the other coder on the codebook. Next, the coders independently coded all responses, met to discuss disagreements and update the codebook, then re-coded the answers again. This process was repeated two times until all disagreements were resolved. We started with the same codebook for Survey 2 and involved a third author as a coder. The same initial coder reviewed responses and trained the other coders on the codebook. Then, all three coders independently coded all answers, meeting to resolve differences and update the codebook. This process was repeated twice until we reached 100% agreement The goal of our coding was to identify themes and our sample was sufficiently small that we could use multiple coders for the entire dataset [41].

Aspects contributing to feeling data is safe or unsafe. The second open-ended question about aspects of safety was analyzed much like the first. One coder started by reading through all the answers, developing a codebook, and training the other two coders. After, each coder independently coded all responses, meeting to resolve differences and update the codebook. This process was repeated twice until all disagreements were resolved.

4.5 Quantitative data analysis

We performed logistic and ordinal logistic regressions as well as Mann-Whitney U and Wilcoxon signed-rank tests. The Mann-Whitney U compares those who received TEE information and those who didn't. The dependent variable was perception of safety. The Wilcoxon signed-rank test was used to compare each participant's paired scores (mean of scores for Q1-5 vs. mean of scores Q6-10). We use logistic regressions instead of a hierarchical model because the treatment (i.e., the structure of the explanations) was not nested. We kept our predictors consistent across all regressions, except we added the FAQ as a predictor for Survey 2. We choose predictors that allow us to explore the relationship between our explanations and the outcome variables (e.g., whether they answered a True/False question correctly). Our predictors are the *explanation* shown, *computer science experience*, *medical or IoT experience*, and *FAQ* condition. To tailor our analyses to the scenarios, we use medical experience as a predictor for medical scenarios and smart home experience for smart home scenarios. We selected our models and planned our analyses in advance to limit Type I error rates associated with running multiple tests. Each test covers a different hypothesis, so we do not perform corrections for multiple testing.

The explanations in Survey 1 consisted of all possible variations and combinations of explanations between the first three sentences (a total of 12 different explanations). The baseline for these predictors is *Unsubstantial*, *Technical*, and *No Prevents* for each of the explanation sentences. In Survey 2, we had four possible explanations shown, and the baseline is *None* (no explanation). The baseline for medical and smart home experience is False (no experience).

Comprehension questions. We assess user understanding based on a set of True/False questions (10 in Survey 1 and 12 in Survey 2). To analyze these binary outcomes, we performed logistic regressions for each comprehension question in each scenario (e.g., 10 questions $\times$ 2 scenarios = 20 models for Survey 1). Because we used different models for medical and home IoT scenarios, each participant was in the data set exactly one time, so we do not need to account for repeated measures in our model. The coefficients represent the odds of the outcome occurring for a one-unit increase in the predictor. A coefficient greater than zero indicates that the predictor increases the odds of the outcome variable to 1 (a correct

answer). Conversely, a coefficient less than zero would indicate a negative impact. Additionally, we assessed the significance of each predictor by looking at the p-value with a significance level of 0.05.

Safety and willingness questions. We also asked participants about their perceptions of safety and willingness to engage with our scenario. These questions did not have binary answers. Instead, participants answered using a 3-to-5-point Likert scale. To ensure consistency across models, we binned all Likert scale data used in statistical analysis into 3 levels. For the willingness to engage with our scenario, there was no need to re-bin, we had "Would not" (baseline), "Maybe would," and, "Definitely would." For the safety perceptions, we binned all answers into "Not at all safe" (baseline), "Somewhat safe," and "Safe" (from binning "Mostly safe" with "Completely safe.").

To analyze this data, we used an ordinal logistic regression. We conducted one regression per question, per scenario, using the same predictors as the comprehension questions. Because we used different models for medical and home IoT scenarios, each participant was in the data set exactly one time, so we do not need to account for repeated measures in our models. We conducted Brant tests to ensure the proportional odds assumption for all predictors. The results indicated that the proportional odds assumption holds for all predictors ($p = 0.05$). Interpreting ordinal logistic regressions is similar to binary logistic regressions. The difference is that a coefficient greater than zero indicates that the predictor increases the odds ratio of the outcome variable reaching or exceeding a higher category when compared to the baseline—for example, a positive coefficient for our willingness questions would indicate the participant is more willing to use the technology, while a negative coefficient indicates they are less willing. We keep the same significance level of 0.05.

We also wanted to understand the aspects of the scenario that affect perceptions of safety with vs. without information about TEEs. For this, we used the Mann-Whitney U test, a nonparametric test that allows for the comparison of median ranks between two independent groups, even with non-normal data. To compare the average score for questions **Q1-Q5** to questions **Q6-Q10** we use a Wilcoxon signed rank, a nonparametric test to compare the median of the differences between two groups. We examine each scenario separately and use a significance level of 0.05.

4.6 Limitations

We chose an IoT and Medical scenario to reflect real-life situations where our participants could make choices about the use of a TEE-enhanced technology. However, these scenarios, while designed to be realistic, might not fully capture the complexity of a real-world context and may not be representative of the entire range of contexts where users may need some understanding of TEEs. The study relies on self-reported data, which may be affected by social desirability bias or participants' willingness to disclose their true thoughts and feelings. We tried to mitigate this limitation by ensuring the confidentiality of the participants. We also checked to make sure participants had read and understood the scenarios we were asking about. Moreover, within the online crowdsourcing platforms available, Prolific seems to be one of the most reliable [25, 55]. Our sample of participants is skewed young and may not represent the larger population.

4.7 Ethical Considerations

The surveys and consent forms were approved by the IRB at the authors' institution(s). The only personally identifiable data collected were Prolific IDs for recruiting and paying participants and IP addresses for bot detection.

5 Survey 1 Results

In this section, we summarize the results of Survey 1 evaluating candidate TEE explanations.

5.1 RQ1: Factors Influencing Comprehension

To measure our participants' comprehension of TEE concepts, we asked them a series of True/False questions. Each question has one correct answer. We evaluated their responses for correctness and summarize the scores in Figure 2. The full regression table can be found in Table 7, and scores per scenario and TEE explanation can be found in the supplementary materials [2].

Participants are less likely to recognize TEE limitations. Looking at the overall trend in comprehension scores across all conditions, shown in Figure 2, participants are more likely to correctly answer questions about the features of TEEs (**Q1** through **Q5**, 86.5% correct overall) than about the limitations (**Q6** through **Q10**, 71.5% overall). We also tested this hypothesis with a Wilcoxon signed-rank test comparing the average score for questions about limitations, to the average score for questions about features in Survey 2. We found a significant difference between these two groups for the two smart home scenarios and for the medical scenario without AI ($p - values$ for these three scenarios ranged between $4.378e - 09$ and 0.0044, see Table 6).

TEE *Prevents* and *Non-technical* explanations can improve comprehension. As discussed in Section 4.5, we ran 40 regression models to predict the relationship between each explanation factor and experience on each of the four scenarios and 10 comprehension questions. We found that some explanations are better at describing TEE concepts than others. The *Non-technical* explanation is especially good at explaining who is (or is not) allowed to access the data in the TEE (e.g., **Q2** and **Q5**) while the *Prevents* explanation is best at explaining that the TEE protects against malicious software on the rest of the computer (e.g., **Q3** and **Q4**). The effects for the *Non-technical* explanation hold across all scenarios for **Q2** (significant for the medical scenario without AI) and all medical scenarios for **Q5**. Similarly, the effects for the *Prevents* explanation hold across three of the four scenarios for **Q3** (significant for the medical scenario without AI) and across all scenarios for **Q4** (significant for both medical scenarios and the smart home scenario with AI).

5.2 RQ2: Factors Influencing Willingness and Feeling of Safety

While the *type of technology* we described in the scenario seems to have an effect on participant willingness to use TEE-enhanced technology and belief that TEE-enhanced technology will keep their

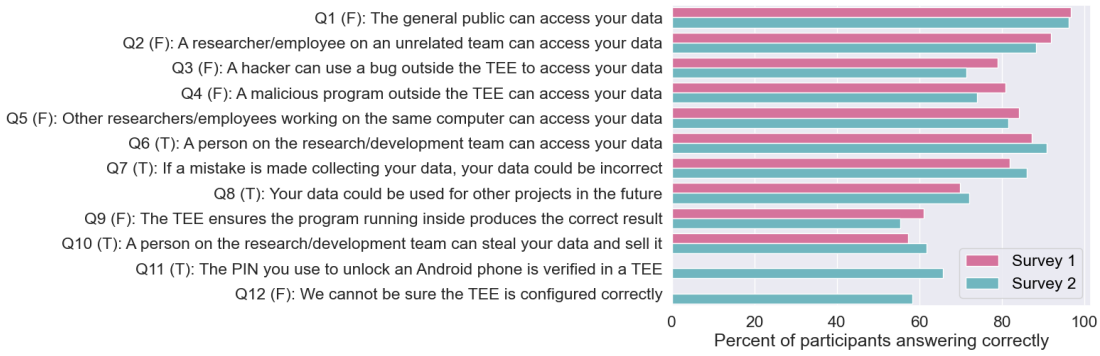


Figure 2: Overall scores for the True/False comprehension questions in both surveys. Q1-Q5 are about features of TEEs, Q6-Q10 are about limitations of TEEs, and Q11 and Q12 are questions that can be answered based on information in the FAQ and appear in Survey 2 only. The correct answer for each question is shown in parentheses by the question number.

data safe, this does not seem to be the case for the *TEE explanation*. Most explanation predictors are not significant in our regression models, except for the *Non-Technical* explanation, which seems to make participants feel significantly safer in the smart home device scenario without AI (see Table 3).

TEE explanations seem to have little effect on willingness and feeling of safety. Regardless of TEE explanation, our results (shown in Table 3) suggest that participants were nearly equally willing to engage with the TEE-enabled technology in our scenarios. 20%-22.4% said they were "definitely willing" and 50.4%-55.7% were "maybe willing" across all scenarios. Similarly, participants seem to believe their data would be nearly equally safe regardless of how the TEE was explained. 24.0%-28.3% said it would be "completely safe" and 62.3-66.9% said it would be "somewhat" safe across all scenarios.

5.3 Questions from our participants

The survey had two opportunities for participants to ask us questions about TEEs. We received 310 questions from 252 participants. In this section, we describe the most common types of questions asked. Note that participants may have written multiple questions in a single response, with each question potentially having one or more theme. Our codebook describing themes and the frequency of each theme can be found in the supplementary materials [2].

Our participants had many questions that our TEE explanations did not answer. The most common questions were about TEEs, but there were many other questions about the scenario where the TEE is used, potential risks they might encounter, and what guarantees there are that the TEE will function as described. We also received some comments indicating that participants lack trust in TEEs and data privacy, in general. Participants asked more questions after the medical scenarios, and these questions were more likely to focus on TEEs and potential risks than in the smart home scenarios.

Attributing quotes to participants. When attributing quotes, we report the participant ID, which survey the quote is from, and the treatment they were assigned. For Survey 1, each participant receives three letters, corresponding to the three sentences in the TEE explanation they received: (H)ardware, (T)rust, or (U)nsubstatial; (T)echnical or (N)on-technical; and (P)revents, or (N)o Prevents. For example, (P30S1-HTN) means participant #30 in Survey 1, who received the *Hardware*, *Technical*, *No Prevents* explanation.

Questions about TEEs. The most common questions we received were about TEEs (143 responses). 49 of these questions asked for more technical details generally: "How exactly does a TEE work?" (P55S1-TTP). 21 participants wanted more information about how the TEE creates an isolated environment: "How exactly is a TEE isolated from the rest of the computer?" (P146S1-HNP). 15 participants wanted more implementation details: "Is there a second set of RAM with an independent CPU or something?" (P379S1-HTP). In addition, 15 participants wanted more information about what else the machine is capable of: "…I presume that means that the [researchers] cannot use any other programs at the same time?" (P48S1-UTN). It is noteworthy that only 13 participants asked questions that should have already been answered by the scenario text or the TEE explanation they received. Since this represents relatively few of the responses we received (less than 5%), it suggests that most participants were paying attention to our survey.

Questions about the scenarios. We received 91 questions about our scenarios. 41 asked about the data involved, including what data is collected, data retention policies, and how/whether the data is anonymized: "What happens to my data when I no longer wish for it to be stored" (P149S1-TNN). 25 questions were about the people on the research/development team: "How many people have access to the TEE, what are their qualifications…." (P12S1-HTN).

Questions about risks. 74 participants asked about potential risks. The most common risk, mentioned by 27 participants, was hackers: "I get that the program is safe from other possibly malicious programs, but what about hackers" (P47S1-TTP). 23 participants were concerned about people behaving maliciously, including the people in the scenario with legitimate access to their data: "What kind of process ensures that the researchers will not share my data?" (P181S1-HTN).

Questions about guarantees or real-world uses. 51 participants wanted to know how they could be sure the TEE would work: "…how [is] it guaranteed that it can't be accessed?" (P87S1-TNN). 21 had questions about real TEEs, including 11 who asked whether

they had ever been involved in a breach: "I would like to know if there have been cases in the past where TEEs have been hacked" (P204S1-HTP). 4 wondered whether TEEs are actually real: "Is it a real thing? Or a hypothetical idea just for the study?" (P127S1-TTP).

Other concerns. 43 participants did not ask questions, instead using the space to share opinions. 10 commented on the scenario "…I was biased about this to begin with. I don't trust these devices" (P62S1-TNP). 16 wrote about technology: "You do understand that people don't trust technology?" (P389S1-UTN). 10 people mentioned that they don't trust TEEs: "I don't trust my information will be secure, especially with the words 'trusted environment' " (P243S1-HNN).

6 Survey 2 Results

Our first survey shows that TEE explanations might be effective at communicating TEE concepts, especially when they are *Non-technical*, mention specific threats a TEE can *Prevent*, and do not expect people to infer new things. However, our explanations had little effect on willingness to use TEE-enhanced technology or the belief that the TEE will keep data safe. Moreover, the questions we collected suggest that a potential reason that TEE explanations have little effect may be that our participants' primary data privacy concerns are beyond the capabilities of TEEs. In this section, we describe our follow-up survey, Survey 2, where we introduce an FAQ based on the questions asked by participants in our first survey and additional questions related to their belief that the TEE-enhanced technology will keep their data safe.

6.1 RQ3: Effect of FAQ

We summarize the scores for each question in Figure 2. The full regression table can be found in Table 8. Having an FAQ seems to have helped participants answer questions about TEE features correctly, but it also seems to have made them less likely to answer questions about TEE limitations correctly. The FAQ had little effect on participants' willingness to adopt TEE-enhanced technology. Still, it did tend to make people feel more confident that their data would be safe when protected by a TEE.

Participants did interact with the FAQ. To determine whether people were reading the FAQ, we added two comprehension questions. **Q11** asked about real-world use of TEEs ("How are TEEs used in real life?" in the FAQ) and **Q12** asks whether we can know that a TEE is configured correctly ("How do we know the TEE is working correctly?"). In both cases, participants were significantly more likely to answer the question correctly if they had an FAQ than if they didn't (Table 8). 77% of participants who received a *Hidden* FAQ expanded the questions at least once.

The FAQ has a mixed effect on comprehension. Participants with an FAQ were more likely to correctly answer questions about TEE features (**Q1**-**Q5**) or the FAQ-specific questions (**Q11**-**Q12**). The difference between the *Shown* FAQ and *None* FAQ condition was statistically significant for **Q2**, **Q3**, and **Q5**, for different scenarios. On the other hand, the *Hidden* FAQ condition was significantly better than the *None* FAQ condition for **Q3** in only the medical scenario without AI. Meanwhile, both *Shown* and *Hidden* FAQ conditions were better than the *None* FAQ for **Q11** and **Q12** (statistically significant for all scenarios). When the FAQ helped participants answer the question correctly, we found similar results for both types of FAQ presentations, except for the FAQ-specific questions, where the *Shown* FAQ was better than the *Hidden* one.

Interestingly, having an FAQ made it more likely that participants would answer questions about TEE limitations (**Q6**-**Q10**) *incorrectly* than if they didn't have an FAQ at all. The difference between the *Shown* FAQ condition and *None* FAQ condition was statistically significant for **Q8** and **Q10** for a few (but not all) scenarios. The *Hidden* FAQ condition was significantly worse than the *None* FAQ condition for **Q6**, **Q8**, and **Q10**, also for a few (but not all) scenarios.

Having an FAQ or explanation seems to have little effect on willingness to use technology. Similar to the findings in Survey 1, where we saw almost no impact from different explanations, in Survey 2, we see that explanations and FAQ do not seem to significantly affect participants' willingness to use TEE-enabled technology (see Table 3).

Having an FAQ or explanation seem to make people more confident their data will be safe. More participants receiving an FAQ believed their data would be completely or mostly safe (75% for *Shown* and 71.4% for *Hidden*) than those who did not receive an FAQ (64.1%). We observed a similar trend between the participants receiving a TEE explanation and those not receiving one (70-74% depending on the explanation vs. 63.2% for no explanation). These differences are significant only for the *Shown* FAQ condition in the smart home scenario without AI (see Table 3).

6.2 RQ4: Aspects Contributing to Safety

For each scenario, we asked participants which aspects of the scenario contribute to their belief that their data would be safe (or unsafe), including: the use of a TEE, that a hospital (or company, depending on the scenario) is collecting the data, the people on the team, what data is collected, and the purpose of the data collection. We also asked if any other aspects of the scenario not already mentioned contributed to their belief that their data would be safe or unsafe. Overall, we found that providing information about TEEs (by giving them an explanation *or* an FAQ) seems to make people more confident that the TEE would keep their data safe. There were many other aspects of the scenario that people were concerned about that TEE explanations and FAQs did not address. The results in this section are supported by a Wilcoxon signed-rank test, see Table 5 for details.

Attributing quotes to participants. We attribute quotes using a similar strategy as Survey 1, except that, here, the treatment is represented using two letters. The first letter is the TEE explanation: (H)ardware, (T)rust, (U)nsubstantial, or (X) for no explanation. The second letter is the FAQ condition: (H)idden, (S)hown, or (X) for no FAQ. For example, (P68S2-HX) is participant #68 in Survey 2, who received the *Hardware* explanation and the *None* FAQ condition.

Explaining TEEs seems to make people more confident the TEE will keep their data safe. In the group that had access to information about TEEs, 80.3% said the use of a TEE made them feel their data was definitely or somewhat safe, while only 52.3% of those who had no access to information about TEEs said the use of a TEE made them feel their data was definitely or somewhat safe ($p - values$ between 0.0002 and 0.0026 depending on the scenario).

	Survey 1 Medical Scenario Without AI		Survey 1 Smart Home Scenario Without AI		Survey 1 Medical Scenario With AI		Survey 1 Smart Home Scenario With AI	
Variable	**Willingness**	**Safety**	**Willingness**	**Safety**	**Willingness**	**Safety**	**Willingness**	**Safety**
Expln sentence 1 [Baseline = Unsubstantial]								
Hardware	1.39	0.97	1.38	0.95	0.99	1.02	1.12	1.07
Trust	1.16	1.15	1.43	1.08	0.72	0.74	0.89	0.84
Expln sentence 2 [Baseline = Technical]								
Non-Technical	0.78	0.91	1.4	2.39**	1.20	1.14	0.93	0.79
Expln sentence 3 [Baseline = No Prevents]								
Prevents	1.31	1.26	1.35	1.03	0.84	0.84	0.74	1.51
Medical/Smart home exp	1.54	0.86	3.25***	0.84	1.15	0.79	2.34**	1.80
CS Experience	1.01	1.02	1.12	2.12*	1.36	1.28	1.14	1.13

	Survey 2 Medical Scenario Without AI		Survey 2 Smart Home Scenario Without AI		Survey 2 Medical Scenario With AI		Survey 2 Smart Home Scenario With AI	
Variable	**Willingness**	**Safety**	**Willingness**	**Safety**	**Willingness**	**Safety**	**Willingness**	**Safety**
TEE Explanation [Baseline = None]								
Unsubstantial	0.73	1.88	0.81	0.70	0.99	1.08	1.57	2.59*
Hardware	1.12	1.36	1.58	1.92	1.21	1.97	0.99	1.36
Trust	1.02	2.05	0.87	1.08	0.69	1.55	1.04	1.57
FAQ [Baseline = None]								
Hidden	0.91	1.32	1.70	1.68	0.76	1.20	0.76	1.57
Shown	0.99	1.75	1.38	2.39*	1.52	1.52	1.27	1.72
Medical/Smart home exp	0.95	0.80	6.23***	3.19**	0.99	0.99	3.46***	1.68
CS Experience	1.08	1.17	1.14	1.55	1.23	1.15	0.85	0.70

Table 3: Regression table for questions about willingness to use technology and belief that the TEE will keep data safe in Survey 1 and 2 respectively. The first column is how willing the participant would be to use the TEE-enhanced technology, the second column is the belief that their data will be safe. There is one ordinal logistic regression model for each question in each scenario (24 models total). The numbers in this table are the odds ratios for each predictor, with the baseline explanations used in each model noted in *italics*. Statistical significance is noted with asterisks and shaded cells: blue for positive coefficients and orange for negative.

TEE information seems to have little effect on other aspects. For aspects other than the use of a TEE, providing a TEE explanation or FAQ seems to make little difference to our participants' feelings of safety ($p > 0.05$ except for the people involved in the medical scenario without AI with $p = 0.0413$). For example, 61.6% of participants reported feeling definitely or somewhat safe about the purpose of the data collection when they had information about the TEE vs. 57.8% without information. For the other aspects, providing information about the TEE made people somewhat *less* sure their data would be safe. The place where information made the biggest difference was when we asked about the people involved in the scenario. Here, 50.8% of participants with information about the TEE reported the people made them feel their data would be definitely or somewhat safe, while 54.4% without information about the TEE said the same.

Other aspects of the scenario mentioned by participants. Here, we describe some of the most common aspects, not already discussed above (many participants used this opportunity to expand on their previous answers). We received 660 responses total from 382 participants, where each response might mention one or more aspects of the scenario. 392 responses mentioned at least one aspect contributing to the feeling their data would be unsafe and 249 responses mentioned aspects contributing to the feeling their data would be safe.

Some aspects of the scenario participants reported contributing to the feeling that data would be unsafe include: prior experiences with/knowledge of breaches (42 responses), the future use clause in the scenario text (28 responses), the belief that some of the data was being collected unnecessarily (24 responses), the use of AI in the scenario (19 responses), the risk that there could be a bug in the TEE code (14 responses), and the risk that their data would be sold (12 responses). 5 people were concerned that we mentioned future research: "The fact that it says researchers are looking for new ways to verify the program is working correctly. That makes me a little hesitant. Sounds like there are still bugs…" (P144S2-TS). 3 people seemed suspicious about being told to "trust" the technology: "Comes across a bit like: 'Yeah trust me bro your medical records are

totally safe bro, trust me, bro there's an acronym. You like acronyms right man?' " (P237S2-TX).

Most aspects participants reported contributing to the feeling that their data would be safe were repeated from previous questions. The most common new aspect contributing to the feeling of safety is the perception that the data being collected is not interesting enough to an attacker anyway (25 responses).

6.3 More questions from our participants

Similar to the first survey, we gave participants two opportunities to ask us questions they have about TEEs and received 267 responses. In this section, we summarize the most common questions we received, following the same structure as Section 5.3, and how questions differed between participants who did and did not have access to an FAQ. We began with the same codebook as in the first survey, with only a few additional codes emerging during the analysis. The codebook describing all of the themes and how frequently they occurred may be found in the supplementary materials [2].

Giving participants an FAQ made them less likely to ask questions about TEEs or the scenario, which were the most common kinds of questions we received overall. Some other questions were more common from participants who received an FAQ, like asking for more examples or about guarantees.

An FAQ seems to reduce questions about TEEs. As in the first survey, we received the most questions (117 responses) about TEEs themselves. Although only 34% of people did not receive an FAQ, 45% of the questions about TEEs came from people who did not receive an FAQ. The most common questions were, again, asking for more information about how the TEE (31 responses) or its isolation mechanism (7 responses) work. Unlike in the first survey, we also saw 17 people asking what a TEE is, more generally: "What is a TEE??" (P351S2-XX). Other common questions requested more implementation details (14 responses) or compared TEEs to other technologies (8 responses). We also had 13 requests for a less technical explanation: "Need more details about how they work in general without the use of complicated verbiage." (P52S2-XH). Most of these (69% of the requests) came from people who were forced to wait on the FAQ page.

An FAQ seems to reduce questions about people in the scenario. We also received 74 questions about the scenario. Again, 45% of the questions about the scenario came from people who did not receive an FAQ. The most common questions were about the people involved in the scenario (28 responses) or the data (25 responses). A disproportionate 57% of questions about people come from the participants who did not receive an FAQ, while the questions about data are more evenly distributed between FAQ conditions.

A hidden FAQ seems to reduce questions about hackers. 60 participants had questions about the risks they might encounter. Similar to above, 43% of these questions came from people who did not receive an FAQ. Unlike other questions, though, participants were least likely to ask questions about hackers (28 responses, total) if they got the expandable FAQ: 18% of questions about hackers came from the hidden FAQ condition, while 43% came from the shown FAQ and 39% from the no FAQ condition. Questions about people behaving maliciously (12 responses) were nearly evenly distributed between FAQ conditions. The remaining questions about risks disproportionately came from the people who did not receive an FAQ (54% of the remaining questions asked about risks).

Questions about guarantees or real-world uses seem to be more common with an FAQ. We received 20 questions about guarantees and 29 questions about real-world uses for TEEs. Both questions were more common with an FAQ than without. 45% of questions about guarantees came from participants in the hidden FAQ condition and 45% of questions about real uses of TEEs came from participants who were shown the FAQ. It is possible that some questions came from participants who wanted to write something but couldn't think of anything else to ask: "I can't think of any more questions. Maybe, would be nice to see more real world examples" (P22S2-XS).

A hidden FAQ also seems to reduce other concerns. Similar to our initial survey, 41 participants did not ask a question but used the space to share other thoughts. The most common thoughts were general distrust (23 responses), followed by opinions about the scenario (9 responses). The participants receiving the hidden FAQ condition seemed to be the least likely to use this space to express distrust (these account for 17% of the 23 responses), while the remaining questions were nearly evenly distributed between the shown FAQ and no FAQ conditions (43% and 39%, respectively).

7 Discussion

In this section, we make recommendations for explaining technical concepts to non-experts, navigate the (seemingly) contradictory results between our study and prior work [43], and highlight opportunities for future research.

7.1 Explaining technical concepts to non-experts

Avoid technical jargon. Our results in Section 5.1 echo prior work [24, 64, 66] on the importance of avoiding jargon when explaining technical concepts to non-experts. This was also mentioned by participants reading the supplementary technical details we introduced with the FAQ: "Need more details about how they work in general without the use of complicated verbiage." (P52S2-XH).

Be direct and tell users what you want them to know. In Section 5.1, we found that people were more likely to answer questions correctly when the answer was in the explanation or scenario text directly than questions where people had to generalize what they learned and *infer* the answers. For example, participants in the *Prevents* TEE explanation condition were told that the TEE can protect against malicious software on the computer. This group was significantly more likely to answer the question about malicious programs (**Q4**) correctly in three of the four scenarios because the explanation they received gave them the answer to the question. On the other hand, while 87.2% of Survey 1 participants knew that the research/development team could access the data (**Q6**), only 57.2% used that knowledge in **Q10** to infer that the same group of people could *steal* their data and use it for personal gain. It is possible that our participants had trouble inferring that even people authorized to access their data might use it for malicious purposes.

Don't tell people what technology they should trust. In Section 6.2, we showed that explaining TEEs does little to address some of the concerns our participants have about technology. In fact, in some cases, information about TEEs made people slightly *more* skeptical. One reason for this might be that TEEs do not address all security and privacy threats, so explaining them, even if they are explained well, does not address all of the concerns people have. These concerns could also explain why some participants were wary of the word "trust" in "Trusted Execution Environment" as we noted in Sections 5.3 and 6.2. Because security technologies are often orthogonal to the concerns people shared with us, it could be counterproductive for users already feeling skeptical if these solutions are marketed to them as trusted: "I don't trust my information will be secure, especially with the words 'trusted environment' " (P243S1-HNN).

7.2 Comparing our findings to prior work

One of the main motivations of our study was the finding from prior work [43] that the presence of cloud-based TEEs can make people more comfortable sharing their data with home IoT, especially if they understand what a TEE is. On the surface, our finding that the TEE explanation has little effect on participants' willingness to use TEE-enhanced technology or their perception of safety (Section 5.2 and Table 3) seem to contradict these results. One explanation for this difference could simply be the methodological differences between the previous study and ours.

The previous study's main goal was to understand whether the presence of a TEE alters existing privacy norms within a smart home environment. In particular, they asked participants to imagine that they own a smart home device (either a smart camera or smart speaker) and how comfortable they feel about having their (or other occupants) data collected under certain conditions (e.g., if the data is shared with law enforcement, if they—the device owner—are notified). In this study, the assumption is that *the participants already own and interact with a smart device* and the goal is to understand how the introduction of a TEE affects participants' perceptions of what makes them comfortable (or uncomfortable) with certain data sharing practices. Our study, on the other hand, does not ask participants to *assume that they will interact* with the TEE-enhanced technology. Instead, we evaluate their comfort by asking them about their *willingness to interact with the technology* and their perception of safety.

7.3 Future research

Explaining limitations, not just features. Our explanations were better at describing the protections provided by TEEs than their limitations. In fact, despite ensuring that our explanations faithfully represent TEE security features, participants believed the TEE would offer some protections that it does not, such as guaranteeing the results of a computation are correct or preventing people with legitimate access from selling their data (**Q9** and **Q10** and in Sections 5.1 and 6.1). A similar phenomenon was observed in prior work [4]. More research is necessary to understand how we can highlight the limitations of security technology. However, as in our study, this research needs to measure comprehension, willingness to use, and beliefs about safety.

Investigating showing vs. hiding the FAQ. In Section 5.3, we explained that many participants in Survey 1 asked for more technical details about TEEs. In Survey 2, we provided participants with those details in an FAQ, and in Section 6.3, we explained that it did lead to fewer questions. However, we also saw that the technical details could be overwhelming to some and that the *Shown* FAQ was more effective for some, *but not all*, of the True/False comprehension questions (Section 6.1). More research is needed to understand why different FAQ models perform differently for some comprehension questions. One hypothesis is that hiding the FAQ allows people to focus their attention on the relevant information, but also makes it more likely that they won't read it at all. Future work could also shed light on how we might balance the trade-offs between providing additional technical details to those who want them and hiding them from those who find them unnecessary.

Revisit prior work with our enhanced explanations. As explained above, the methodological differences between our study and the one from prior work [43] likely explain the seemingly contradictory results about user comfort. Nevertheless, it would be useful to repeat their study using our most effective explanations to see if their results can be reproduced. Repeating the study using their methodology would make it possible to compare results more directly and better understand why even our best explanations seem to have little effect on user comfort.

7.4 How much do users need to know about TEEs?

Our results provide some insights into how we can communicate about technical security concepts more effectively, but suggest that understanding TEEs does not impact decisions about whether or not to use TEE-enhanced technology. While we started off with the hypothesis that understanding TEEs would improve users' trust in technology, our participants' responses drive home the point that, as some of our participants correctly realized, knowledge that a system uses a TEE is insufficient to draw conclusions that a user's data will be adequately protected. We might imagine that the TEE is just one of several components that are being used to protect user data in our scenarios and we could potentially provide a much more detailed explanation of all the protective components to assure users that their data is safe, or to highlight exactly what risks they might face. But this begs the question of whether we should really expect users to understand the inner workings of a security system, or if it should simply be offered to improve transparency around data privacy.

Ultimately, decisions about TEEs are still best left to experts, not end users. Experts' choices about whether and how to use TEEs should revolve around the technology they are developing and the data they require, not whether the TEE would make users more willing to use the technology.

8 Conclusion

In this study, we evaluated strategies for explaining TEEs. Some were more effective at enhancing understanding than others. Our findings highlight the importance of avoiding technical jargon and directly communicating what people should learn. On the other hand, we found that our explanations have limited effects on

willingness to use technology or the feeling of safety, likely because TEEs do not address many of the privacy concerns our participants have. Our results provide insights into how we can communicate more effectively about technical security concepts, but also suggest that explaining security technology might not resolve the concerns users have about data privacy.

References

[1] 1996. Health Insurance Portability and Accountability Act of 1996. 45 C.F.R. §§ 160, 162, 164. United States.

[2] 2024. Supplementary Material. https://anonymous.4open.science/r/TEE-2024-D1A4/README.md.

[3] Ruba Abu-Salma and Benjamin Livshits. 2020. Evaluating the end-user experience of private browsing mode. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*.

[4] Omer Akgul, Wei Bai, Shruti Das, and Michelle L Mazurek. 2021. Evaluating In-Workflow messages for improving mental models of End-to-End encryption. In *Proceedings of the 30th USENIX Security Symposium*.

[5] Amazon. 2024. LLM-powered Alexa experiences. https://developer.amazon.com/en-US/alexa/alexa-ai. Accessed: 2024-05-17.

[6] Suzanne Ambiel. 2024. The Case for Confidential Computing. [Accessed 11-11-2024].

[7] AMD. 2020. Strengthening VM isolation with integrity protection and more. *White Paper* 53 (2020), 1450–1465.

[8] Android. 2024. TrustZone. https://source.android.com/docs/security/features/trusty. [Accessed 27-06-2024].

[9] Android Open Source Project. 2024. Android Authentication. https://source.android.com/docs/security/features/authentication. [Accessed 27-06-2024].

[10] Android Open Source Project. 2024. Android Gatekeeper. https://source.android.com/docs/security/features/authentication/gatekeeper. [Accessed 17-06-2024].

[11] ARM. 2024. ARM CCA. https://www.arm.com/architecture/security-features/arm-confidential-compute-architecture. [Accessed 27-06-2024].

[12] Arm Developer Hub. 2024. Arm TrustZone. https://developer.arm.com/documentation/102418/0101/What-is-TrustZone-?lang=en. [Accessed 27-06-2024].

[13] Gbadebo Ayoade, Vishal Karande, Latifur Khan, and Kevin Hamlen. 2018. Decentralized IoT data management using blockchain and trusted execution environment. In *Proceedings of the 2018 IEEE International Conference on Information Reuse and Integration*.

[14] Elijah Robert Bouma-Sims, Megan Li, Yanzi Lin, Adia Sakura-Lemessy, Alexandra Nisenoff, Ellie Young, Eleanor Birrell, Lorrie Faith Cranor, and Hana Habib. 2023. A US-UK usability evaluation of consent management platform cookie consent interface design on desktop and mobile. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*.

[15] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. 2010. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy* 9, 2 (2010).

[16] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie Faith Cranor, Robert W Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. 2013. Your attention please: Designing security-decision UIs to make genuine risks harder to ignore. In *Proceedings of the 9th Symposium on Usable Privacy and Security*.

[17] Marcel Busch, Johannes Westphal, and Tilo Müller. 2020. Unearthing the TrustedCore: A Critical Review on Huawei's Trusted Execution Environment. In *Proceedings of the 14th USENIX Workshop on Offensive Technologies*.

[18] Carolina Carreira, Joao F. Ferreira, Alexandra Mendes, and Nicolas Christin. 2021. Exploring Usable Security to Improve the Impact of Formal Verification: A Research Agenda. *Electronic Proceedings in Theoretical Computer Science* 349 (Nov. 2021).

[19] Somnath Chakrabarti, Thomas Knauth, Dmitrii Kuvaiskii, Michael Steiner, and Mona Vij. 2020. Trusted execution environment with Intel SGX. In *Responsible Genomic Data Sharing*. Elsevier.

[20] Yu Chen, Fang Luo, Tong Li, Tao Xiang, Zheli Liu, and Jin Li. 2020. A training-integrity privacy-preserving federated learning scheme with trusted execution environment. *Information Sciences* 522 (2020).

[21] Confidential Computing Consortium. 2022. Confidential Computing: Hardware-Based Trusted Execution for Applications and Data. https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC_outreach_whitepaper_updated_November_2022.pdf. [Accessed 10-09-2024].

[22] Confidential Computing Consortium. 2024. Common Terminology for Confidential Computing. https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/Common-Terminology-for-Confidential-Computing.pdf. [Accessed 17-06-2024].

[23] Rachel Cummings, Gabriel Kaptchuk, and Elissa M Redmiles. 2021. "I need a better description": An Investigation Into User Expectations For Differential Privacy. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*.

[24] Verena Distler, Carine Lallemand, and Vincent Koenig. 2020. Making encryption feel secure: Investigating how descriptions of encryption impact perceived security. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 220–229.

[25] Benjamin D Douglas, Patrick J Ewell, and Markus Brauer. 2023. Data quality in online human-subjects research: Comparisons between MTurk, Prolific, CloudResearch, Qualtrics, and SONA. *Plos one* 18, 3 (2023).

[26] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the experts: What should be on an IoT privacy and security label?. In *Proceedings of the 2020 IEEE Symposium on Security and Privacy*. IEEE.

[27] European Union. 2016. Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Accessed: 2024-07-03.

[28] Steven Furnell, Rawan Esmael, Weining Yang, Ninghui Li, et al. 2018. Enhancing security behaviour by supporting the user. *Computers & Security* 75 (2018).

[29] Tim Geppert, Stefan Deml, David Sturzenegger, and Nico Ebert. 2022. Trusted execution environments: Applications and organizational challenges. *Frontiers in Computer Science* 4 (2022), 930741.

[30] Google. 2024. Google Home Gemini. https://support.google.com/gemini/answer/15335456. Accessed: 2024-05-17.

[31] Lawrence O Gostin, Laura A Levit, and Sharyl J Nass. 2009. Beyond the HIPAA privacy rule: enhancing privacy, improving health through research. (2009).

[32] Hana Habib, Jessica Colnago, Vidya Gopalakrishnan, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, and Lorrie Faith Cranor. 2018. Away from prying eyes: Analyzing usage and understanding of private browsing. In *Proceedings of the 14th Symposium on Usable Privacy and Security*.

[33] Seung-Kyun Han and Jinsoo Jang. 2023. MyTEE: Own the Trusted Execution Environment on Embedded Devices.. In *NDSS*.

[34] Trong-Thuc Hoang, Ckristian Duran, Duc-Thinh Nguyen-Hoang, Duc-Hung Le, Akira Tsukamoto, Kuniyasu Suzaki, and Cong-Kha Pham. 2020. Quick boot of trusted execution environment with hardware accelerators. *IEEE Access* 8 (2020).

[35] Intel. 2024. Intel SGX. https://www.intel.com/content/dam/develop/external/us/en/documents/overview-of-intel-sgx-enclave-637284.pdf. [Accessed 27-06-2024].

[36] Intel. 2024. Intel TDX. https://www.intel.com/content/www/us/en/developer/tools/trust-domain-extensions/overview.html. [Accessed 27-06-2024].

[37] Farzaneh Karegar, Ala Sarah Alaqra, and Simone Fischer-Hübner. 2022. Exploring User-Suitable metaphors for differentially private data analyses. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 175–193.

[38] Oleg E Karpov, Elena N Pitsik, Semen A Kurkin, Vladimir A Maksimenko, Alexander V Gusev, Natali N Shusharina, and Alexander E Hramov. 2023. Analysis of publication activity and research trends in the field of AI medical applications. *International Journal of Environmental Research and Public Health* 20, 7 (2023), 5335.

[39] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. 2009. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*.

[40] Colleen McClain, Michelle Faverio, Monica Anderson, and Eugenie Park. 2023. How Americans view data privacy. *Pew Research Center* (2023).

[41] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on human-computer interaction* 3, CSCW (2019), 1–23.

[42] Fan Mo, Zahra Tarkhani, and Hamed Haddadi. 2024. Machine learning with confidential computing: A systematization of knowledge. *ACM computing surveys* 56, 11 (2024).

[43] Pratik Musale and Adam J Lee. 2023. Trust TEE?: Exploring the Impact of Trusted Execution Environments on Smart Home Privacy Norms. *Proceedings on Privacy Enhancing Technologies* 3 (2023).

[44] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don't) use password managers effectively. In *Proceedings of the 15th Symposium on Usable Privacy and Security*.

[45] Sérgio Pereira, David Cerdeira, Cristiano Rodrigues, and Sandro Pinto. 2021. Towards a trusted execution environment via reconfigurable FPGA. *arXiv preprint arXiv:2107.03781* (2021).

[46] Pew Research Center. 2024. Mobile Fact Sheet. https://www.pewresearch.org/internet/fact-sheet/mobile/. Accessed: 2024-05-17.

[47] Prolific. 2024. How do I balance my sample within demographics? https://researcher-help.prolific.com/hc/en-gb/articles/360009221213-How-do-I-balance-my-sample-within-demographics. Accessed: 2024-05-17.

[48] Mohamed Sabt, Mohammed Achemlal, and Abdelmadjid Bouabdallah. 2015. Trusted execution environment: What it is, and what it is not. In *Proceedings of the 2015 IEEE Trustcom/BigDataSE/Ispa*.

[49] Leonie Schaewitz, David Lakotta, M Angela Sasse, and Nikol Rummel. 2021. Peeking into the black box: Towards understanding user understanding of E2EE.

In *Proceedings Of The 2021 European Symposium On Usable Security*. 129–140.
[50] Stuart E Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. 2007. The emperor's new security indicators. In *2007 IEEE Symposium on Security and Privacy*. IEEE, 51–65.
[51] Bingyu Shen, Lili Wei, Chengcheng Xiang, Yudong Wu, Mingyao Shen, Yuanyuan Zhou, and Xinxin Jin. 2021. Can systems explain permissions better? Understanding users' misperceptions under smartphone runtime permission model. In *Proceedings of the 30th USENIX Security Symposium*.
[52] Maria Sommerhalder. 2023. *Trusted Execution Environment*. Springer Nature Switzerland, Cham.
[53] Christian Stransky, Dominik Wermke, Johanna Schrader, Nicolas Huaman, Yasemin Acar, Anna Lena Fehlhaber, Miranda Wei, Blase Ur, and Sascha Fahl. 2021. On the Limited Impact of Visualizing Encryption: Perceptions of E2E Messaging Security. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 437–454.
[54] Kuniyasu Suzaki, Kenta Nakajima, Tsukasa Oi, and Akira Tsukamoto. 2021. Tsperf: General performance measurement of trusted execution environment and rich execution environment on intel sgx, arm trustzone, and risc-v keystone. *IEEE Access* 9 (2021).
[55] Jenny Tang, Eleanor Birrell, and Ada Lerner. 2022. Replication: How well do my results generalize now? The external validity of online privacy and security surveys. In *Proceedings of the 18th Symposium on Usable Privacy and Security*.
[56] Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, et al. 2017. Design and evaluation of a data-driven password meter. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*.
[57] Blase Ur, Jonathan Bees, Sean M Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Do users' perceptions of password security match reality?. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*.
[58] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2015. "I Added '!' at the End to Make It Secure"': Observing Password Creation in the Lab. In *Proceedings of the 11th Symposium on Usable Privacy and Security*.
[59] Maarten van Smeden, Karel GM Moons, Joris AH de Groot, Gary S Collins, Douglas G Altman, Marinus JC Eijkemans, and Johannes B Reitsma. 2019. Sample size for binary logistic prediction models: Beyond events per variable criteria. *Statistical Methods in Medical Research* 28, 8 (2019).
[60] Kapil Vaswani, Stavros Volos, Cédric Fournet, Antonio Nino Diaz, Ken Gordon, Balaji Vembu, Sam Webster, David Chisnall, Saurabh Kulkarni, Graham Cunningham, et al. 2023. Confidential Computing within an AI Accelerator. In *Proceedings of the 2023 USENIX Annual Technical Conference*.
[61] Yong Wang, June Li, Siyu Zhao, and Fajiang Yu. 2020. Hybridchain: A novel architecture for confidentiality-preserving and performant permissioned blockchain using trusted execution environment. *IEEE access* 8 (2020).
[62] Alma Whitten and J Doug Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.. In *Proceedings of the 8th USENIX Security Symposium*.
[63] Justin Wu, Cyrus Gattrell, Devon Howard, Jake Tyler, Elham Vaziripour, Daniel Zappala, and Kent Seamons. 2019. "Something isn't secure, but I'm not sure how that translates into a problem": Promoting autonomy by designing for understanding in Signal. In *Fifteenth Symposium on Usable Privacy and Security*. 137–153.
[64] Tingmin Wu, Rongjunchen Zhang, Wanlun Ma, Sheng Wen, Xin Xia, Cecile Paris, Surya Nepal, and Yang Xiang. 2020. What risk? I don't understand. an empirical study on users' understanding of the terms used in security texts. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*.
[65] Aiping Xiong, Tianhao Wang, Ninghui Li, and Somesh Jha. 2020. Towards effective differential privacy communication for users' data sharing decision and comprehension. In *Proceedings of the 2020 IEEE Symposium on Security and Privacy*.
[66] Shikun Zhang, Yuanyuan Feng, Yaxing Yao, Lorrie Faith Cranor, and Norman Sadeh. 2022. How usable are iOS app privacy labels? *Proceedings on Privacy Enhancing Technologies* (2022).

A Existing TEE explanations

This section includes the final list of the sources of explanations gathered in the wild, the explanations themselves, and the respective URLs. All URLs are truncated for formatting purposes, but the links in the URLs lead to the pages with the explanations.

1. Google cloud From: cloud.google.com

"TEEs are secure and isolated environments that prevent unauthorized access or modification of applications and data while they are in use."

2. Intel SGX From: intel.com/

"A trusted execution environment is a secure area of a main processor. It helps protect the code and data loaded inside it with respect to confidentiality and integrity. Data integrity prevents unauthorized entities from outside the TEE from altering data, while code integrity prevents code in the TEE from being replaced or modified by unauthorized entities, which may also be the computer owner itself as in certain DRM schemes described in SGX. This is done by implementing unique, immutable, and confidential architectural security such as Intel Software Guard Extensions (Intel SGX) which offers hardware-based memory encryption that isolates specific application code and data in memory. Intel SGX allows user-level code to allocate private regions of memory, called enclaves, which are designed to be protected from processes running at higher privilege levels. A TEE as an isolated execution environment provides security features such as isolated execution, integrity of applications executing with the TEE, along with confidentiality of their assets. In general terms, the TEE offers an execution space that provides a higher level of security for trusted applications running on the device than a rich operating system and more functionality than a 'secure element'."

3. NVIDIA From: blogs.nvidia.com/

"Using cryptographic keys linked to the processors, confidential computing creates a trusted execution environment or secure enclave. That safe digital space supports a cryptographically signed proof, called attestation, that the hardware and firmware is correctly configured to prevent the viewing or alteration of their data or application code."

4. Forbes From: forbes.com

"A trusted execution environment is a protected area on the hardware where code can be run securely and in isolation. Code running inside the environment should not be able to be viewed or modified, even if an attacker is able to run malicious code with full permissions on the same processor. As such, trusted execution environments have the potential to significantly boost the security of our systems."

5. AWS From: docs.aws.amazon.com

"Trusted execution environment – The appliance uses a trusted execution environment (TEE) based on ARM TrustZone, with isolated storage, memory, and processing resources. Keys and other sensitive data stored in the trust zone can only be accessed by a trusted application, which runs in a separate operating system within the TEE. The AWS Panorama Appliance software runs in the untrusted Linux environment alongside application code. It can only access cryptographic operations by making a request to the secure application."

6. Wikipedia From: en.m.wikipedia.org

"A trusted execution environment (TEE) is a secure area of a main processor. It helps code and data loaded inside it to be protected with respect to confidentiality and integrity. Data integrity prevents unauthorized entities from outside the TEE from altering data, while code integrity prevents code in the TEE from being replaced or modified by unauthorized entities, which may also be the

computer owner itself as in certain DRM schemes described in SGX. This is done by implementing unique, immutable, and confidential architectural security such as Intel Software Guard Extensions (Intel SGX) which offers hardware-based memory encryption that isolates specific application code and data in memory. Intel SGX allows user-level code to allocate private regions of memory, called enclaves, which are designed to be protected from processes running at higher privilege levels. A TEE as an isolated execution environment provides security features such as isolated execution, integrity of applications executing with the TEE, along with confidentiality of their assets. In general terms, the TEE offers an execution space that provides a higher level of security for trusted applications running on the device than a rich operating system (OS) and more functionality than a secure element (SE)."

7. TrustSonic From: trustonic.com through Google search

"A Trusted Execution Environment (TEE) is an environment for executing code, in which those executing the code can have high levels of trust in that surrounding environment, because it can ignore threats from the rest of the device."

8. DualityTech From: dualitytech.com through Google search.

"A Trusted Execution Environment is a secure area inside the main processor where code is executed and data is processed in an isolated private enclave such that it is invisible or inaccessible to external parties. The technology protects data by ensuring no other application can access it, and both insider and outsider threats can't compromise it even if the operating system is compromised. This level of security is equivalent to what existing classic cryptography methods such as symmetric-key encryption, hashing and digital signature, provide."

9. Android From: source.android.com through Google search.

"Trusty is a secure Operating System (OS) that provides a Trusted Execution Environment (TEE) for Android. The Trusty OS runs on the same processor as the Android OS, but Trusty is isolated from the rest of the system by both hardware and software. Trusty and Android run parallel to each other. Trusty has access to the full power of a device's main processor and memory but is completely isolated. Trusty's isolation protects it from malicious apps installed by the user and potential vulnerabilities that may be discovered in Android."

10. Evervault From: evervault.com through Google search.

"A TEE is an environment for executing code in which those running the code can have high levels of trust in that surrounding environment because it is insulated from the rest of the device. A Trusted Execution Environment (TEE), also known as a Secure Enclave, is a highly constrained compute environment that allows for cryptographic verification (attestation) of the code being executed. TEEs are designed with no persistent storage, no shell access, and no network connectivity by default. As a result, they provide a completely isolated environment with heavily restricted external access, making it possible to run sensitive workloads securely."

11. Piwik From: piwik.pro through Google search.

"A trusted execution environment (TEE) is a secure area of a main processor that guarantees optimal protection for highly sensitive data in all its states, with respect to confidentiality and integrity. TEE can be used on-premises, in the cloud or within embedded hardware platforms. For example, marketing analytics software processes sensitive data about clients and visitors and can keep such data safe during processing by deploying this application in a TEE."

12. PheonixNap From: phoenixnap.com through Google search.

"Trusted Execution Environments (TEEs) are CPU-encrypted isolated private enclaves inside the memory, used for protecting data in use at the hardware level. While the sensitive data is inside an enclave, unauthorized entities cannot remove it, modify it, or add more data to it. The contents of an enclave remain invisible and inaccessible to external parties, protected against outsider and insider threats. As a result, a TEE ensures the following: Data integrity, Code integrity, Data confidentiality. Depending on the vendor and the underlying technology, TEEs can enable additional features"

13. Reddit Post From: reddit.com through Google search.

"The TEE is essentially another, totally separate, totally isolated OS. It runs in parallel with, for example, Android. The TEE is specifically named, because it is way more secure than your REE (your Android, your iOS)."

14. Personal blog From: sergioprado.blog through Google search.

"A Trusted Execution Environment (TEE) is an environment where the code executed and the data accessed is isolated and protected in terms of confidentiality (no one have access to the data) and integrity (no one can change the code and its behavior)."

15. Medium From: medium.com through Google search.

"A Trusted Execution Environment (TEE) is an environment in which the executed code and the data that is accessed are physically isolated and confidentially protected so that no one without integrity can access the data or change the code or its behavior. We are not aware of many devices in the US that use trusted execution environments, including smartphones, set-top boxes, video game consoles, and Smart TVs. A TEE is a secure and integrity-protected processing environment that consists of processing, and storage capabilities."

16. Red Hat From: next.redhat.com through Google search.

"Trusted Execution Environments (TEEs) are a fairly new technological approach to addressing some of these problems. They allow you to run applications within a set of memory pages that are encrypted by the host CPU in such a way even the owner of the host system is supposed to be unable to peer into or modify the running processes in the TEE instance. All TEEs provide confidentiality guarantees for code and data running within them, meaning that the running workload can't be seen from outside the TEE. Some TEEs offer memory integrity protection, which prevents the data loaded into the TEE from being modified from the outside (we will come back to this below). As expected, none provide guaranteed availability, since lower stack levels must still be able to control scheduling and TEE launch, and can block system calls."

17. Scientific Publication From [52] through Google search.

"Trusted execution environments are secure areas of central processors or devices that execute code with higher security than the rest of the device. Security is provided by encrypted memory regions called enclaves. Because the environment is isolated from the rest of the device, it is not affected by infection or compromise of the device. Trusted execution environments have applications

for different usages, such as mobile phones, cloud data processing, or cryptocurrencies. Furthermore, since Trusted execution environments are part of a standard chipset, this inexpensive technology can be leveraged across many devices, resulting in increased security, especially in the mobile sector and IoT products."

18. Scientific Publication From [45] through Google search.

"Trusted Execution Environments (TEEs) are used to protect sensitive data and run secure execution for security-critical applications, by providing an environment isolated from the rest of the system. However, over the last few years, TEEs have been proven weak, as either TEEs built upon security-oriented hardware extensions (e.g., Arm TrustZone) or resorting to dedicated secure elements were exploited multiple times."

19. CSRC From: csrc.nist.gov through Google search.

An area or enclave protected by a system processor.

20. Scientific Publication From [54] through Google search.

"A trusted execution environment (TEE) is a new hardware security feature that is isolated from a normal OS (i.e., rich execution environment (REE)). The TEE enables us to run a critical process, but the behavior is invisible from the normal OS, which makes it difficult to debug and tune the performance. In addition, the hardware/software architectures of TEE are different on CPUs. For example, Intel SGX allows user-mode only, although Arm TrustZone and RISC-V Keystone run a trusted OS. In addition, each TEE has each SDK for programming. Each SDK offers own APIs and makes difficult to write a common program."

21. Scientific Publication From [34] through Google search.

"The Trusted Execution Environment (TEE) offers a software platform for secure applications. The TEE offers a memory isolation scheme and software authentication from a high privilege mode. The procedure uses different algorithms such as hashes and signatures, to authenticate the application to secure. Although the TEE hardware has been defined for memory isolation, the security algorithms often are executed using software implementations."

22. Scientific Publication From [19] through Google search.

"TEEs ensure that code outside of the TEE, including the operating system and hypervisor, cannot compromise the execution integrity and confidentiality of programs run inside the TEE. Based on hardware-rooted trust, TEEs additionally allow to prove the integrity of such execution even to remote third parties (remote attestation). By using TEEs that protect not only against software attackers but also hardware attackers, even the cloud provider is moved out of the trust domain. By leveraging such hardware-based TEEs, there is an alternate approach on building secure multiparty computation toolkits"

23. Linkedin Post From: linkedin.com through Google search.

"A Trusted Execution Environment (TEE) is a secure and isolated area within a computer or mobile device's hardware that can run code and processes with higher levels of security and privacy than the device's main operating system. TEEs are designed to protect sensitive data and processes, such as encryption keys, biometric authentication, and digital payments, from malware, hackers, and other threats. TEEs are typically implemented in microprocessors with hardware-level security features, such as ARM TrustZone or Intel SGX, that provide a separate, isolated environment within the device's main operating system. This isolated environment is designed to prevent unauthorized access to sensitive data or processes and to ensure that code and data executed in the TEE cannot be tampered with or observed by the main operating system or any other software running on the device."

24. NVIDIA Jetson From: docs.nvidia.com through Google search.

"TEE provides an execution environment that includes security features to ensure code and data on a device is protected."

25. ACSM From: australiancybersecuritymagazine.com.au through Google search.

"A Trusted Execution Environment (TEE) is an environment that offers a level of assurance of data integrity, data confidentiality, and code integrity. A hardware-based TEE uses the techniques to provide increased security guarantees for code execution and data protection within that environment."

26. Scientific Publication From [17] through Google search.

"TEEs are an integral part of the security architecture of mobile devices. They provide an execution context where security-critical services, such as user authentication, mobile payment, and digital rights management, can run isolated from the Rich Operating System (Rich OS). "

27. Scientific Publication From [33] through Google search.

"The trusted execution environment (TEE) is one of the reasonable security measures for protecting security-critical services and data on embedded devices. Particularly, considering ARM's high market share in mobile and embedded devices (90% for mobile, IoT, and in-vehicle systems), TrustZone, the security extension of ARM processor, is the most potent measure to enable TEEs on embedded devices. It provides various security extensions, such as separating the security states of the CPU, hardware-based memory access control, and secure IO."

28. Global Platform From: globalplatform.org through Google search.

"The Trusted Execution Environment (TEE) is a secure area in a device that ensures sensitive data is stored, processed, and protected in an isolated and trusted environment. As such, it offers protection against attacks generated in the rest of the device and even other actors inside the TEE."

29. IBM From: ibm.com through Google search.

"The AIX security feature of Trusted Execution (TE) environment provides protection to the installed components and software applications. This security feature is achieved by maintaining and validating integrity of each component of the system and installed supported applications. The kernel trusts and invokes only those objects that the kernel can validate the integrity successfully. Any untrusted object is denied permission to execute. The TE feature of AIX protects the system against many malware that might gain access to the system and infect legitimate system or application components, causing unauthorized execution of the malware code along with the legitimate application."

30. ArgusSec From: argus-sec.com through Google search.

"The Trusted Execution Environment (TEE) is a secure area that resides alongside the Rich Execution Environment (REE) of the main processor in connected devices, most notably smartphones. The purpose of the TEE is to provide a trusted and isolated environment

in which sensitive data and assets can be stored, and trusted code executed, protecting these sensitive assets and Trusted Applications (TAs) from any software attacks generated within the REE."

31. Applus From: appluslaboratories.com through Google search.

"The TEE is a secure execution environment that runs in parallel with the operating system of the device (e.g. Android) and where only authorised and reliable applications are run (trusted apps). The TEE uses software and hardware security resources to protect the applications which are being executed in the TEE. This increases the security in the storage and processing of the sensitive data managed by the trusted applications. Furthermore, the TEE provides secure applications with a standardized set of routines and functions (APIs) that facilitate their development. This solution is applicable not only to smart phones but also to other devices such as tablets, Smart TV, set-boxes and other products that manage sensitive data and are connected to the Internet (Internet of things)."

32. Azeria Labs From: azeria-labs.com through Google search.

"Modern operating system kernels are also large, and have similar problems avoiding memory-corruption vulnerabilities. Isolating these kernels is a lot more complicated than for normal programs. To do this, device developers can make use of a Trusted Execution Environment (TEE). These TEEs isolate critical code and data away from the main operating system, so that even if the main operating system is compromised, the data and code residing inside the TEE remains isolated. Use-cases for TEEs include verifying the integrity of the operating system itself, managing user credentials such as via a fingerprint sensor, and the storage and management of device encryption keys. High-value assets are not limited to kernel-mode components. Video Digital Rights Management (DRM) applications, banking applications and secure messengers may also want to protect their code and data from devices that may have malware installed."

33. Bitfount From: bitfount.com through Google search.

"Trusted Execution Environments (TEEs) are one mechanism for enabling multiple parties to collaboratively do computation. As the name suggests, the security depends on the computation running in an environment that all the parties trust. Imagine a clean room or bunker where everyone knows data can come in but only information they are comfortable with goes out."

34. Cryptologie From: cryptologie.net through Google search.

"Trusted Execution Environment (TEE) is a concept that extends the instruction set of a processor to allow for programs to run in a separate secure environment. The separation between this secure environment and the ones we are used to deal with already (often called rich execution environment) is done via hardware. So what ends up happening is that modern CPUs run both a normal OS as well as a secure OS simultaneously. Both have their own set of registers but share most of the rest of the CPU architecture (and of course system). By using clever CPU-enforced logic, data from the secure world cannot be accessed from the normal world. Due to TEE being implemented directly on the main processor, not only does it mean a TEE is a faster and cheaper product than a TPM or secure element, it also comes for free in a lot of modern CPUs."

35. Stack Exchange From: security.stackexchange.com through Google search.

"A trusted execution environment (TEE) provides a way for one to deploy tamper-proof programs on a device. The most prominent example of TEEs seem to be Intel SGX for PCs."

36. NXP From: nxp.com, through Google search.

"Building more secure embedded system products starts with utilizing advanced hardware security features such as a trusted execution environment (TEE). A TEE isolates sensitive data and processes from non-secure processes, creating secure or trusted zones and non-secure, non-trusted zones in your embedded system product."

A.1 Example of a misleading explanation

From: **NY Times** nytimes.com

"A trusted execution environment that protects software from most kinds of attack. Within the secure enclave, bits of computer code, called smart contracts, allow data owners to control who has access to their data and how it is used."

B Candidate Trusted Execution Environment Explanations

Candidate TEE explanations are composed of 2-3 sentences, where each sentence has a different theme. We evaluate every combination of the 2-3 sentences in our surveys. Each theme is shown below in *italics*, followed by the corresponding sentence from our evaluation.

Sentence 1: Introducing TEEs
Hardware: A Trusted Execution Environment (TEE) is a technique for running programs and interacting with data securely using a protected area of the physical computer.
Trust: A Trusted Execution Environment (TEE) is a technique for running programs and interacting with data securely, even if the rest of the computer is not trustworthy.
Unsubstantial: A Trusted Execution Environment (TEE) is a technique for running programs and interacting with data securely.

Sentence 2: Isolation, confidentiality, and integrity
Technical: A program running in a TEE is isolated from the rest of the computer to protect the confidentiality and integrity of the program and data.
Non-Technical: A program running in a TEE is isolated from the rest of the computer to allow only authorized people to view or change the program and data.

Sentence 3: (Optional) threat prevented by TEE
Prevents: The TEE protects the program and data even when other software on the computer is behaving maliciously.
No Prevents: (No third sentence)

C Complete Scenario Text

This section includes the complete scenario text from our surveys. We use [brackets] to show small differences between scenarios with and without AI (in that order). We note larger differences in (parentheses).

Medical scenarios Suppose you have been invited to participate in a [**medical research study**/**medical research study**].

(Scenario with AI only) The goal of the study is to **develop an AI tool** which can lead to more accurate diagnosis. If the research

is successful, the doctor at your local clinic might use the tool during your visits. Researchers are asking you to share clinical notes, diagnostic tests, and other related health data from the last 5 years, all identified with your name and address.

(Scenario without AI only) The goal of the study is to **determine where to build a new hospital** by investigating transportation-related barriers that might make it more difficult for some patients to receive routine preventative healthcare. If the research is successful, your city may build a new hospital closer to your home. Researchers are asking you to share your name and address, as well as your relevant medical history.

You are also told:

- After being collected, your data will be securely transmitted and stored so that only a small team of researchers will have access to your data
- Everyone else will only have access to the AI tool trained on everyone's combined data
- In the future, your data may be used for other research studies

The researchers also explain that both your data and the [entire AI tool training process/researcher's calculations] will be **protected by a TEE**.

Smart home scenarios Suppose you are shopping for a [**new voice assistant**, like an Amazon Alexa or a Google Home/**smart light bulb**].

(Scenario with AI only) You read about one model online that uses AI to process your voice commands. You can also control the device using an app on your phone. The data collected by the device includes anything you enter into the app as well as the history of your interactions with the assistant (specifically, your name and address, when you make requests, what requests you make, and your voice), which might be used by the company to continue to **improve the AI** and could help it recognize your voice better.

(Scenario without AI only) You read about one model online that you can control using an app on your phone. The data collected by the device includes anything you enter into the app as well as the history of your interactions with the light (specifically, your name and address, when you turn on the light, and what setting you use), which might be used by the company to **develop new light bulbs** that you might be interested in purchasing.

You read that:

- After being collected, your data will be securely transmitted and stored so that only a small team of developers will have access to your data
- Everyone else will only have access to the AI model trained on everyone's combined data
- In the future, your data may be used to develop other devices at the same company

You also read that both your data and the [entire AI tool training process/developer's work] will be **protected by a TEE**.

D Survey Instrument

This section has the detailed survey questions for both surveys. We use [brackets] to indicate places where questions differ between scenarios. Details about survey flow and differences between Survey 1 and 2 are shown in **bold text** while placeholders for scenario text/TEE explanations/FAQ, and other commentary not in the survey are shown in *italics*. We use ∘ to list answer choices. All questions are single choice closed-ended questions unless otherwise noted. Both surveys begin with a consent form explaining the study procedures, participation requirements, possible risks and benefits of participating, compensation rates, information about how data is protected, participants' rights related to voluntary participation, and contact information for the authors' institution(s) if they have questions or concerns. After consenting, we collect the participant's Prolific ID.

D.1 Scenario Intro

Scenario text from Appendix C

(1) How confident are you that you understand the scenario we described above?
∘ Completely confident
∘ Somewhat confident
∘ Not at all confident

(2) **Question shown if it is the first scenario** How confident are you that you understand what protections a TEE offers?
∘ Completely confident
∘ Somewhat confident
∘ Not at all confident

The following two questions serve as an attention check for the medical scenario with AI

(3) In the scenario above, what is the goal of the medical study? If you are not sure, please re-read the scenario above.
∘ Develop an AI tool for diagnosing patients
∘ Investigate potential causes of long COVID
∘ Identify factors contributing to mood disorders in teenagers
∘ Understand the impact of reliable social support for new mothers

(4) **Question shown if they answer the previous question incorrectly** In the scenario above, what is the goal of the medical study? Please re-read the scenario above and try again. This is your second chance to get the question correct.
∘ Develop an AI tool for diagnosing patients
∘ Investigate potential causes of long COVID
∘ Identify factors contributing to mood disorders in teenagers
∘ Understand the impact of reliable social support for new mothers

The following two questions serve as an attention check for the medical scenario without AI

(3) In the scenario above, what is the goal of the medical study? If you are not sure, please re-read the scenario above.
∘ Determine where to build a new hospital
∘ Investigate potential causes of long COVID
∘ Identify factors contributing to mood disorders in teenagers
∘ Understand the impact of reliable social support for new mothers

(4) **Question shown if they answer the previous question incorrectly** In the scenario above, what is the goal of the medical study? Please re-read the scenario above and try

again. This is your second chance to get the question correct.
- ○ Determine where to build a new hospital
- ○ Investigate potential causes of long COVID
- ○ Identify factors contributing to mood disorders in teenagers
- ○ Understand the impact of reliable social support for new mothers

The following two questions serve as an attention check for the smart home scenario with AI

(3) In the scenario above, what kind of device are you shopping for? If you are not sure, please re-read the scenario above.
- ○ Smart voice assistant
- ○ Smart refrigerator
- ○ Smart television
- ○ Smart security camera

(4) **Question shown if they answer the previous question incorrectly** In the scenario above, what kind of device are you shopping for? Please re-read the scenario above and try again. This is your second chance to get the question correct.
- ○ Smart voice assistant
- ○ Smart refrigerator
- ○ Smart television
- ○ Smart security camera

The following two questions serve as an attention check for the smart home scenario without AI

(3) In the scenario above, what kind of device are you shopping for? If you are not sure, please re-read the scenario above.
- ○ Smart light bulb
- ○ Smart refrigerator
- ○ Smart television
- ○ Smart security camera

(4) **Question shown if they answer the previous question incorrectly** In the scenario above, what kind of device are you shopping for? Please re-read the scenario above and try again. This is your second chance to get the question correct.
- ○ Smart light bulb
- ○ Smart refrigerator
- ○ Smart television
- ○ Smart security camera

D.2 FAQ Intro

This section is shown in the "Show" FAQ condition of Survey 2 only

On this page, we answer some frequently asked questions about TEEs.

FAQ text from Appendix E

Participants are not allowed to proceed to the next page of the survey until at least 60 seconds have elapsed.

D.3 Willingness and Feeling of Safety

The following questions are about Scenario *Number* and the same TEE description you were shown before. You may re-read the scenario if you click the "show/hide scenario" button. *Show/Hide button for displaying scenario text*

The following is included in the "Show" or "Hide" FAQ conditions of Survey 2 only: We've also answered some frequently asked questions about TEEs. You can read the answers by clicking the "Expand" buttons. *Buttons for displaying the FAQ in the follow-up survey*

TEE explanation from Appendix B

The following question is for medical scenarios only

(5) Imagine that you have enough free time to participate in the medical study described above. In this scenario, how likely would you be willing to participate in the medical study?
- ○ Definitely would
- ○ Maybe would
- ○ Would not
- ○ Not sure (Why?) *Free-response*

The following question is for smart home scenarios only

(5) Imagine that the [voice assistant/smart light bulb] described above is within your budget and you know how to set it up. How likely would you be to purchase the [voice assistant/smart light bulb]?
- ○ Definitely would
- ○ Maybe would
- ○ Would not
- ○ Not sure (Why?) *Free-response*

(6) How safe do you think data would be when it is protected by a TEE?
- ○ Completely safe
- ○ Mostly safe (**Survey 2 only**)
- ○ Somewhat safe
- ○ Not at all safe

The following two questions are for Survey 2 only

(7) We want to understand which aspects of the scenario make you feel that your data would be safe or unsafe. For each of the following aspects of the scenario, tell us how safe it makes you feel your data would be.
- ○ Definitely safe
- ○ Somewhat safe
- ○ Neither safe nor unsafe
- ○ Somewhat unsafe
- ○ Definitely unsafe

  (a) The use of a TEE
  (b) That a [hospital/company] is collecting the data
  (c) The people on the [research/development] team
  (d) Which data is collected
  (e) The purpose of the data collection

(8) If there is anything else about the scenario that makes you feel that your data would be safe or unsafe, what is it? Does it make you feel that your data would be safe? Or unsafe? *Free-response*

(9) What questions do you still have about TEEs, if any? *Free-response*

The following question is for Survey 1 only

(10) How much would knowing the answers to these questions change your willingness to [participate in the medical study/purchase the voice assistant/purchase the light bulb]?
- Definitely would change
- Probably would change
- Probably would not change
- Definitely would not change
- I have no questions

D.4 Comprehension

The following questions are about Scenario *Number* and the same TEE description you were shown before. You may re-read the scenario if you click the "show/hide scenario" button. *Show/Hide button for displaying scenario text*

The following is included in the "Show" or "Hide" FAQ conditions of Survey 2 only: We've also answered some frequently asked questions about TEEs. You can read the answers by clicking the "Expand" buttons. *Buttons for displaying the FAQ in the follow-up survey*

TEE explanation from Appendix B

(11) Based on what you read above *about TEEs*, please tell us whether the following statements are true or false. *The True/False questions are shown in Table 4*

(12) How confident are you about your answers to the questions on this page?
- Completely confident
- Somewhat confident
- Not at all confident

(13) After answering the questions on this page, how confident are you that you understand what protections a TEE offers?
- Completely confident
- Somewhat confident
- Not at all confident

(14) After answering the questions on this page, how safe do you think data would be when it is protected by a TEE?
- Completely safe
- Somewhat safe
- Not at all safe

D.5 Demographics and Feedback

In the last part of the survey, we want to learn more about your background. You will also have an opportunity to give us feedback at the end.

(14) Before this survey, were you familiar with the concept of TEEs?
- Yes
- No
- I'm not sure/Other *Free-response*

(15) Are you employed in a computing field (e.g., IT, software engineer, programmer)?
- Yes
- No
- No, but I have been in the past
- I'm not sure/Other *Free-response*

(16) Do you have formal education in a computing field (e.g., degree in computer science or computer engineering)?
- Yes
- No
- I'm not sure/Other *Free-response*

(17) Do you have prior experience with medical research?
- Yes, as a participant
- Yes, as a researcher
- No
- I'm not sure/Other *Free-response*

(18) Do you work in a medical field (e.g. nurse, doctor, hospital staff)?
- Yes
- No
- No, but I have been in the past
- I'm not sure/Other *Free-response*

(19) Do you own any smart devices? When we say "smart devices" we are referring to devices that can be controlled remotely or interact with each other over the internet, including: smart TVs, smart voice assistants (e.g., Alexa, Google Home), smart light bulbs, doorbells, cameras, and more.
- Yes, and I use the smart features
- Yes, but I don't use the smart features
- No
- No, but I have in the past
- I'm not sure/Other *Free-response*

(20) Do you have experience with home automation? When we say "home automation" we are referring to setting up smart devices to operate automatically, either by using schedules, routines, or scenes; or through another service like IFTTT or SmartThings.
- Yes, I currently use home automation
- Yes, I have used home automation, but not currently
- No, I do not use home automation, but I do own smart devices
- No, I don't own smart devices
- I'm not sure/Other *Free-response*

E FAQ Text

In the follow-up survey, we answer some of the frequently asked questions from the first survey.

1. How do TEEs work? The details of how different TEEs work can vary. For example, Arm TrustZone is a feature of modern processors that splits computer resources between a "Normal World" and a "Trusted World" (a TEE). Software running in each world has access to different regions of memory. Software running in the Normal World cannot access or modify data in the Trusted World. TrustZone is appropriate for protecting entire trusted applications while Intel SGX, on the other hand, works well with software that has both trusted and untrusted parts. SGX allows software to create one or more "enclaves" (TEEs). The data in the enclave can only be accessed while the trusted part of the software is running.

2. How do we know the TEE is working correctly? TEEs support hardware-based cryptographic functions that can be used

to guarantee that both the TEE and all the code running in the TEE are configured properly. This process is called "attestation". Researchers are also working on new ways to ensure that software running in a TEE works as expected.

3. How are TEEs used in real life? TEES are used in computers, smart phones, and other devices. For example, authentication in modern Android phones is typically handled by code (called "Gatekeeper") residing in a TEE based on ARM TrustZone. For example, when you enter a PIN or scan your fingerprint to unlock your phone, it is sent to GateKeeper in the secure zone of the CPU to verify. The response from GateKeeper is encrypted with a secret, hardware-backed key that is never shared outside the TEE.

F Aspects

The complete set of comprehension questions from Survey 1 and 2 are shown in Table 4. Tables 5- 8 include details about our statistics.

G Additional Results and Statistics

Results for the True/False comprehension questions in the initial survey are summarized in Tables 9 and 10. The first table includes results overall and split by scenario, while the second table splits the results by TEE explanation. Table 11 has similar data for Survey 2, split by TEE explanation and FAQ type.

The regression table for questions about participants' willingness to use the TEE-enhanced technology and their belief that the TEE will keep the data safe.

H Questions About TEEs

The codebook used to analyze the questions asked by participants is shown in Table 12. Each response could receive codes from multiple categories and up to two codes from the *TEE*, *Scenario*, and *Risk* categories.

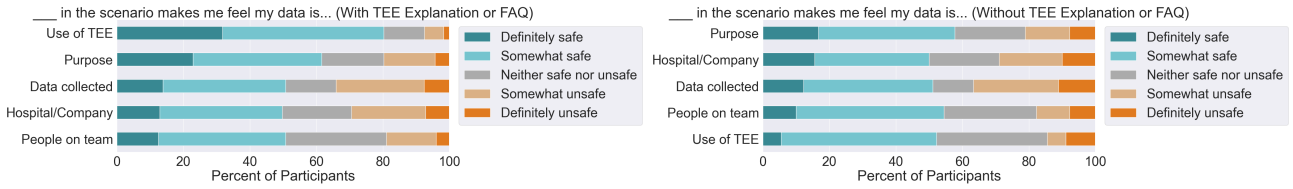
For this first codebook, we identified six main codes: *distrust, risk, general, real, scenario*, and *guarantees* (see Table 12 for the full codebook). In the *distrust* group, we have sub-codes like *distrust TEE* or *distrust manufacturer* where the participants do not ask questions but instead express a lack of trust in a particular aspect. The second group involves *risk* related codes, capturing instances where participants mention risks such as hacking or data leaks. The third group consists of *general* codes, which are predominantly questions. A frequent sub-code here is *how*, where participants ask broad questions about how the TEE works. This category also includes codes related to questions about encryption, isolation, and other technical aspects. The fourth group consists of questions about the *real* use of TEEs outside of the scope of our study. The fifth group consists of *scenario*-related codes, focusing on the elements not directly tied to the TEE but to the scenario described. For example, when participants ask questions about the hospital in the Medical scenario or the privacy policy of particular manufacturers. Finally, the sixth group deals with *guarantees*, where participants ask for assurances on the TEE functionality.

The frequency of codes for questions asked by participants are shown in Figure 12.

I Other Aspects Contributing to Feeling Data is Safe or Unsafe

We asked participants if there were any other aspects of the scenario that made them feel their data would be safe/unsafe. The codebook used to analyze these responses is shown in Table 13.

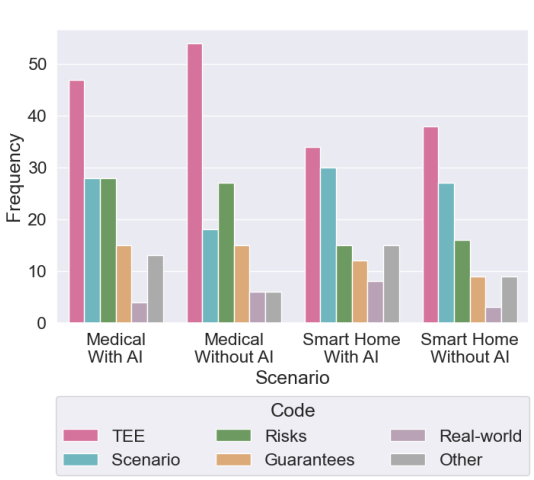
The second codebook focuses on which aspects of the scenario make the participants feel safe or unsafe. This codebook is divided into four main groups: *distrust*, *trust*, *information*, and *miscellaneous* (see Table 13 for the full codebook). The first group is about *distrust*, where the participant mentions specific elements of the scenario that make them feel that their data would be unsafe. For example, they may express concerns about the AI used or fear hackers. The second group includes *trust*-related codes that make participants feel safe in the scenario. These codes include positive perceptions of the TEE or the people involved. The third group, *information*, consists of codes where participants do not explicitly mention aspects that feel safe/unsafe but instead request additional information. For example, asking questions about the data retention policies of the hospital. The final group is *miscellaneous*. Here, we have codes that do not fit into the previous categories. These describe answers where the participant gave unclear answers or mentioned unrelated technologies.



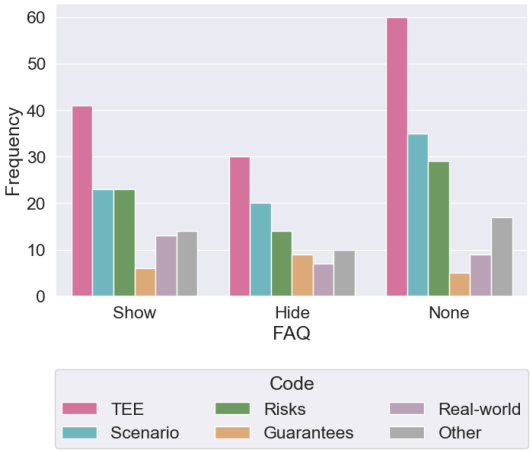
(a) Aspects of the scenario contributing to the belief that the data would be safe/unsafe, with a TEE explanation or FAQ

(b) Aspects of the scenario contributing to the belief that the data would be safe/unsafe, without a TEE explanation or FAQ

Figure 3: Willingness to use TEE-enhanced technology, overall belief that the TEE will keep data safe, and aspects of the scenario contributing to those beliefs.



(a) Question frequency for Survey 1, split by scenario.



(b) Question frequency for Survey 2, split by FAQ condition.

Figure 4: Question frequency for both surveys.

Q#	T/F	Question Text
Q1	F	A member of the general public can access your data
Q2	F	___ can access your data *Medical*: A hospital employee unrelated to the research team *Smart home*: Someone working at the company on an unrelated team
Q3	F	If there were a bug in other software on the computer, outside of the TEE storing your data, then a hacker could use the bug to access your data
Q4	F	If a disgruntled [___] installed a malicious program on the computer storing your data, then they could access your data *Medical*: hospital employee unrelated to the research team *Smart home*: employee on an unrelated team
Q5	F	Other [___] working on different projects on the same computer can access your data *Medical*: researchers *Smart home*: developers
Q6	T	A member of the [___] can access your data *Medical*: research team *Smart home*: development team
Q7	T	If [___] makes a mistake collecting your data, then your data could be incorrect *Medical*: a member of the research team *Smart home*: the light bulb / the voice assistant
Q8	T	A [___] could later use your data to [___] *Medical without AI*: A member of the research team / choose the location for a new fire station *Medical with AI*: A member of the research team / train another AI diagnosis tool for a different medical condition *Smart home*: Someone on the development team / develop a smart vacuum
Q9	F	The TEE ensures [___] *Medical without AI*: the hospital being constructed will be closer to the patients who most need it *Medical with AI*: the diagnosis made by the AI tool will always be correct *Smart home without AI*: the new light bulbs will have features relevant to you *Smart home with AI*: your voice will always be recognized by the improved AI
Q10	T	[___] could steal your data and sell it on the dark web *Medical*: A member of the research team *Smart home*: Someone on the development team
Q11	T	When you unlock your Android phone with a PIN, the PIN is verified in a TEE
Q12	F	We cannot be sure that a TEE is configured correctly

Table 4: Questions for evaluating TEE concept comprehension. The expected answer (True or False) is shown in the second column. Q11 and Q12 only appear in the follow-up survey. We note the places where the questions differ between scenarios.

	Medical				Smart Home			
	With AI		Without AI		With AI		Without AI	
Aspects	W	p-value	W	p-value	W	p-value	W	p-value
Use of TEE	1421	0.002597**	1638.5	0.0002417***	1483.5	0.0006844***	1547.5	0.0005205***
Purpose	2168	0.636	2689	0.8193	2231	0.3749	2258.5	0.3077
Data Collect	2258	0.8642	2815.5	0.8709	2363	0.6407	2384	0.5405
Hospital/Company	2090	0.4634	3285	0.09689	2637.5	0.6806	2263	0.3194
People on the team	1965	0.2447	3412.5	0.04132*	2580	0.8183	2309.5	0.3909

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$

Table 5: Table with results of Mann-Whitney U tests for the aspects contributing to the belief that the data would be safe/unsafe, with information about the TEE (TEE explanation or FAQ) vs no TEE information provided. Each scenario was treated separately. Statistical significance is noted with asterisks.

	Medical				Smart Home			
	With AI		Without AI		With AI		Without AI	
	W	p-value	W	p-value	W	p-value	W	p-value
Average Score	8226	0.5146	11723	$1.505e-06^{***}$	10020	0.004367^{**}	13756	$4.378e-09^{***}$

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$

Table 6: Table with results of Wilcoxon signed-rank tests comparing the average score for questions Q1-Q5, to the average score for questions Q6-Q10 in the follow-up study. Each scenario was treated separately. Statistical significance is noted with asterisks.

Medical Scenario Without AI										
Variable	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Q9**	**Q10**
Explanation sentence 1 [Baseline = Unsubstantial]										
Hardware	1.52	0.38	1.32	0.99	0.43	1.03	0.47	0.91	0.41**	1.28
Trust	1.46	0.54	1.97	0.99	0.56	1.51	0.70	1.51	0.79	0.93
Explanation sentence 2 [Baseline = Technical]										
Non-technical	1.17	8.50**	0.93	1.19	1.39	1.63	0.89	1.15	1.08	1.22
Explanation sentence 3 [Baseline = No Prevents]										
Prevents	0.68	1.11	1.89*	3.67***	1.04	0.90	0.74	0.99	1.14	0.53*
Medical experience	0.24	0.92	1.09	2.12	1.34	0.84	1.02	1.02	1.31	1.40
CS experience	0.73	1.63	0.97	1.21	1.42	1.17	1.08	1.70	1.45	0.93
Medical Scenario With AI										
Variable	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Q9**	**Q10**
Explanation sentence 1 [Baseline = Unsubstantial]										
Hardware	1.03	4.95	1.07	1.12	1.12	2.83	1.86	1.51	0.88	0.73
Trust	0.17	0.46	0.86	0.84	1.16	1.43	1.63	1.20	0.84	1.04
Explanation sentence 2 [Baseline = Technical]										
Non-technical	0.79	1.60	1.11	0.63	1.54	0.89	0.63	0.61	0.58	2.03*
Explanation sentence 3 [Baseline = No Prevents]										
Prevents	0.57	0.39	1.70	2.83**	1.27	0.96	1.75	1.67	0.54	1.01
Medical experience	1.38	2.20	1.23	1.01	0.79	1.31	0.95	2.75	3.10	3.60***
CS experience	0.23*	0.44	0.87	0.468*	0.39*	0.93	1.27	1.49	0.79	1.30
Smart Home Scenario Without AI										
Variable	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Q9**	**Q10**
Explanation sentence 1 [Baseline = Unsubstantial]										
Hardware	0.96	0.52	0.76	0.70	1.02	1.21	0.90	0.90	0.92	1.38
Trust	0.62	0.63	1.39	1.21	0.75	0.93	0.71	0.99	0.88	1.21
Explanation sentence 2 [Baseline = Technical]										
Non-techncial	0.84	2.56	1.26	0.92	1.04	1.32	0.87	1.12	0.78	1.27
Explanation sentence 3 [Baseline = No Prevents]										
Prevents	0.37	0.99	1.07	1.67	1.17	1.03	0.59	1.03	1.12	1.01
Smart home experience	0.00	0.23	0.28*	0.36	0.63	0.57	0.60	0.73	0.45*	0.97
CS experience	0.17*	1.51	0.70	0.59	0.85	0.37*	0.95	0.51*	1.93	0.65
Smart Home Scenario With AI										
Variable	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Q9**	**Q10**
Explanation sentence 1 [Baseline = Unsubstantial]										
Hardware	0.44	0.90	1.36	1.48	1.34	0.70	0.66	0.90	0.61	0.66
Trust	0.18	0.35	1.42	0.81	0.80	0.80	1.17	1.49	0.50*	1.02
Explanation sentence 2 [Baseline = Technical]										
Non-technical	1.14	2.03	1.15	0.70	0.95	1.02	0.54	1.23	1.12	1.42
Explanation sentence 3 [Baseline = No Prevents]										
Prevents	0.55	2.08	0.68	2.69**	2.23	1.16	1.30	1.12	0.78	0.67
Smart home experience	0.55	2.08	0.68	1.26	1.20	0.52	1.06	0.70	1.01	0.61
CS experience	0.45	0.63	1.17	1.26	0.68	1.07	1.39	1.27	1.52	1.34

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$

Table 7: Regression table for True/False comprehension questions in Survey 1 where each question in each scenario is a different model (40 models total). The numbers are the odds ratios for each predictor, with the baseline used in each model noted in *italics*. Statistical significance is noted with asterisks and shaded cells: blue for positive and orange for negative coefficients.

Medical Scenario Without AI												
Variable	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Q9**	**Q10**	**Q11**	**Q12**
Explanation [Baseline = No Explanation]												
Unsubstantial	0.66	0.31	2.14*	2.01	2.59*	0.26	1.42	0.98	1.26	0.67	0.61	1.23
Hardware	1.93	0.76	2.53*	4.22**	1.92	0.49	1.34	0.88	1.55	0.72	0.58	1.40
Trust	0.71	0.19*	3.90**	2.69*	1.65	0.61	0.90	0.82	1.15	0.70	0.67	1.17
FAQ [Baseline = No FAQ]												
Hidden	7×10^7	1.34	3.63**	1.39	2.05	1.27	−0.75	1.13	0.93	0.44*	19.30***	6.23***
Shown	1.70	2.32	1.45	1.97	2.03	0.75	0.37	0.74	1.20	0.36**	23.81***	6.42***
Medical Exp	0.38	2.64	0.89	0.58	0.63	0.47	1.04	1.52	0.90	1.13	1.36	0.90
CS Exp	0.43	0.91	1.11	1.40	1.09	0.68	0.90	1.22	1.14	0.98	1.04	0.71

Medical Scenario With AI												
Variable	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Q9**	**Q10**	**Q11**	**Q12**
Explanation [Baseline = No Explanation]												
Unsubstantial	3.56	1.48	1.75	3.35**	3.60*	2.51	2.86	1.31	3.03*	1.57	0.55	0.58
Hardware	5.00	2.41	2.20*	2.41*	2.23	2.53	1.73	1.55	1.43	0.99	0.92	0.79
Trust	1.27	1.21	1.68	2.69*	0.99	5.26*	1.88	1.39	2.03	1.42	1.14	0.53
FAQ [Baseline = No FAQ]												
Hidden	0.99	2.16	0.87	1.22	1.28	0.24*	1.54	0.26**	0.79	0.62	9.97***	3.32***
Shown	1.60	3.71*	1.14	1.28	1.06	0.58	2.14	0.44	0.92	0.86	26.31***	4.76***
Medical Exp	0.50	0.61	0.70	0.46*	0.78	0.53	1.28	1.75	0.55	1.57	0.96	0.66
CS Exp	2.32	0.88	0.64	0.39**	1.13	0.41	1.03	1.88	1.12	1.03	1.72	0.84

Smart Home Scenario Without AI												
Variable	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Q9**	**Q10**	**Q11**	**Q12**
Explanation [Baseline = No Explanation]												
Unsubstantial	0.23	0.99	2.18	2.92*	0.59	1.07	1.21	1.17	0.95	1.42	0.53	0.59
Hardware	0.30	1.68	2.69*	2.86*	1.22	0.68	0.98	0.66	0.90	1.17	0.58	0.81
Trust	0.54	1.43	1.84	2.01	0.90	2.18	1.63	1.39	0.87	1.31	0.92	0.74
FAQ [Baseline = No FAQ]												
Hidden	2.16	1.15	1.11	1.36	1.62	1.14	0.95	1.08	0.59	0.54*	19.89***	3.13***
Shown	5.00	3.10	1.14	1.21	2.53*	1.99	0.46	0.68	0.81	0.80	18.73***	4.18***
Smart Home Experience	1.54	1.02	1.97	2.12	2.08	1.05	1.02	1.05	0.74	0.73	1.42	1.17
CS Exp	0.35	1.23	0.58	0.54	0.68	0.76	0.84	2.10	2.36**	1.15	1.67	0.66

Smart Home Scenario With AI												
Variable	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Q9**	**Q10**	**Q11**	**Q12**
Explanation [Baseline = No Explanation]												
Unsubstantial	2.44	2.41	3.46**	2.77*	5.16***	0.39	0.99	0.86	0.65	0.99	0.63	0.94
Hardware	1.90	2.05	3.00**	3.06**	3.22**	0.93	1.14	0.89	1.21	0.50	0.71	1.06
Trust	0.51	0.95	3.13**	2.29*	2.16	0.53	1.63	0.78	1.19	0.71	0.68	0.86
FAQ [Baseline = No FAQ]												
Hidden	1.05	0.83	1.07	1.17	0.75	0.72	0.58	0.77	0.98	0.53	12.55***	3.49***
Shown	0.84	0.49	2.36*	1.26	1.15	0.54	0.67	0.44*	0.69	0.60	43.38***	3.67***
Smart Home Experience	3.25	0.27	1.27	0.59	0.28*	0.38	0.37	0.50	0.47*	0.66	2.18	0.85
CS Exp	0.24	0.53	0.71	0.55	1.04	1.27	0.79	0.83	1.68	1.34	1.54	0.66

$^{***}p < 0.001$; $^{**}p < 0.01$; $^{*}p < 0.05$

Table 8: Regression table for True/False comprehension questions in survey 2. There is one logistic regression model for each question in each scenario (48 models total). The numbers in this table are the odds ratios for each predictor, with the baseline explanations used in each model noted in *italics*. Statistical significance is noted with asterisks and shaded cells: blue for positive coefficients and orange for negative coefficients.

Q#	T/F	Overall	Medical		Smart Home	
			With AI	Without AI	With AI	Without AI
Features of TEEs						
Q1	F	96.7%	96.2%	97.0%	96.6%	97.0%
Q2	F	91.9%	92.4%	93.1%	90.6%	91.5%
Q3	F	79.0%	80.9%	76.8%	78.1%	80.1%
Q4	F	80.9%	83.1%	81.5%	80.7%	78.4%
Q5	F	84.2%	83.5%	84.1%	87.1%	82.2%
Limitations of TEEs						
Q6	T	87.2%	91.1%	87.6%	83.3%	86.9%
Q7	T	82.0%	86.9%	80.3%	82.0%	78.8%
Q8	T	69.8%	87.3%	63.1%	66.1%	62.7%
Q9	F	61.1%	82.2%	57.1%	54.1%	50.8%
Q10	T	57.2%	59.3%	55.4%	61.4%	53.0%

Table 9: Overall scores for each comprehension question highlighting features and limitations of TEEs and the correct answers. Results are split by scenario.

	T/F	Overall	First sentence			Second sentence		Third sentence	
			Hardware	Trust	Unsubstantial	Technical	Non-technical	Prevents	No Prevents
Features of TEEs									
Q1	F	96.7%	97.8%	94.5%	97.8%	96.6%	96.8%	95.7%	97.7%
Q2	F	91.9%	94.0%	87.7%	93.9%	88.7%	95.1%	91.5%	92.3%
Q3	F	79.0%	78.6%	81.8%	76.6%	78.4%	79.6%	82.5%	75.5%
Q4	F	80.9%	80.5%	80.8%	81.4%	82.7%	79.1%	87.8%	74.0%
Q5	F	84.2%	84.6%	82.5%	85.6%	82.9%	85.5%	85.9%	82.6%
Limitations of TEEs									
Q6	T	87.2%	88.1%	87.3%	86.2%	86.1%	88.3%	87.2%	87.2%
Q7	T	82.0%	79.6%	82.8%	83.7%	84.0%	80.0%	81.6%	82.3%
Q8	T	69.8%	67.9%	73.7%	67.9%	69.2%	70.4%	71.2%	68.5%
Q9	F	61.1%	56.9%	60.1%	66.3%	62.8%	59.4%	60.5%	61.7%
Q10	T	57.2%	57.5%	58.1%	56.1%	53.0%	61.5%	53.8%	60.6%

Table 10: Overall scores for each comprehension question in Survey 1, highlighting features and limitations of TEEs and the correct answers. Results are split by TEE explanation.

Q#	T/F	Overall	Show	Hide	None	Hardware	Trust	Unsubstantial	None
Features of TEEs									
Q1	F	96.2%	97.0%	97.6%	94.0%	97.6%	95.5%	95.3%	96.3%
Q2	F	88.3%	89.9%	89.2%	85.9%	92.0%	85.4%	89.4%	86.5%
Q3	F	71.4%	74.4%	73.2%	66.8%	77.2%	76.4%	74.4%	57.4%
Q4	F	73.9%	76.2%	75.6%	70.1%	80.8%	77.2%	78.3%	59.0%
Q5	F	81.6%	83.8%	83.1%	77.8%	86.0%	79.7%	86.2%	74.2%
Limitations of TEEs									
Q6	T	90.9%	91.2%	89.8%	91.9%	90.8%	93.5%	88.2%	91.4%
Q7	T	86.1%	84.5%	86.1%	87.7%	86.0%	87.4%	87.8%	83.2%
Q8	T	72.0%	67.4%	72.6%	76.0%	70.0%	72.8%	73.6%	71.7%
Q9	F	55.4%	54.9%	53.6%	57.8%	56.8%	56.9%	55.9%	52.0%
Q10	T	61.8%	60.1%	54.8%	70.4%	56.0%	62.2%	65.7%	63.1%
FAQ-specific Questions									
Q11	T	65.7%	89.3%	82.2%	26.0%	66.8%	68.3%	59.8%	68.0%
Q12	F	58.2%	71.6%	67.8%	35.6%	62.0%	56.5%	54.7%	59.8%

Table 11: Overall scores for each comprehension question in Survey 2, highlighting features and limitations of TEEs and the correct answers. Results are split by FAQ type and TEE explanation.

Code	Description	Frequency First survey	Frequency Follow-up
Questions about TEEs			
How?	General questions about how TEEs work	49	31
Isolation	Questions about how "isolation" works	21	7
Implementation	Questions about what hardware is involved/other implementation details	15	14
Features	Questions about what else the machine can do	15	0
Answered	Questions already answered in the scenario text/TEE explanation received by the participant	13	1
Encryption	Questions about the cryptography involved	11	2
Tech	Questions comparing TEEs to other technology	9	8
Authorization	Questions about the authorization process giving access to the TEE	5	1
Different	Questions that would have been answered by a different TEE explanation	3	0
Open-Source*	Questions about whether software supporting TEEs is open-source	-	3
What?*	General questions about what a TEE is	-	17
Non-technical*	Request for a less technical explanation of TEEs	-	13
Visual*	Request for a visual description of TEEs	-	4
Misc.	Other questions about TEEs, appearing in fewer than 5 responses in the first survey	32	30
Questions about the scenario			
Data	Questions about what is collected, how/when data is anonymized, data retention policies, etc.	41	25
People	Questions about the people in the scenario	25	28
Future	Questions about the future use of data clause in the scenario text	8	6
Positive	Mention that they are less worried about this scenario than the other	6	0
Fail	Questions about the hospital's/company's procedures if there is a data breach	5	4
Compensation	Questions about how they will be compensated for giving their data	5	1
Misc.	Other questions about the scenario, appearing in fewer than 5 responses in the first survey	13	14
Questions about potential risks			
Hacking	Questions about hacking/hackers	27	28
People	Questions about how people (on the research/development team, or not) might leak the data	23	12
Fail	Questions about what happens to their data if the TEE fails	12	2
Misc.	Other questions about risks, appearing in fewer than 5 responses in the first survey	24	24
Questions about guarantees			
General	Questions about how they know the TEE will work/how good they are	46	15
Testing	Questions about how TEEs are tested	4	4
Cert	Questions about whether/how TEEs are certified	1	0
(Non-)Questions expressing distrust			
General	Express distrust, but the distrust is vague or about data collection in general	16	23
TEE	Indicates they don't trust the TEE	10	6
Scenario	Indicates they don't trust the technology in the scenario	10	9
Manufacturer	Indicates they don't trust the manufacturer of the technology in the scenario or the TEE	7	3
Questions about TEE use in real life			
Breaches	Questions about whether TEEs have been involved in real breaches	11	5
Request	Request to try one for themselves	4	1
Real	Questions about whether TEEs are real	4	7
New	Questions about how new TEEs are	2	1

Table 12: Codebook for questions asked by participants for both surveys. Codes marked with an asterisk* were used in the follow-up survey only.

Code	Description	Frequency
Aspects of the scenario contributing to feeling data is unsafe		
General	General distrust, the belief that no data is (truly) safe	54
Hacker	Mentions hacker/hacking	52
Breaches	Mentions real or hypothetical breaches	42
Future Use	Feel uncomfortable with the idea their data may be used for future research/projects	28
Unnecessary	Believe that unnecessary data collection is taking place	24
AI	The use of AI in the scenario feels unsafe	19
Vague	Feel the data is unsafe, but do not give a specific reason why	15
Human Error	Believe the risk of human error makes their data unsafe	14
Sell	Believe their data will be sold	12
Transmission/Storage	The transmission process/cloud storage seems unsafe	7
Lying	Believe the boundaries set in the scenario text could be untrue	5
Research	The part of the FAQ mentioning "ongoing research" makes the data seem unsafe	5
"Trust"	The emphasis on "trust"/safety makes the data seem unsafe	3
Inference	Believe their personal data could be inferred from whatever is made public from the research/development	2
Data*	The type of data being collected feels unsafe	82
People*	The people involved feels unsafe	67
Destination*	The fact that it is a hospital/company collecting the data feels unsafe	39
Purpose*	The purpose of the data collection feels unsafe	10
TEE*	The involvement of a TEE feels unsafe	6
Aspects of the scenario contributing to feeling data is safe		
Vague	Feel the data is safe, but do not give a specific reason why	105
Boring	Believe their data would not be worth stealing/is not very personal	25
Crypto	The fact that the data is encrypted feels safe	3
Real	Know TEEs have been used in real life/in familiar technology feels safe	3
"Trust"	The emphasis on "trust" makes the data seem safe	3
Inference	Believe their personal data could *not* be inferred from whatever is made public from the research/development	3
AI	The use of AI in the scenario feels safe	2
Transmission	The way the data is transmitted feels safe	1
TEE*	The involvement of a TEE feels safe	76
Purpose*	The purpose of the data collection feels safe	18
People*	The people involved feels safe	12
Destination*	The fact that it is a hospital/company collecting the data feels safe	11
Data*	The type of data being collected feels safe	3
Aspects of the scenario where more information is needed		
TEE	More information is needed about TEEs to know if they feel safe or unsafe	39
Data	More information is needed about data retention/anonymization policies to know if they feel safe or unsafe	25
People	More information is needed about the people and their training to know if they feel safe or unsafe	13
Destination	More information is needed about the policies at and reputation of the hospital/company to know if they feel safe or unsafe	7
Sell	More information is needed about whether the data will be sold to know if they feel safe or unsafe	2
Crypto	More information is needed about the cryptography involved to know if they feel safe or unsafe	2
Other things discussed by participants		
Despite Risk	Indicate they feel safe overall, while acknowledging there is some risk	15
Don't Want	Regardless of how safe the data is, they don't want to participate in the study/buy the device	9
Inaccurate	Response indicates the participant misunderstood our explanation/FAQ	9
Unclear	Unclear from the response whether they feel safe or unsafe	6
Other tech	Suggest another kind of technology to improve safety	4

Table 13: Codebook for aspects of the scenario affecting participants' perception of safety. Codes marked with an asterisk* are repeated from a previous question in the survey.