# Trust TEE?: Exploring the Impact of Trusted Execution Environments on Smart Home Privacy Norms

Pratik Musale
Department of Computer Science
University of Pittsburgh
Pittsburgh, Pennsylvania, USA
prm73@pitt.edu

Adam J. Lee
Department of Computer Science
University of Pittsburgh
Pittsburgh, Pennsylvania, USA
adamlee@pitt.edu

## ABSTRACT

IoT devices like smart cameras and speakers provide convenience but can collect sensitive information within private spaces. While research has investigated user perception of comfort with information flows originating from these types of devices, little focus has been given to the role of the sensing hardware in influencing these sentiments. Given the proliferation of trusted execution environments (TEEs) across commodity- and server-class devices, we surveyed 1049 American adults using the Contextual Integrity framework to understand how the inclusion of cloud-based TEEs in IoT ecosystems may influence comfort with data collection and use. We find that cloud-based TEEs significantly increase user comfort across information flows. These increases are more pronounced for devices manufactured by smaller companies and show that cloud-based TEEs can bridge the previously-documented gulfs in user trust between small and large companies. Sentiments around consent, bystander data, and indefinite retention are unaffected by the presence of TEEs, indicating the centrality of these norms.

## KEYWORDS

Privacy, Trusted Hardware, Trusted Execution Environment, Contextual Integrity

## 1 INTRODUCTION

Internet of Things (IoT) devices often sense sensitive details about users and transmit this information to various recipients over the Internet [22, 56]. The estimated deployment of smart speakers stands at 335.3 million, and cameras stand at 180.7 million by 2027 [10]. It shows the flourishing popularity of these devices and will constitute the highest number of devices in the home [32, 34]. Furthermore, device manufacturers often create integration platforms to utilize the sensed information for other services and service providers, making it a complex task to understand the privacy norms of the users.

Several prior works have studied privacy norms and attempted to measure them using contextual integrity (CI) for smart home personal assistants [2, 3]. Additionally, there was work that studied commercially available IoT devices ranging from speakers, surveillance cameras, fitness tracking bands, thermostats, door locks, and power meters used in the home [1, 8, 9, 20, 29, 39, 53, 65]. The importance of CI methodology is that it can be directly adapted to test the conformity of specific information flow exchanges to privacy norms, providing much-needed data to policymakers, device manufacturers, or the research community. The work has showcased the importance of users' access to the sensed data and get notified of changes in data collection practices or information utilization. However, this body of work studies existing commercial hardware and does not examine the future possibilities of privacy norms that may arise with the changing technologies.

Trusted Execution Environments (TEEs) are an industry initiative to process and compute over data in the secure part of the processor. TEEs store sensitive information encrypted in memory. Remote attestation is used to assert the integrity of secure processes running on other hardware. These types of features can help establish trust in devices computing over private data. The impacts of cloud-based TEEs on privacy norms for data collection and retention, information utilization, and requirement for notifications in the context of smart devices have yet to be studied. In this model, IoT-enabled services running in the cloud make use of TEEs to provide assurances to users regarding the confidentiality of data handled by these services. In this work, we leverage a well-established survey methodology based on scenarios generated by varying parameters within the contextual integrity [41] framework to investigate this space.

With our survey, we examine the following research questions:

(1) Does the introduction of TEEs in cloud-based IoT information flows within a smart home alter the existing privacy norms? Which of the parameters that describe information flows (i.e., the receiver, sender, utilization of data, the type of device used to sense, and the company manufacturing the device) most affect user sentiments in sharing the information under cloud-based TEE deployment model?
(2) Do we observe more confidence in sharing the information for users' correct understanding of the concepts on TEE?

We conducted a between-subject survey on Amazon Mechanical Turk (Mturk) [57] with a total of 1049 participants. The first group of 539 participants responded to inquiries about smart home information flows without TEEs, and the remaining 510 participants responded to inquiries about information flows with TEEs. The survey ran in batches over two weeks until we observed a near equal distribution among populations based on gender, income, and age between both groups. The survey cost $1537 and allowed us to query the acceptance of 48 information sharing scenarios from each participant.

Our work makes the following contributions:

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license visit https://creativecommons.org/licenses/by/4.0/ or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.
Proceedings on Privacy Enhancing Technologies 2023(3), 5–23
© 2023 Copyright held by the owner/author(s).
https://doi.org/10.56553/popets-2023-0067

(1) We show that the presence of a cloud-based TEE has significant influence on user comfort with information flows in the smart home in certain circumstances. These effects can smooth comfort disparities across sensing modalities (i.e., audio vs. video), and are particularly pronounced for devices manufactured by smaller companies.
(2) By contrast, we also find certain features of smart home information flows that are unaffected by the presences of cloud-based TEEs, including sentiments around consent, bystander data, and indefinite data retention. This establishes TEEs as one part of the smart home privacy infrastructure, but not a panacea.
(3) We provide design implications based upon the changes that we observe under cloud-based TEE information-sharing scenarios. These provide the device manufacturers, service providers, and policymakers insights into how TEEs may adjust the privacy landscape in smart homes.

The rest of the paper is organized as follows. In Section 2, we explain the concept of TEEs and CI and review the related work. In Section 3, we describe our survey method, followed by the results of the analysis done on the survey in Section 4. In Section 5, we discuss the implications of our findings. Finally, we discuss the limitation of our work in Section 6, and conclude in Section 7.

# 2 BACKGROUND AND RELATED WORK

## 2.1 TRUSTED EXECUTION ENVIRONMENT

A Trusted Execution Environment (TEE) is a secure area of the processor and that guarantees confidentiality and integrity of code and data [16, 46, 61]. TEEs facilitate trust by keeping applications isolated within the hardware by keeping its stack, heap, and code separate from rest of the processor. This isolation is called an enclave and is provided within ARM TrustZone by splitting the processor into two logical modes: a secure world containing TEE and a normal world containing the normal OS [43]. Because of the split, each has its own registers and memory. On Intel architectures, isolated enclaves are provided by multiplexing the hardware resources between trusted and untrusted software [27]. TEE has three main concepts:

(1) Secure Computing: The untrusted world does not have access to application secrets (e.g., passwords, secret keys) that exist within an enclave. The enclave executes the application code when invoked, and it accesses enclave memory, reads, and writes untrusted memory. A set of entry functions are at the enclave, and untrusted software can utilize to perform certain operations [16].
(2) Secure Storage: The TEE clears all data on termination, and to securely persist sensitive data across executions, enclave data is stored in untrusted memory by encrypting it with TEE-resident secret keys. The enclave can decrypt this data when it is required in future invocations [16].
(3) Remote Attestation: Remote attestation allows a device/user to validate the identity and integrity of a remote enclave. This process also establishes a secret key between the device and enclave upon validation. The secret key protects the communication between the remote enclave and the device [16].

Current work has shown how to utilize the TEE concepts in the IoT ecosystem [42, 50]. There are works that showcase TEE concepts in blockchains to improve smart contracts working [13, 51]. We also see TEE on the mobile platforms of Google [25] and Apple [6] to store credit cards in mobile wallets and secrets required for authentication.

## 2.2 CONTEXTUAL INTEGRITY

The theory of Contextual Integrity (CI) is a well-established framework for studying privacy norms and expectations [41]. CI defines privacy in terms of acceptance of given information exchange to contextual information norms [41]. The norms usually come as a part of context due to specific settings established by law, policies, common practices, or even social pressures. An information exchange that is misaligned with the norms violates the privacy expectation of the user.

Information flows within the CI framework are described by five parameters: (1) the sender of the information, (2) the subject of the information being transferred, (3) the attribute or information type, (4) the recipient of information, and (5) the transmission principle or condition imposed on the transfer of information from the sender to the recipient [8]. The concept of Contextual integrity (CI) has been used to elicit expected general privacy norms across online environments [38, 52].

## 2.3 CONTEXTUAL INTEGRITY USED IN UNDERSTANDING PRIVACY NORMS IN IOT

Several prior works have utilized the CI framework to explore information sharing scenarios in the IoT context [1–3, 8, 9, 20, 29, 39, 53, 65]. This is usually accomplished through the use of factorial vignette surveys [3, 8, 9, 20, 65] or an interview methodology exploring participants' acceptance [1, 2, 53]. Another approach utilized storyboarding techniques with CI parameters to understand users' privacy norms [29].

The work in [8, 9] implemented the CI framework to examine the acceptability of information sharing in IoT devices and toys. They always considered IoT devices' information can get monitored by the internet service provider (ISP) and were one of the recipients. Furthermore, their focus was on understanding the impacts of transmission principles of data retention, notification, and data encryption in the information flows for various recipients. The work in [39] first captures privacy preferences in smart homes, such as considering different senders and attributes to recipients, and proposes a machine learning model for predicting personalized privacy preferences for a user. The work in [20] was focused on understanding and evaluating privacy norms with Google My Activity dashboards and later discussed the advantages of having a dashboard for a user to understand its privacy norms. The research in [65] was on the understanding perception of users on video analytics in which they covered various applications from tracking (attendance and productivity), sentiment analysis, health prediction, and authentication. The work in [29] was concentrated on understanding privacy norms in smart homes with the mitigation strategies used by the users. And later on, they discussed the plausible and the easiest way a device manufacturer or service provider

can provide that service. The rest of the works [1–3, 53] focus on understanding general privacy norms for smart home assistants and associated data sharing risk perceptions.

The work in [1–3] only covered smart speakers as senders, and [65] used only a video camera. In [8, 29, 39], the senders were IoT devices ranging from smart speakers, fitness bands, sleep monitors, thermostats, light bulbs, and cameras. The work [9] used only smart toys with CI for checking COPPA compliance. The work in [20] uses pre-recorded google activities of devices to enquire on privacy norms. Recently [14, 47] are also using smart home devices with IFTT applets for CI inquiry.

## 2.4 OUR APPROACH

We generate information-sharing scenarios within the smart home by varying CI parameters, as described in prior works [8, 9]. Unlike prior work, our flows also consider the deployment of TEEs within these scenarios. We provide quantitative analysis on changes observed in privacy norms and the parameters describing the context under both with TEE and without TEE information flows. And finally, we investigate the impact of a correct understanding of the concepts of TEE on CI parameters and privacy norms.

# 3 METHOD

In this section, we describe our survey-based study methodology, which has been adapted from [8]. We will describe the contextual integrity [41] factors included in our analysis, the design of our survey instrument, and our analysis approach. This study was evaluated and approved by our organization's Institutional Review Board (IRB).

## 3.1 SELECTION CI INFORMATION FLOW PARAMETERS

When considering privacy through the lens of the contextual integrity framework, we must consider the subject, sender, and recipient of the data being shared, the type of data being shared, and the transmission principles governing the data sharing practice [41]. In designing the survey instrument to support our inquiries, we made the following choices when parameterizing these dimensions.

- Subject. Throughout our survey, scenarios investigated the collection of data about either the device owner or other occupants within the space. In each of these cases, we asked respondents to act as if they were the owner of the device collecting data when formulating their response.
- Sender. Given their prevalence in the marketplace, our survey focused on data collected and transmitted by two types of senders: smart cameras and smart speakers. Prior work has shown that a device manufacturing companies has significant impacts on user privacy concerns [18, 19, 31, 62]. To this end, we further divided these senders into subgroups based upon the manufacturing company: established companies like Google and Amazon that provide established products (e.g., Ring, Alexa, Nest) and small companies who provide similar devices (e.g., Wyze, Eufy).
- Recipient. Our survey explored data sharing with six types of recipients: Law Enforcement agencies investigating a reported crime, Device Manufacturers who may seek to understand device utilization, Other Devices at Place that may coordinate activities through platforms such as Apple HomeKit or Samsung SmarthThings, Recommendation Services tha t might connect users to offer/services nearby, Health Services that may monitor patient health or coordinate emergency response, and Family Members or Friends.
- Type of Data. In our survey, the type of data collected and sent was purely a function of the device. The use of audio data was investigated in scenarios involving a smart speaker, while the use of video data was investigated in scenarios involving smart cameras.
- Transmission Principles. The contextual integrity framework relies on the concept of transmission principles to specify constraints or conditions on the circumstances surrounding information use. We built upon prior work [8, 9, 39, 65] and investigated the impacts transmission principles related to notification (e.g., "if you have been notified"), retention (e.g., "if information is not stored", "if information is stored for a duration of 1–3 months", "if the information is stored indefinitely"), and purpose of collection (e.g., "if information is used for maintenance of device/feature", "if the privacy policy mentions the recipient and purpose of sharing").

In line with prior work [8], we build questions for information flows by sampling from this space of contextual integrity parameters. We now describe how our survey instrument investigates these scenarios.

## 3.2 SURVEY DESIGN

To facilitate our study, we created and hosted a survey using the Qualtrics platform [44]. The survey was designed as a between-subjects study, with one group of participants being shown only scenarios that involve the use of cloud-based TEE-enabled sensing platforms (i.e., with TEE), and the other group being shown only scenarios that involve the use of cloud-based commodity (i.e., without TEE) sensing platforms. The survey considered scenarios in which data was sent to a cloud-based infrastructure for processing and feedback. We considered cloud-based architecture as they are commonly used in smart home applications, particularly where device integration is concerned [7, 26, 49]. Potential limitations of this design choice are discussed in Section 6. The survey itself consisted of four sections: consent and overview, an informational video, questions on acceptance of information flows, and post-completion demographic questions.

3.2.1 CONSENT AND OVERVIEW. Initially, we presented the participants with a consent form approved by our organization's IRB. If the participants did not consent, they were not allowed to participate further in the study. Participants were then shown the survey overview depicted in Appendix F.1, which contains a brief overview of concepts related to IoT devices, device ownership, and differentiation between small and established companies.

3.2.2 INFORMATIVE VIDEO. For participants in our baseline (without TEE) group, we prepared a short video exploring a sensing/sharing

scenario in the context of a commodity (without TEE) sensor. The video explores a scenario in which a connected camera uses a cloud-based facial recognition service to automatically unlock the door of a smart home. The scenario starts with the collection of data by an on-premises camera and communication to the remote receiver's cloud. The remote receiver maintains a cloud database of authorized faces. Based on the outcomes of the face recognition algorithm being executed on the remote receiver's processor, an actuation command is sent to the smart home's door. To ensure that we did not influence individual perceptions of IoT technologies in this baseline condition, we followed the practice of prior work [8, 9] and described the data items flowing between entities, but did not address specific threats to data security in-flight or at-rest.

For participants in the TEE group, we prepared an analogous short video that provided a brief overview of TEE functionality and a sensing/sharing scenario in the context of a cloud-based TEE-enabled sensor. In addition to the content in the 'without TEE' video, we showcased the cloud-based TEE model for the same example. Specifically, we first covered the topic of remote attestation in TEE infrastructures, where the clients could identify the functionalities used by the cloud service and the establishment of a secure channel to send the sensed data (i.e., camera frames). Secondly, we showed how the data sent to a face recognition algorithm is protected from other processes demonstrating the isolated execution of TEE. And at last, the concept of sealed storage was introduced to showcase one way that databases can be securely stored and maintained in the cloud. After this video, participants in the TEE group were presented a brief true/false questionnaire exploring their understanding of basic cloud-based TEE functionality.

3.2.3 CONTEXTUAL INTEGRITY QUESTIONS. The main section of our survey presented questions about the acceptability of information flows derived from the collection of contextual integrity parameters outlined above. To limit the number of questions asked of any one participant, the sender (i.e., smart camera or smart speaker), company (i.e., large or small), and subject (i.e., the owner or other occupants within the space) were chosen randomly on a per-participant basis and did not vary during the course of the survey. The remaining contextual integrity parameters were then varied over eight questions (1 null + 7 non-null transmission principles) for each of the recipient, leading to investigation of 48 transmission flows, i.e., ((1 null + 7 non-null transmission principles) × 6 recipients) per participants.

As shown in Figure 1a, we first presented a question matrix with information flows corresponding to data being transmitted to each of the six recipients with an unspecified (null) transmission principle. Each of the remaining six questions focused on a single recipient and explored each transmission principle identified above (cf. Figure 1b). All question matrices used a 5-Point Likert Scale: (2) Extremely acceptable, (1) Somewhat acceptable, (0) Neutral, (-1) Somewhat unacceptable, (-2) Extremely unacceptable. Our survey also included two randomly-inserted attention-check response matrices.

3.2.4 IUIPC AND DEMOGRAPHICS. The final section of the survey contained the Internet Users' Information Privacy Concerns (IUIPC) scale, as well as a series of demographic questions. We

2. A **smart camera** from **small company** records **video** of **you** in your smart home. In your opinion as the device owner, how acceptable is it for the smart camera to send video of you to the following types of **recipients when data processing occurs within a Trusted Execution Environment (TEE)**?

| | Extremely unacceptable | Somewhat unacceptable | Neutral | Somewhat acceptable | Extremely acceptable |
|---|---|---|---|---|---|
| Law enforcement with TEE | ○ | ○ | ○ | ○ | ○ |
| Device manufacturer with TEE | ○ | ○ | ○ | ○ | ○ |
| Other smart home devices at place with TEE | ○ | ○ | ○ | ○ | ○ |
| Recommendation services with TEE | ○ | ○ | ○ | ○ | ○ |
| Health services with TEE | ○ | ○ | ○ | ○ | ○ |
| Family members/ friends with TEE | ○ | ○ | ○ | ○ | ○ |

(a) Null transmission question

3.1. A **smart camera** from **small company** records **video** of **you** in your smart home. In your opinion as the device owner, how acceptable is for the smart camera to send video of you to **Law enforcement** under the following circumstances and when data processing occurs **within a Trusted Execution Environment(TEE)** for investigation into a reported crime?

| | Extremely unacceptable | Somewhat unacceptable | Neutral | Somewhat acceptable | Extremely acceptable |
|---|---|---|---|---|---|
| if you have given consent | ○ | ○ | ○ | ○ | ○ |
| if you are notified | ○ | ○ | ○ | ○ | ○ |
| if information used for maintenance of device/ feature | ○ | ○ | ○ | ○ | ○ |
| if information is not stored | ○ | ○ | ○ | ○ | ○ |
| if information is stored for duration on 1-3 months | ○ | ○ | ○ | ○ | ○ |
| if information is stored indefinitely | ○ | ○ | ○ | ○ | ○ |
| if privacy policy mentions the Law enforcement and the purpose of sharing | ○ | ○ | ○ | ○ | ○ |

(b) Varying recipients with transmission principles question

Figure 1: Example of matrix question presented to participants. Each participant saw the null transmission question Figure 1a. Later on each participant saw the varying recipient questions with transmission flows 1b.

report demographic percentages and IUIPC scores in the Appendix D and E. Our responses were nearly equally divided between male and female users, reflecting expected trends [45]. Furthermore, 15% of our participants have not owned or used IoT devices and it corroborates with the trends reported in April 2022 in Statista [5].

| Subject | Vendor | Sender | Without TEE | With TEE |
|---|---|---|---|---|
| You | Small Company | Smart Speaker | 63 | 60 |
| You | Small Company | Smart Camera | 73 | 60 |
| You | Established Company | Smart Speaker | 64 | 61 |
| You | Established Company | Smart Camera | 68 | 75 |
| Other Occupants | Small Company | Smart Speaker | 63 | 67 |
| Other Occupants | Small Company | Smart Camera | 79 | 77 |
| Other Occupants | Established Company | Smart Speaker | 69 | 61 |
| Other Occupants | Established Company | Smart Camera | 60 | 49 |
| Total | | | 539 | 510 |

Table 1: Participants distribution after filtering.

## 3.3 SURVEY DEPLOYMENT

We created our survey using Qualtrics platform [44], and our institution's IRB approved our survey content and recruitment process of participants. We recruited participants from Amazon Mechanical Turk (Mturk) [57]. Only the workers who met the requirements of 95% and above HIT rating, age 18 years and above, and residence in the US were selected to participate in the survey. Respondents were compensated with a $1 payment upon completion of the survey, which took 8 minutes on average. Overall, we collected 1091 unique responses to our survey.

## 3.4 RESPONSE ANALYSIS

We first removed 42 participant responses that had incorrect answers for the attention check questions. This left 1049 unique responses, and each participant gave seven responses for transmission flows. We had 510 and 539 participants in 'with TEE' and 'without TEE' groups, respectively. The distribution of participants between groups and scenarios is shown in Table 1. In total, each participant answered questions about 48 transmission flows.

3.4.1 AVERAGE ACCEPTABILITY SCORES. In our survey, each participant responded to questions about information flows for all the recipients. To observe the trends in comfort for each recipient, we averaged the acceptability scores of flows categorized by the CI parameters of the group, the sender, the manufacturing company, and the subject across null and non-null transmission principles. For example, we averaged the acceptability scores for each transmission principle by recipient (e.g., law enforcement) and parameters (e.g., group: without TEE, subject: you, manufacturing company: small company, sender: smart speaker). To easily visualize the average scores, we have plotted heatmaps for recipients with and without TEE in the form of CI parameters (the sender, manufacturing company, the subject) by transmission principles.

3.4.2 SIGNIFICANCE TEST. We divided the information flows based on sets of pairs (sender, manufacturing company, and subject) that are independent. It allows us perform a non-parametric Wilcoxon signed-rank test to measure the effect of non-null transmission principles. To study the impact of presenting the non-null transmission principle, we compare the average acceptability scores between pairs of information flows with the null transmission principle and the non-null transmission principle having the same sender, manufacturing company, and subject. For example, we compared averaged scores for a set of pairs (smart speaker, established company, and you) for Law Enforcement's non-null transmission principle "if you have given consent" against the average scores of Law Enforcement's null transmission principle. We performed 42 tests for finding the significant non-null transmission principles for all recipients and set the threshold for significance to $\alpha = 0.05/42 \approx 0.001$ to account for the Bonferroni multiple-testing correction [60].

3.4.3 INDEPENDENCE TEST. In the survey, the information flows utilize the parameters of the sender, manufacturing company, and subject. Each of these parameters had two variables, and we wanted to measure the effect of these variables on the parameter across all non-null transmission principles and recipients. To study the influence of variables on the individual parameter with the comfort measured for non-null transmission principles and recipients, we performed a Mann-Whitney U Test within each group. The test finds the likelihood of having one distribution of the average acceptance scores being stochastically greater than the second. For example, the sender has two variables smart speaker and a smart camera. The test will determine the distribution of comfort measured for a non-null transmission principle "if you have notified" is the same across the smart speaker and smart camera.

3.4.4 INDEPENDENCE TEST - TEE UNDERSTANDING. Our survey enquired about the understanding of TEE after the informative video. It led to three groups Answered Correct (correct responses to all three questions), Answered Wrong (one or more incorrect responses), and Combine (responses to TEE questions not considered). As we had more than one group and the comfort was the measure of the average acceptance scores of the transmission principles and recipients, we performed the Kruskal-Wallis test. The test finds the likelihood of having at least one stochastically dominant group.

For all of the independence tests mentioned, we performed 13 comparisons (six recipients and seven non-null transmission principles). We accounted for the corrected p-value using Bonferroni correction $\alpha = 0.05/13 \approx 0.004$ [60].

# 4 RESULTS

Our analysis of the survey responses provides insights into how TEE's may influence privacy norms in smart home scenarios. In this section, we describe results from our analysis procedures described in Section 3.4.

## 4.1 INFLUENCE OF TEES ACROSS MULTI-FACETED INFORMATION FLOWS

We first sought to explore the influence of TEE in information flows with transmission principles across every combination of sender, manufacturing company, and subject. To evaluate this, we calculated the average acceptability scores for all recipients as discussed in Section 3.4.1. We visualized average acceptability scores as heatmaps, e.g., as shown in Figure 2. Overall, we observed higher comfort (i.e., darker shading) in scenarios involving a TEE. This phenomenon was particularly pronounced in the context of the "if you have given consent" transmission principle. Across the board, the "information is stored indefinitely" transmission principle exhibits the lowest comfort across both TEE and without TEE scenarios.

We observed the highest variation in average acceptance scores for the Law Enforcement recipient scenarios (cf. Figure 2), with the

TEE scenarios exhibiting markedly higher comfort levels than the without TEE scenarios. This trend is even reflected in the context of the "null" transmission principle, which does not specify constraints on consent, data use, or data retention. By contrast, the lowest variation in average acceptance scores occurred in scenarios involving Other Devices within the space (cf. Figure 8 in Appendix C). This is likely resulting from device owners holding a baseline level of trust in the devices that they purchase and deploy within their homes.

All other scenarios exhibited variations on the spectrum between the extremes of Law Enforcement and Other Devices. Across each scenario and transmission principle, we observed that TEE cases registered higher average comfort scores than the without TEE cases. The notable exception is the "information is stored indefinitely" transmission principle, which remained consistent across the TEE and without TEE use cases.

## 4.2 INFLUENCE OF TEE ON COMFORT WITH TRANSMISSION PRINCIPLES ACROSS SCENARIOS

We evaluate the effect of the non-null transmission principles in the information flows. We utilize user comfort as a function of transmission principle, as shown in Figure 2. We carried out a within-subject analysis and used the Wilcoxon Signed Ranked Test, as described in Section 3.4.2 to compare the change in effect for the non-null transmission principles from null transmission principle within each group. In the case of without TEE information flows, we found significant differences across pairs of average acceptance scores between null and non-null transmission principles, and we have reported them in Table 6 of Appendix A. For each pair of significant difference observed, we calculated the percentage change using the average scores of respective pair of recipient's null transmission principle and non-null transmission principles.

To easily display the change in percentage from the null transmission principles, we have plotted a percentage bar graph (cf. Figure 3). The percentage indicates the aggregate difference across all relevant scenarios where we observed significant differences. For example, the transmission principle "if you are notified" vs null transmission principle, in without TEE case, we saw differences of 9.42% for the Law Enforcement recipient, 7.05% for the Device Manufacturer recipient, 17.22% for the Health Services recipient and 8.61% for the Family Members/Friends recipient, the sum of which is 42.3%. We followed the same procedure to calculate the percentage change for the pairs of significant differences observed in with TEE information flows.

We observe that the transmission principle "if you have given consent" changes from the null transmission principle for both with TEE and without TEE information flows in nearly the same way. As we observe the percentage change for information flows without TEE is 71.6% and for with TEE is 71.5%. We observe the transmis-sion principle "if you are notified" provides a higher comfort for information flows without TEE, as the percentage change is 42.3%. In comparison, we observe that the information flows with TEE alter the comfort by only 17.27%. It showcases the transmission principle "if you are notified" provides higher comfort in without TEE information flows. The participants with TEE have a higher comfort in information flows using the null transmission principle and that results in lower change in comfort for the "if you are notified" transmission principle. For the transmission principle "if information is used for maintenance of device/feature", we observe the percentage change for information flows without TEE is 37.03% and with TEE is 30.48%. The participants with TEE already have a higher comfort in information flows using the null transmission principle and we again observer smaller alteration of comfort. In case, of transmission principles describing the data retention policies "if information is not stored" and "if information is stored for 1-3 months" we observe the information flows with TEE have higher comfort. We observe a significantly lower acceptance for transmission principle "if information is stored indefinitely." Under both information flows with TEE has a change of -70.1% and without TEE has change of -47.12%. Again with TEE the information flows for the null transmission principle is higher but the acceptance scores for indefinite storage is in the similar range of with that of without TEE information flows. Lastly, we observe the similar change in comfort for the transmission principle "if privacy policy mentions recipient and the purpose of sharing." The change is 52.16% for without TEE information flows and the change is 56.5% for with TEE information flows.

## 4.3 INFLUENCE OF TEES ON TRUST IN DEVICE'S MANUFACTURING COMPANY

Here we seek to explore whether presence of a TEE significantly impacts user comfort with information flows in smart home scenarios. More specifically, we investigate user comfort as a function of data recipient (averaged over all transmission principles), as well as comfort as a function of transmission principle (averaged over all recipients). In both cases, we carried out a within-subjects analysis split between information flows transmitted by a device manufactured by a small company vs. an established company. To conduct our analysis, we used the Mann-Whitney U test, as described in Section 3.4.3.

In the case of without TEE information flows, 278 participants answered questions about information flows transmitted by devices manufactured by small companies vs. 261 participants for devices manufactured by established companies. We found significant differences in comfort as described in Table 2. Specifically, we observed a significant difference in the transmission principle "if information is stored indefinitely" with a $\square - \square \square \square$ of 0.003. Additionally, we have plotted a percent sum graph to observe the distribution of the scores between the small and established companies (cf. Figure 4a), where we also see the mean rank for the distribution for a devices manufactured by established companies is higher (284.98) than for small companies (255.94). Similarly, we saw significant differences in comfort for the recipients Law Enforcement ($\square - \square \square \square$ of 0.0035) and Health Services ($\square - \square \square \square$ of 0.0041). In comparison to the small companies, the spread and average acceptance scores were higher for the established companies in each of the significant differences observed. We did not observe any significant differences for other transmission principles or recipients in the without TEE group.

The TEE group had 264 participants answered questions about information flows transmitted by devices manufactured by small

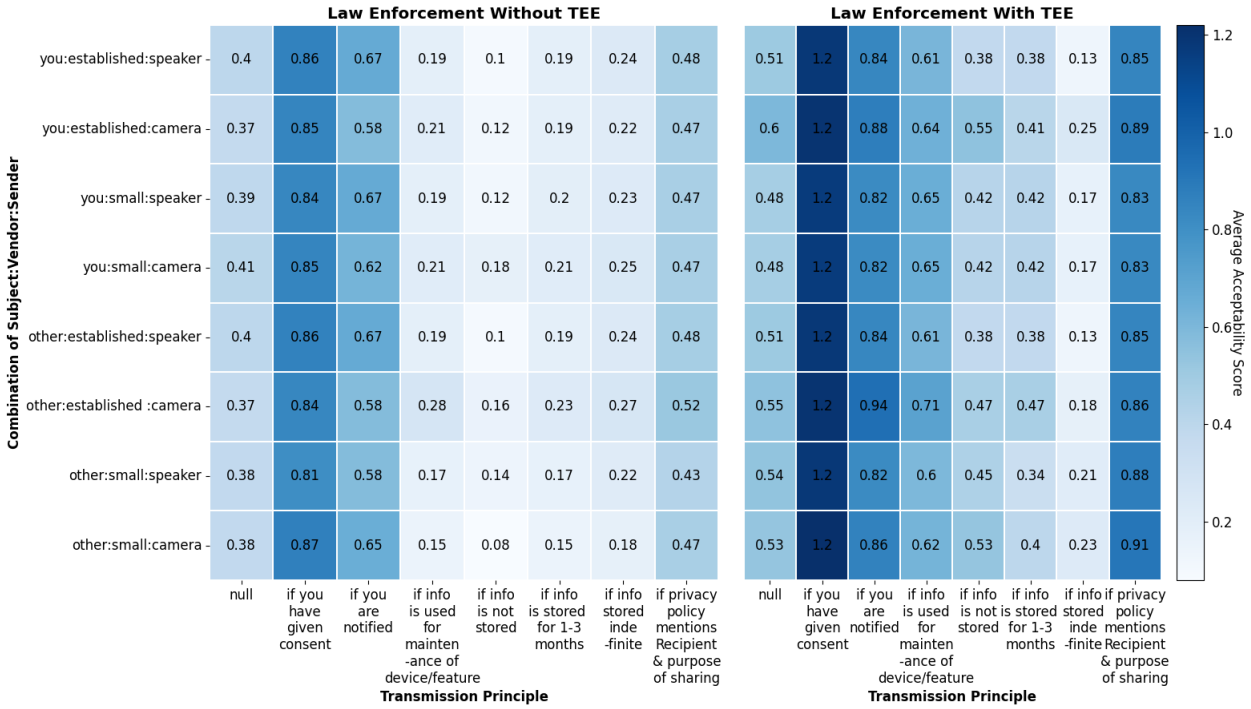



Figure 2: Law Enforcement's Average Acceptability of information flows grouped by without TEE on left and with TEE on right.

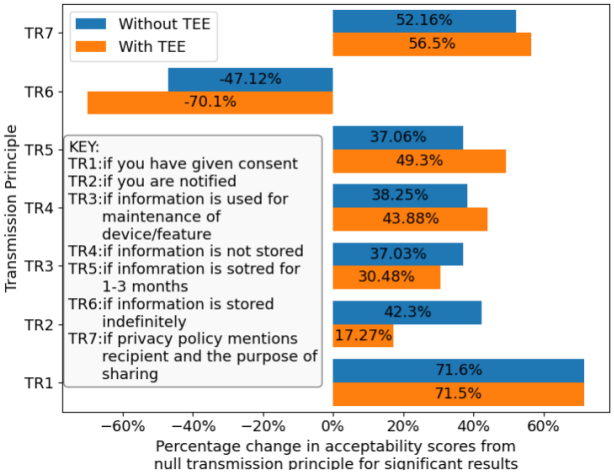



Figure 3: The percentage change where the inclusion of a specific transmission principle resulted in statistically significant difference.

companies vs. 246 participants for devices manufactured by established companies. In contrast to the without TEE case, we did not see any significant differences in user comfort with information flows as a function of either recipient or transmission principle between the small company and established company device groups.

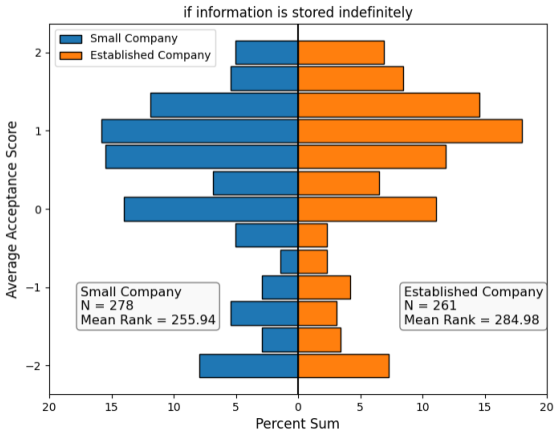
| Transmission Principle | Without TEE | | With TEE | |
|---|---|---|---|---|
| if information is stored indefinitely | 32369.5 | 0.0030* | 29282.0 | .055 |
| Recipient | Without TEE | | With TEE | |
| Law Enforcement | 32486.5 | 0.0035* | 32395.0 | 0.138 |
| Health Services | 32600.0 | 0.0041* | 30008.5 | |

Table 2: Mann Whitney's U test for manufacturing company's effect on transmission principles and recipients for both groups with and without TEE. Reporting values for significant differences. * stands for $\square \leq 0.004$ and shows significance.

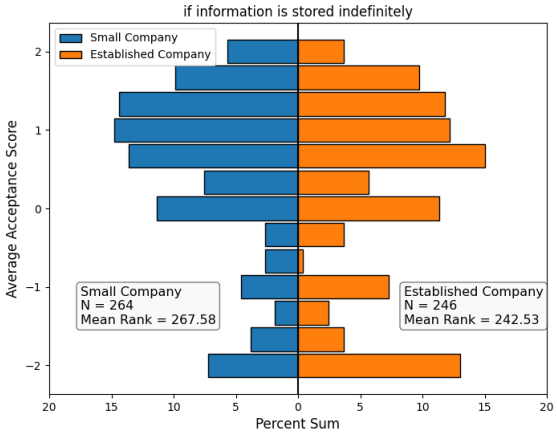
This is reflected in Figures 4b ("if information stored indefinitely"). The spread and average acceptance scores were nearly the same between small and established companies for all transmission principles and recipients.

## 4.4 IMPACT OF TEES ON COMFORT RATINGS BY THE DEVICE TYPE

The survey had two types of devices, smart speaker and smart camera, and we were interested in examining the changes for users' comfort in the smart home information flows based on device sensing. Similar to Section 4.3, we investigate user comfort as a function of data recipient, as well as comfort as a function of transmission principle. In both cases, we carried out a within-subject analysis split between information flows transmitted by a smart speaker




(a) Without TEE




(b) With TEE

Figure 4: Distribution of average acceptance scores as a percent sum graph between small company and established company for the transmission principle "if information is stored indefinitely". In Figure 4a, the information flow without TEE shows the distribution of scores is inclined towards established company and in Figure 4b the distribution of scores are nearly the same between device's manufacturing company when the information flow involves a TEE.

| Transmission Principle | Without TEE | | With TEE | |
|---|---|---|---|---|
| if information is used for maintenance of device/feature | 31270.5 | 0.0039* | 34812.5 | 0.163 |
| if policy mentions the {recipient} and the purpose of sharing | 31965.0 | 0.0017* | 33860.0 | 0.411 |
| Recipient | Without TEE | | With TEE | |
| Law Enforcement | 32207.5 | 0.0024* | 34602.0 | 0.204 |
| Device Manufacturer | 32333.0 | 0.0029* | 32405.0 | 0.957 |
| Other Devices at Place | 29978.0 | 0.0031* | 33915.5 | 0.392 |
| Recommendation Services | 32180.5 | 0.0024* | 32924.0 | 0.796 |

Table 3: Mann Whitney's U test for sender effect for transmission principles and recipients for both groups with and without TEE. Reporting values for significant differences. * stands for $\alpha \leq 0.004$ and shows significance.

(audio) vs. smart camera (video). To conduct our analysis, we again used the Mann-Whitney U test, as described in Section 3.4.3.

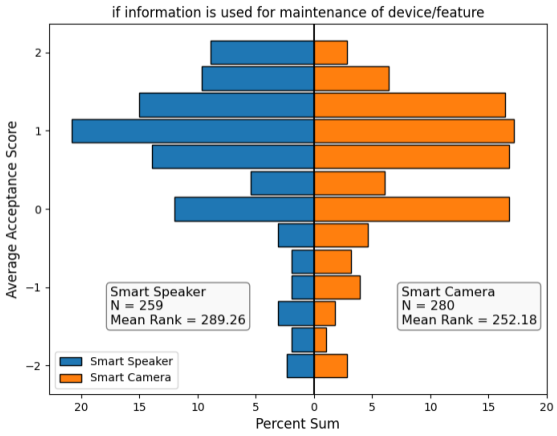
In case of without TEE information flows, 259 participants answered questions about information flows transmitted by smart speaker vs. 280 participants for smart camera. We found significant differences in comfort as described in Table 3. Specifically, we observed a significant difference in transmission principles "if information used for maintenance of device/feature" with a $\alpha$-value of 0.0039. Additionally, we have plotted a percent sum graph to observe the distribution of the scores between smart speaker and smart camera (cf. Figure 5a), where we also see the mean rank for the distribution for a smart speaker is higher (289.26) than for a smart camera (252.18). Similarly, we saw significant differences in comfort for transmission principle "if privacy policy mentions the recipient and the purpose of sharing" ($\alpha$-value of 0.0017) and for the recipients Law Enforcement ($\alpha$-value of 0.0024), Device Manufacturers ($\alpha$-value of 0.0029), Other Devices at Place ($\alpha$-value of 0.0031) and Recommendation Services ($\alpha$-value of 0.0024). In comparison to the smart camera, the spread and average acceptance scores were higher for the smart speaker in each of the significant differences observed. We did not observe any significant differences for other transmission principles or recipients in without TEE group.

The TEE group had 249 participants answered questions about information flows transmitted by smart speaker vs. 261 participants for smart camera. In contrast to the without TEE case, we did not see any significant differences for user comfort with information flows as a function of sensor type either for a recipient or for a transmission principle. This is reflected in Figures 5b ("if information used for maintenance of device/feature") for with TEE. The spread and average acceptance scores were nearly the same between smart speaker and smart camera for all transmission principles and recipients.

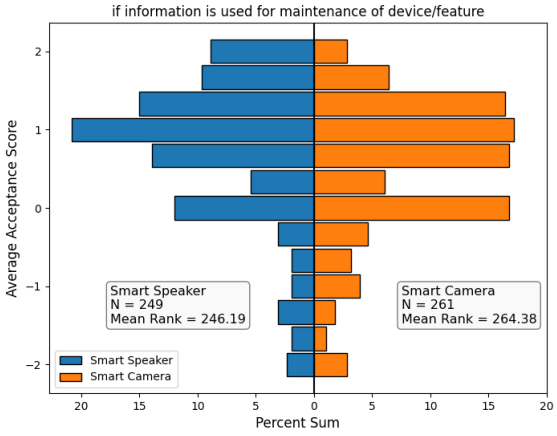
## 4.5 INFLUENCE OF TEES ON COMFORT WITH INFORMATION FLOWS BY SUBJECT OF DATA

In this section, we explore whether presence of TEE significantly influences user comfort with smart home scenarios based upon subject of sensing. Similar to Section 4.3, we investigate user comfort as a function of data recipient, as well as comfort as function of transmission principle. In both cases, we carried out a between-subject analysis split between information flows where the subject of sensing is the device owner in the smart home without TEE vs. the smart home with TEE. To conduct our analysis, we again used the Mann-Whitney U test, as described in Section 3.4.3.

In the case of subject of sensing being the device owner, 268 participants answered questions about information flows without TEE vs. 256 participants for with TEE information flows. We did not observe any significant differences in the user's comfort for all




(a) Without TEE




(b) With TEE

Figure 5: Distribution of average acceptance scores as a percent sum graph between smart speaker and smart camera for transmission principles "if information used for maintenance of device/feature". In Figure 5a we observe the distribution of average scores more inclined towards smart speaker. In Figure 5b the distribution of the scores increases for smart camera under TEE.

transmission principles and recipients. The device owner's spread and the average acceptance scores were nearly the same between those without TEE and with TEE information flows. Similarly, we carried out another between-subject analysis split between information flows where the subject of sensing is other occupants. In the other occupants' group, 271 participants answered questions about information flows without TEE vs. 254 participants answered questions about information flows with TEE information flows. We did not observe any significant differences in the user's comfort for all transmission principles and recipients. The other occupants' spread and the average acceptance scores were nearly the same between those without TEE and with TEE information flows.

We additionally, performed a within-subject analysis split between information flows where the subject of sensing in the smart home is the device owner vs. other occupants. In the case of without TEE information flows, we observed significant differences across all transmission principles and recipients. Similarly with TEE information flows, we observed significant differences across all transmission principles and recipients. In comparison to other occupants, the spread and the average acceptance scores were higher for device owners for all of the transmission principles and recipients for both cases without and with TEE information flows. And this corroborates the results shown in the prior work [4, 24, 55, 63], showing the complexity of bystander privacy that involves the perceived trust, the relationship between the device owner and other occupants, and the devices' purpose in the shared space. We have reported the test scores for both analysis in Appendix B.

## 4.6 EFFECT OF UNDERSTANDING TEE CONCEPTS CORRECTLY ON SMART HOME INFORMATION FLOWS

We surveyed participants with TEE group about their correct understanding of TEE concepts of secure storage, secure computing, and remote attestation. There were three questions with binary choices and answering all three questions right entailed that the participant understood the TEE concept correctly. We explore whether a correct understanding of TEE concepts influences user comfort with information flows in smart home scenarios. Similar to Sec-tion 4.3, we investigate user comfort as a function of data recipient and transmission principle. We carried out analysis split between information flows transmitted by Answered Correct (respondents answering correctly to all three questions on the concepts of TEE after informative video), Answered Wrong (respondents answering one or more questions wrong for the questions after informative video), and Combined (responses to TEE questions not considered). To conduct our analysis we used the Kruskal Wallis independence test described in Section 3.4.4.

We had 202 participants in Answered Correct, 308 participants in Answered Wrong, and Combine had 510 participants. We found significant differences in comfort as described in Table 4. We observed significant differences in all transmission principles and recipients between all the comparisons. For instance, we found significant difference for transmission principle "if you are notified" with a □– □ □ □ of 0.004. Additionally, we have plotted box plot to ob-

serve the distribution of scores between Answered Correct, Answered Wrong, and Combined (cf. Figure 6), where we also see the average acceptance scores were lower for a Answered Wrong (median below 1) than for Answered Correct (median above 1) with the average acceptance scores being higher. The average acceptance scores for the Combine was lower compared to Answered Correct.

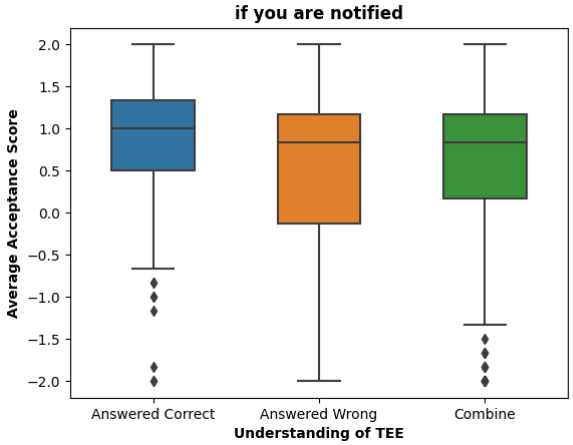



Figure 6: Distribution of average acceptance scores between three groups Answered Correct, Answered Wrong and Combine for "if you are notified" transmission principle.

| Transmission Principles | | | | |
|---|---|---|---|---|
| if you have given consent | | | 46.239 | 2 |
| if you are notified | | | 0.001[2] | |
| if information is used for maintenance of device/feature | 10.199 | 2 | 0.004[2] | |
| if information is not stored | 28.385 | 2 | 0.001[2] | |
| if information is stored for duration of 1-3 months | 53.316 | 2 | 0.001[2] | |
| if information is stored indefinitely | 102.689 | 2 | 0.0001[2] | |
| if privacy policy mentions {recipient} and purpose of sharing | 154.441 | 2 | 0.0001[2] | |
| | 31.451 | 2 | 0.001[2] | |
| Recipients | | | | |
| Law Enforcement | | | 30.191 | 2 |
| Device Manufacturer | | | 0.001[2] | |
| Other Devices at Place | 48.913 | 2 | 0.001[2] | |
| Recommendation Services | 50.035 | 2 | 0.001[2] | |
| Health Services | | 92.295 | 2 | 0.0001[2] |
| Family Members/ Friends | | 40.993 | 2 | 0.001[2] |
| | | 49.828 | 2 | 0.001[2] |

Table 4: Kruskal Wallis test for effect of understanding TEE concept correctly. The table includes Chi value □, Degree of Freedom □ □,and □− □ □ □. Reporting values for significant differences. [2] stands for □≤ 0.004 and shows significance.

## 4.7 EFFECT OF IOT DEVICE USAGE EXPERIENCE ON TRANSMISSION PRINCIPLES AND RECIPIENTS

We compared the effect on comfort for having TEE in information flows between the respondents who self-reported they have prior experience on usage of IoT devices (users) and the respondents who have no prior experience on usage of IoT devices (nonusers). Similar to Section 4.3, we investigate user comfort as a function of data recipient, as well as comfort as a function of transmission principle. In both cases, we carried out a within-subject split between information flows transmitted by a user vs. nonuser. To conduct our analysis, we again used the Mann-Whitney U test, as described in Section 3.4.3.

In case of without TEE information flows, 464 participants answered for having a prior experience with an IoT device vs. 75 participants having none. We observed significant differences for all transmission principles and recipients for comfort as described

| Transmission Principle | Without TEE | | With TEE | |
|---|---|---|---|---|
| | □− □ □□ □□□− | | □− □ □□ □ □□□− | |
| if you have given consent | □ □ □16623.5 | | □ □ □12937.5 | |
| if you are notified | 0.0001[2] 23469.0 | | 0.0002[2] 23512.5 | |
| if information is used for maintenance of device | 0.0001[2] | | 0.0001[2] | |
| if information is not stored | 25448.5 | 0.0001[2] | 24552.0 | 0.0001[2] |
| if information is stored for duration of 1-3 months | 22383.0 | 0.0001[2] | 23546.0 | 0.0001[2] |
| if information is stored indefinitely | 26090.0 | 0.0001[2] | 27048.0 | 0.0001[2] |
| if policy mentions {recipient} and the purpose of sharing | 27233.0 | 0.0001[2] | 28466.0 | 0.0001[2] |
| Recipient | 25600.0 | 0.0001[2] | 24667.5 | 0.0001[2] |
| | Without TEE | | With TEE | |
| | □− □ □□ □□□− | | □− □ □□ □ □□□− | |
| Law Enforcement | □ □ □24514.5 | | □ □ □24011.5 | |
| Device Manufacturer | 0.0001[2] 24321.0 | | 0.002[2] 24211.5 | |
| Other Devices at Place | 0.0001[2] 22422.5 | | 0.0001[2] 24543.0 | |
| Recommendation Services | 0.0001[2] 25857.0 | | 0.0001[2] 26611.0 | |
| Health Services | 0.0001[2] 24336.5 | | 0.0001[2] 23895.0 | |
| Family Members/ Friends | 0.0001[2] 24691.5 | | 0.0001[2] 25319.5 | |
| | 0.0001[2] | | 0.0001[2] | |

Table 5: Mann Whitney's U test for IoT Device experience effect for transmission principles and recipients for both groups with and without TEE. Reporting values for significant differences. [2] stands for □≤ 0.004.

in Table 5. For instance, we found significant difference for transmission principle "if information is stored indefinitely" with a □− □ □ □ □ □ of 0.0001. Additionally, we have plotted the percent sum graph between the users and nonusers (cf. Figure 7a), where we also observe the mean rank for prior experienced device users is higher (284.98) than for nonusers (255.94). Overall, we always observed the users are more comfortable in sharing their information for all of the 7 transmission principles and 6 recipients.

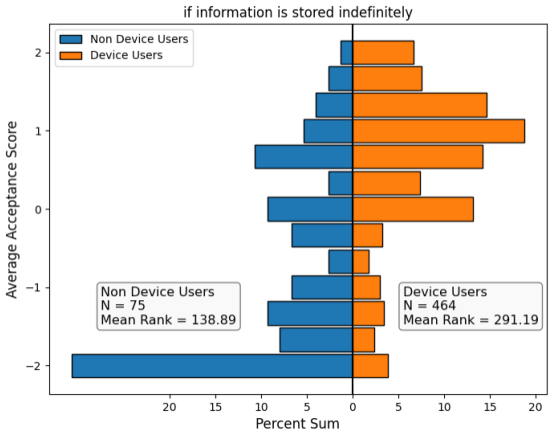
The TEE group had 428 participants answered questions about having prior experience with an IoT device vs. 82 participants having none. Similar to TEE, we observed significant differences for all transmission principles and recipients. Additionally, we observed the user comfort was higher for users having prior experience compared to nonusers. This is reflected in Figure 7b for "if information is stored indefinitely."

# 5 DISCUSSION

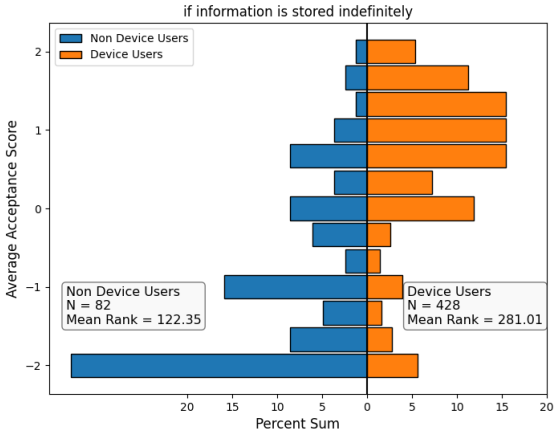
We analyze our survey responses to find insights into IoT privacy norms under TEE in the smart home context. The following discussions incorporate our findings into design implications on the usage of TEE for IoT device manufacturers, policymakers, and regulators.

## 5.1 TEES CAN HELP LEVEL THE PLAYING FIELD BETWEEN SMALL AND ESTABLISHED COMPANIES

Prior literature has shown that users are more likely to trust IoT and other devices manufactured by established companies such as Amazon, Apple, or Google [40, 58]. Interestingly, our results in Section 4.3 show that the inclusion of a TEE in devices manufactured by small companies closed this gap and led to average user acceptance scores that were on par with those for more established companies (cf. Figure 4). This provides a pathway for smaller companies to articulate a value proposition that is meaningful to potential users,




(a) Without TEE




(b) With TEE

Figure 7: Distribution of average acceptance scores as a percent sum graph between nonusers and users for transmission principles if information is stored indefinitely. The IoT device users were more comfortable in sharing the information irrespective with or without TEE seen in Figure 7a and Figure 7b.

and perhaps can pave the way to growing market share for these manufacturing companies.

At a minimum, this would offer a wider array of device options for users without requiring users to lower their standards as they related to fear of data breaches or other security issues [11, 28, 33, 35, 54], and will allow users to make purchase choices based upon features afforded by the device regardless of whether the device was manufactured by a small or established companies. In the best case, increased uptake of TEE-enabled devices manufactured by smaller company could help create a competitive marketplace that incentivizes all manufacturing companies to prioritize data protection as a first-order priority.

## 5.2 FEWER NOTIFICATIONS ARE REQUIRED

Smart home app developers, device manufacturers, and service providers often push numerous notifications to the end user, often as reminders of data collection practices or events detected. Users do not typically change the device settings after initial installation and configuration and tend to ignore most of the notifications, which results in lower usability [59] and notification saturation for the user [30]. Additionally, recent work has shown that users who are highly concerned about their data, express a desire for additional push notifications providing information about how their data is being used and stored [21].

As observed in Section 4.2 with TEE, there was a 17.27% change in average acceptance scores for the non-null transmission principle "if you are notified." This indicates that notifications played a less significant role in acceptance in TEE-enabled data-sharing scenarios, which presents an opportunity to reduce their use in the smart home environment.

Decreasing the number of notifications experienced by a given user may help reduce notification fatigue, and enable vendors to interact with users more substantively via the notifications that do get sent. This may lead to increased awareness of device activities and engagement in a smart home.

## 5.3 TEES IMPACT FIXED-DURATION DATA RETENTION CONCERNS

Sections 4.1 and 4.2 indicate that the presence of a TEE in smart home devices increases user acceptance of information retention for fixed periods of time (e.g., 1–3 months) as compared to scenarios without a TEE. Given that the features of most smart home devices are based upon fixed usage of data (e.g., responding to verbal commands, detecting events in a video stream), the inclusion of a TEE that enforces these retention constraints may lead to an increase of device adoption by users who would otherwise be skeptical of the data collection practices of a manufacturing company. The findings indicate that device manufacturers and service providers remain transparent with their data retention practices, and support emerging regulatory frameworks that place purpose- and retention-based limits on the use of personal information [12, 15].

## 5.4 USERS NO LONGER DIFFERENTIATE BETWEEN AUDIO AND VIDEO DATA UNDER TEES

In Section 4.4, we observed that in information flows without TEEs, users indicated a higher average acceptance for audio as compared to video data. Prior work [39, 65] has shown similar findings. Interestingly, in information flows with TEEs, we observed an increase in average acceptance for sharing video data that was nearly at the same level as for audio data. This indicates that differences in user acceptance as a function of sensor modality may level out in the presence of TEEs. This is of particular importance as de-vices incorporate larger collections of sensors, e.g., as in the case of general-purpose sensing infrastructures [36].

### 5.5 UNDERSTANDING OF TEE IMPROVES THE ACCEPTANCE OF INFORMATION FLOWS

Our survey analysis in Section 4.6 showcased that users who correctly answered questions about TEE functionality expressed a higher degree of comfort in sharing data across all transmission principles. The average acceptance scores were higher in participants understanding TEE correctly for consent, purpose, notifications, and data retention principles (cf. Figure 6), except for indefinite storage. It showed us that the participants with correct understanding are more likely to share the information for all the principles except for indefinite storage.

Prior work shows that new technologies take time to adapt as users are reluctant to adapt [23, 37], and IoT devices are in their nascent stage. In [64], the authors discuss the user's mental model of IoT devices' security risks and privacy concerns due to a lack of awareness. The authors recommend providing more information to the users about IoT devices working. It supports our findings that a better understanding of TEE will influence the privacy choices made under TEE, similar to threat models understood by the user after receiving more information. Device manufacturers, service providers, or policymakers cannot just assume by stating the usage of secure technologies users are willing to share more.

### 5.6 CENTRALITY OF FEW PRIVACY NORMS REMAINS UNCHANGED WITH TEES

The concept of consent has a pivotal role in data-sharing privacy norms, and prior studies have established it by showing the higher comfort of the participants in sharing the information after consent [8, 9, 17, 39, 65]. Our survey illustrated the acceptance scores were higher for both groups with and without TEE for the transmission principle "if you have given consent" in Section 4.2. Similarly, we did not see any significant change in user acceptance in scenarios that involved indefinite data collection, regardless of whether a TEE was present in the smart home device. This aligns with previous studies [8, 9, 39, 65] in which users disliked indefinite data sharing and indicates the centrality of retention in shaping information-sharing norms, again shown in Section 4.2.

Furthermore, we did not observe any significant change in user acceptance in scenarios that involved other people as the subject of sensing in the smart home for having TEE in the information flows. It coincides with the previous work where authors often suggest a bystander is a complex problem of the relationship between owners and individuals and the devices' purpose in a shared space [4, 24, 55, 63]. Additionally, users' prior experience with devices impacts the acceptance of sharing the information across all of the privacy norms, as seen in Section 4.7 (cf. Figure 7). Similar results were observed in [8], where users were more comfortable in sharing the information compared to nonusers. But compared to prior work [8] we had fewer nonusers, it illustrates the nonusers seen here are lagging in adoption, and as per [48], these are nonusers who haven't used the technology yet.

The device manufacturers, service providers, and policymakers should note that indefinite time storage of information, consent, bystander privacy, and device experience issues cannot be solved with the induction of secure technologies like TEE. The fundamentals of digital privacy norms for indefinite time storage and obtaining consent play an important role in user comfort and are unlikely to be overcome through the introduction of new hardware alone. Bystander privacy and device usage experience is a complex problem that requires a longitudinal study with the contextualization of space, social status/dynamics, and purpose. Furthermore, there may be an alteration in privacy norms after the adoption of devices by nonusers. The device manufacturers, service providers, and policymakers need to understand constant updates and surveys would be required to follow the ever-evolving privacy norms.

## 6 LIMITATIONS

Our terminology of "small vs. established" companies does not fully capture the nuance of this space, as established companies may be small in size, and there may exist large but non-mainstream vendors. As a result, participant's perception and understanding of small vs. established companies may benefit from further exploration using different terminology (e.g., "emerging vs. established").

Our survey examined a cloud-based TEE deployment model. However, other models for TEE deployment do exist, e.g., edge, fog, and local (i.e., on-device). These alternate deployment models for TEE placements, as well as their combinations, will result in different information flows that may influence the comfort of a user. Additional research is necessary to quantify the potential performance impacts of TEE use in IoT settings (in any deployment model) and the influence that these overheads have on users' perceptions. Furthermore, it would be informative to add a third condition to our study, which explicitly compares end-to-end encryption of information flows with TEE-enabled information flows.

Additionally, we have measured privacy based on survey responses and quantitative analysis from a US population that does not account for the real-world practices of the participants. This includes the case in which participants may have over-ascribed a sense of trust in TEE scenarios simply because they leverage a TEE. A further investigation of perceived vs. actual benefits of TEEs is a subject of future research. Additionally, our results do not generalize to non-US populations. While we made efforts to avoid straight-lining in our responses, there is still the possibility of erroneous data collection. Use of a longitudinal diary, log study, or qualitative interviews would help validate our findings and is left as future work. Finally, our survey examined two types of IoT devices: smart speakers and smart cameras. Our results may not generalize to other types of IoT devices.

## 7 CONCLUSION

This paper builds upon prior work leveraging the contextual integrity framework to explore user acceptance of information scenarios in the context of smart homes. Unlike prior work, we specifically investigate whether the incorporation of low-cost cloud-based Trusted Execution Environments (TEEs) into IoT devices has the potential to shift the privacy landscape in a meaningful way. Through a between-subject survey of 1049 participants, we have found that use of TEEs can lead to changes in user perceptions of privacy across several important dimensions, yet does not change other long-standing norms around data collection and sharing.

Important changes in user perception occur around themes of data retention, device manufacturer, and sensing modality. Namely,

users were more comfortable with information flows originating from smart home devices across recipients and transmission principles when these flows were mediated by sensors that included cloud-based TEEs. The inclusion of cloud-based TEEs in smart speaker and camera platforms also eliminated differences in comfort with sensing these types of data that existed in scenarios that do not include TEEs and are documented elsewhere in the literature. Finally and importantly, we found that the inclusion of cloud-based TEEs also eliminated differences in user acceptance of smart home devices manufactured by large vs. small manufacturing companies that existed in scenarios that do not include TEEs and are documented elsewhere in the literature. These findings pave the way for the development of richer sensing platforms, increased vendor options for users, and trust in limited-retention data collection.

Importantly, we found that the inclusion of TEEs is not a panacea and that certain well-documented privacy norms are unaffected. User desire for consent prior to data collection and discomfort with indefinite data storage are unaffected by the presence of a TEE. This demonstrates the need for adoption and enforcement of privacy regulations that ensure that these principles are respected. Similarly, concerns around bystander data collection are unimpacted by the presence of a TEE, which further supports the centrality of this concern in our increasingly sensor-rich environments.

## ACKNOWLEDGMENTS

We would like to acknowledge Andrew Xu, Injung Kim, and Erin Walker for their valuable feedback during the development of our study. This work was supported in part by the National Science Foundation under awards 1704139 and 2211507.

## REFERENCES

[1] Denielle Abaquita, Paritosh Bahirat, Karla A. Badillo-Urquiola, and Pamela Wisniewski. 2020. Privacy Norms within the Internet of Things Using Contextual Integrity. In Companion of the 2020 ACM International Conference on Supporting Group Work (Sanibel Island, Florida, USA) (GROUP '20). Association for Computing Machinery, New York, NY, USA, 131–134. https://doi.org/10.1145/3323994.3369891

[2] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019). USENIX Association, Santa Clara, CA, 451–466. https://www.usenix.org/conference/soups2019/presentation/abdi

[3] Noura Abdi, Xiao Zhan, Kopo M. Ramokapane, and Jose Such. 2021. Privacy Norms for Smart Home Personal Assistants. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (Yokohama, Japan) (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 558, 14 pages. https://doi.org/10.1145/3411764.3445122

[4] Wael SAlbayaydh and Ivan Flechais. 2022. Exploring Bystanders' Privacy Concerns with Smart Homes in Jordan. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (New Orleans, LA, USA) (CHI '22). Association for Computing Machinery, New York, NY, USA, Article 446, 24 pages. https://doi.org/10.1145/3491102.3502097

[5] Kunst Alexander. 2022. Smart home device ownership in the U.S. in 2022. Retrieved November 17, 2022 from https://www.statista.com/forecasts/997160/smart-home-device-ownership-in-the-us

[6] Apple. 2021. Secure Enclave. Retrieved August 24, 2022 from https://support.apple.com/en-gb/guide/security/sec59b0b31ff/web

[7] Apple. 2023. Homekit. Retrieved Feb 14, 2023 from https://developer.apple.com/documentation/homekit

[8] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2, 2, Article 59 (jul 2018), 23 pages. https://doi.org/10.1145/3214262

[9] Noah Apthorpe, Sarah Varghese, and Nick Feamster. 2019. Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus COPPA. In 28th USENIX Security Symposium (USENIX Security 19). USENIX Association, Santa Clara, CA, 123–140. https://www.usenix.org/conference/usenixsecurity19/presentation/apthorpe

[10] Martin Armstrong. 2022. The market for smart home devices is expected to boom over the next 5 years. Retrieved July 24, 2022 from https://www.weforum.org/agenda/2022/04/homes-smart-tech-market/

[11] Macy Bayern. 2019. Infographic: People still have no idea what IoT actually is. Retrieved August 02, 2022 from https://www.techrepublic.com/article/infographic-people-still-have-no-idea-what-iot-actually-is/

[12] PRESTON BUKATY. 2019. RIGHTS OF CONSUMERS AND OBLIGATIONS OF THE BUSINESS. IT Governance Publishing, 55–89. http://www.jstor.org/stable/j.ctvjghvnn.9

[13] Raymond Cheng, Fan Zhang, Jernej Kos, Warren He, Nicholas Hynes, Noah Johnson, Ari Juels, Andrew Miller, and Dawn Song. 2019. Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts. In 2019 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 185–200. https://doi.org/10.1109/EuroSP.2019.00023

[14] Camille Cobb, Milijana Surbatovich, Anna Kawakami, Mahmood Sharif, Lujo Bauer, Anupam Das, and Limin Jia. 2020. How Risky Are Real Users' IFTTT Applets?. In Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020). USENIX Association, 505–529. https://www.usenix.org/conference/soups2020/presentation/cobb

[15] Council of European Union. 2018. General Data Protection Regulation. https://gdpr.eu/.

[16] Judicael B. Djoko. 2019. Towards Practical Access Control and Usage Control on the Cloud Using Trusted Hardware. Ph. D. Dissertation. Copyright - Database copyright ProQuest LLC; ProQuest does not claim copyright in the individual underlying works; Last updated - 2022-03-01.

[17] Nico Ebert, Kurt Alexander Ackermann, and Björn Scheppler. 2021. Bolder is Better: Raising User Awareness through Salient and Concise Privacy Notices. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (Yokohama, Japan) (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 67, 12 pages. https://doi.org/10.1145/3411764.3445516

[18] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2021. Which Privacy and Security Attributes Most Impact Consumers' Risk Perception and Willingness to Purchase IoT Devices?. In 2021 IEEE Symposium on Security and Privacy (SP). IEEE, 519–536. https://doi.org/10.1109/SP40001.2021.00112

[19] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (Glasgow, Scotland Uk) (CHI '19). Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300764

[20] Florian M. Farke, David G. Balash, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. 2021. Are Privacy Dashboards Good for End Users? Evaluating User Perceptions and Reactions to Google's My Activity. In 30th USENIX Security Symposium (USENIX Security 21). USENIX Association, 483–500. https://www.usenix.org/conference/usenixsecurity21/presentation/farke

[21] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (Yokohama, Japan) (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 64, 16 pages. https://doi.org/10.1145/3411764.3445148

[22] Lorenzo Franceschi-Bicchierai. 2017. Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings. Retrieved September 01, 2022 from https://www.vice.com/en/article/pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings

[23] Darius-Aurel Frank, Polymeros Chrysochou, and Panagiotis Mitkidis. 2022. The paradox of technology: Negativity bias in consumer adoption of innovative technologies. Psychology & Marketing n/a, n/a (2022). https://doi.org/10.1002/mar.21740

[24] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (Glasgow, Scotland Uk) (CHI '19). Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3290605.3300498

[25] Google. 2022. Trusty TEE. Retrieved August 24, 2022 from https://source.android.com/docs/security/trusty

[26] Google. 2023. Home Graph. Retrieved Feb 14, 2023 from https://developers.home.google.com/cloud-to-cloud/primer/home-graph

[27] Intel. 2014. Intel Software Guard Extensions Programming Reference. Retrieved March 18, 2022 from https://www.intel.com/content/dam/develop/external/us/en/documents/329298-002-629101.pdf

[28] Schlesinger Jennifer and Day Andrea. 2019. It's Not Just Ring. Google, SimpliSafe, and Others Could Share Video Footage With Police Without Consent. Retrieved August 02, 2022 from https://www.cnbc.com/2019/02/07/privacy-policies-give-companies-lots-of-room-to-collect-share-data.html

[29] Haojian Jin, Boyuan Guo, Rituparna Roychoudhury, Yaxing Yao, Swarun Kumar, Yuvraj Agarwal, and Jason I. Hong. 2022. Exploring the Needs of Users for

Supporting Privacy-Protective Behaviors in Smart Homes. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (New Orleans, LA, USA) (CHI '22). Association for Computing Machinery, New York, NY, USA, Article 449, 19 pages. https://doi.org/10.1145/3491102.3517602
[30] Niklas Johannes, Harm Veling, Thijs Verwijmeren, and Moniek Buijzen. 2019. Hard to Resist? Journal of Media Psychology 31, 4 (2019), 214–225. https://doi.org/10.1027/1864-1105/a000248 arXiv:https://doi.org/10.1027/1864-1105/a000248
[31] Heikki Karjaluoto, Jari Karvonen, Manne Kesti, Timo Koivumäki, Marjukka Manninen, Jukka Pakola, Annu Ristola, and Jari Salo. 2005. Factors Affecting Consumer Choice of Mobile Phones: Two Studies from Finland. Journal of Euromarketing 14, 3 (2005), 59–82. https://doi.org/10.1300/J037v14n03_04
[32] Mark Keierleber. 2022. 'Really alarming': the rise of smart cameras used to catch maskless students in US schools. Retrieved March 30, 2022 from https://www.theguardian.com/world/2022/mar/30/smart-cameras-us-schools-artificial-intelligence
[33] Dongyeon Kim, Kyuhong Park, Yongjin Park, and Jae-Hyeon Ahn. 2019. Willingness to provide personal information: Perspective of privacy calculus in IoT services. Computers in Human Behavior 92 (2019), 273–281. https://doi.org/10.1016/j.chb.2018.11.022
[34] Kate Kozuch. 2022. The best smart home devices in 2022. Retrieved March 18, 2022 from https://www.tomsguide.com/us/best-smart-home-devices,review-2008.html
[35] Lancen LaChance. 2016. How to Prevent an IoT Botnet Attack. Retrieved October 27, 2022 from https://www.globalsign.com/en/blog/how-to-prevent-an-iot-botnet-attack
[36] Gierad Laput, Yang Zhang, and Chris Harrison. 2017. Synthetic Sensors: Towards General-Purpose Sensing. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (Denver, Colorado, USA) (CHI '17). Association for Computing Machinery, New York, NY, USA, 3986–3999. https://doi.org/10.1145/3025453.3025773
[37] Azizbek Marakhimov and Jaehun Joo. 2017. Consumer adaptation and infusion of wearable devices for healthcare. Computers in Human Behavior 76 (2017), 135–148. https://doi.org/10.1016/j.chb.2017.07.016
[38] Kirsten Martin and Helen Nissenbaum. 2016. Measuring privacy: An empirical test using context to expose confounding variables. Colum. Sci. & Tech. L. Rev. 18 (2016), 176.
[39] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). USENIX Association, Santa Clara, CA, 399–412. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini
[40] David Nield. 2022. The best smart home systems 2022: Top ecosystems explained Google Home, Alexa, HomeKit, SmartThings and more compared. Retrieved November 01, 2022 from https://www.the-ambient.com/guides/smart-home-ecosystems-152
[41] Helen Nissenbaum. 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, Redwood City. https://doi.org/10.1515/9780804772891
[42] Sandro Pinto, Tiago Gomes, Jorge Pereira, Jorge Cabral, and Adriano Tavares. 2017. IIoTEED: An Enhanced, Trusted Execution Environment for Industrial IoT Edge Devices. IEEE Internet Computing 21, 1 (2017), 40–47. https://doi.org/10.1109/MIC.2017.17
[43] Sandro Pinto and Nuno Santos. 2019. Demystifying Arm TrustZone: A Comprehensive Survey. ACM Comput. Surv. 51, 6, Article 130 (jan 2019), 36 pages. https://doi.org/10.1145/3291047
[44] Qualtrics. 2022. . https://www.qualtrics.com
[45] Pew Research. 2021. Internet/Broadband Fact Sheet. Retrieved April 7, 2021 from https://www.pewresearch.org/internet/fact-sheet/internet-broadband/?menuItem=6d2e5a1d-0fea-4cff-84ef-5999713abe5e
[46] Mohamed Sabt, Mohammed Achemlal, and Abdelmadjid Bouabdallah. 2015. Trusted Execution Environment: What It is, and What It is Not. In 2015 IEEE Trustcom/BigDataSE/ISPA, Vol. 1. 57–64. https://doi.org/10.1109/Trustcom.2015.357
[47] Mahsa Saeidi, McKenzie Calvert, Audrey W Au, Anita Sarma, and Rakesh B Bobba. 2022. If this then that: exploring users' concerns with IFTTT applets. Proceedings on Privacy Enhancing Technologies 2022, 1 (2022), 166–186. https://doi.org/10.2478/popets-2022-0009
[48] Christine Satchell and Paul Dourish. 2009. Beyond the User: Use and Non-Use in HCI. In Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group: Design: Open 24/7 (Melbourne, Australia) (OZCHI '09). Association for Computing Machinery, New York, NY, USA, 9–16. https://doi.org/10.1145/1738826.1738829
[49] Connectivity Standards Service. 2023. Matter. Retrieved Feb 14, 2023 from https://csa-iot.org/all-solutions/matter/
[50] Carlton Shepherd, Raja Naeem Akram, and Konstantinos Markantonakis. 2017. Establishing Mutually Trusted Channels for Remote Sensing Devices with Trusted Execution Environments. In Proceedings of the 12th International Conference on Availability, Reliability and Security (Reggio Calabria, Italy) (ARES '17). Association for Computing Machinery, New York, NY, USA, Article 7, 10 pages. https://doi.org/10.1145/3098954.3098971
[51] Carlton Shepherd, Raja Naeem Akram, and Konstantinos Markantonakis. 2017. Establishing Mutually Trusted Channels for Remote Sensing Devices with Trusted Execution Environments (ARES '17). Association for Computing Machinery, New York, NY, USA, Article 7, 10 pages. https://doi.org/10.1145/3098954.3098971
[52] Yan Shvartzshnaider, Schrasing Tong, Thomas Wies, Paula Kift, Helen Nissenbaum, Lakshminarayanan Subramanian, and Prateek Mittal. 2016. Learning privacy expectations by crowdsourcing contextual informational norms. In Fourth AAAI conference on human computation and crowdsourcing.
[53] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. 2019. "I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019). USENIX Association, Santa Clara, CA, 435–450. https://www.usenix.org/conference/soups2019/presentation/tabassum
[54] Securicon Team. 2020. Why Third-Party Vendors Are Responsible for the IoT Security Problem. Retrieved October 27, 2022 from https://www.securicon.com/why-third-party-vendors-are-responsible-for-the-iot-security-problem/
[55] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. 2022. "It Would Probably Turn into a Social Faux-Pas": Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (New Orleans, LA, USA) (CHI '22). Association for Computing Machinery, New York, NY, USA, Article 404, 13 pages. https://doi.org/10.1145/3491102.3502137
[56] John Lucker Tom Davenport. 2015. Running on data: Activity trackers and the Internet of Things. Retrieved September 01, 2022 from https://www.linkedin.com/pulse/running-data-activity-trackers-internet-things-tom-davenport
[57] Amazon Mechanical Turk. 2022. . https://www.mturk.com
[58] Aliza Vigderman and Gabe Turner. 2022. The Best Smart Home Devices of 2022. Retrieved October 27, 2022 from https://www.security.org/smart-home/best/#wyze-cam
[59] Alexandra Voit, Dominik Weber, and Niels Henze. 2018. Qualitative Investigation of Multi-Device Notifications. In Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers (Singapore, Singapore) (UbiComp '18). Association for Computing Machinery, New York, NY, USA, 1263–1270. https://doi.org/10.1145/3267305.3274117
[60] Wikipedia contributors. 2022. Bonferroni correction — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Bonferroni_correction&oldid=1093604073 [Online; accessed 5-August-2022].
[61] Wikipedia contributors. 2022. Trusted execution environment — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Trusted_execution_environment&oldid=1105563332 [Online; accessed 25-August-2022].
[62] Meredydd Williams, Jason R. C. Nurse, and Sadie Creese. 2016. The Perfect Storm: The Privacy Paradox and the Internet-of-Things. In 2016 11th International Conference on Availability, Reliability and Security (ARES). IEEE, 644–652. https://doi.org/10.1109/ARES.2016.25
[63] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019. Privacy Perceptions and Designs of Bystanders in Smart Homes. Proc. ACM Hum.-Comput. Interact. 3, CSCW, Article 59 (nov 2019), 24 pages. https://doi.org/10.1145/3359161
[64] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). USENIX Association, Santa Clara, CA, 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng
[65] Shikun Zhang, Yuanyuan Feng, Lujo Bauer, Lorrie Faith Cranor, Anupam Das, and Norman Sadeh. 2021. "Did you know this camera tracks your mood?": Understanding Privacy Expectations and Preferences in the Age of Video Analytics. Proceedings on Privacy Enhancing Technologies 2021, 2 (2021), 282–304.

# A TABLE FOR INFLUENCE OF TRANSMISSION PRINCIPLES

| Recipients | Comparison | Without TEE | | With TEE | |
|---|---|---|---|---|---|
| | | □– □ □ □ □ □ % | | □– □□ □ | % |
| Law Enforcement | TR1-NULL | 0.000** | 18.48% | 0.000** | 16.67% |
| | TR2-NULL | 0.000** | 9.42% | 0.000** | 10.44% |
| | TR3-NULL | 0.208 | 2.17% | 0.034 | 3.03% |
| | TR4-NULL | 0.42 | 1.81% | 0.08 | 3.33% |
| Continued | | | | | |

| Recipients | Comparison | Without TEE | | With TEE | |
|---|---|---|---|---|---|
| | | □– □ □ □ □ □ % | | □– □ □ □ □ □ % | |
| Device Manufacturer | TR5-NULL | 0.889 | 1.45% | 0.037 | 3.94% |
| | TR6-NULL | 0.048 | -2.9% | 0.000** | -11.21% |
| | TR7-NULL | 0.000** | 16.71% | 0.000** | 16.36% |
| | TR1-NULL | 0.000** | 13.78% | 0.000** | 9.9% |
| | TR2-NULL | 0.001* | 7.05% | 0.282 | 1.49% |
| | TR3-NULL | 0.0001* | 12.5% | 0.0006* | 7.46% |
| | TR4-NULL | 0.203 | 1.92% | 0.001* | 9.95% |
| | TR5-NULL | 0.001* | 6.4% | 0.000** | 8.71% |
| | TR6-NULL | 0.000** | -8.97% | 0.000** | -11.69% |
| | TR7-NULL | 0.0003* | 12.18% | 0.0002* | 10.7% |
| Other Devices at Places | TR1-NULL | 0.001* | 7.21%% | 0.000* | 11.2% |
| | TR2-NULL | 0.304 | 0.75% | 0.187 | 1.82% |
| | TR3-NULL | 0.0003* | 6.97% | 0.0007* | 8.07% |
| | TR4-NULL | 0.0003* | 6.96% | 0.005 | 0.52% |
| | TR5-NULL | 0.000** | 5.47% | 0.0001* | 8.85% |
| | TR6-NULL | 0.000** | -8.71% | 0.000** | -8.33% |
| | TR7-NULL | 0.843 | 0.25% | 0.0004* | 9.38% |
| Recommend-ation Services | TR1-NULL | 0.001* | 11.7% | 0.001* | 10.92% |
| | TR2-NULL | 0.263 | 1.77% | 0.303 | 0.57% |
| | TR3-NULL | 0.245 | -1.77% | 0.001* | 0.29% |
| | TR4-NULL | 0.001* | 13.48% | 0.000** | 12.36% |
| | TR5-NULL | 0.001* | 9.93% | 0.000** | 11.49% |
| | TR6-NULL | 0.000** | -13.02% | 0.000** | -15.26% |
| | TR7-NULL | 0.001* | 12.06% | 0.085 | 0.86% |
| Health Services | TR1-NULL | 0.000** | 11.49% | 0.0004* | 12.9% |
| | TR2-NULL | 0.001* | 17.22% | 0.218 | 1.61% |
| | TR3-NULL | 0.0003* | 10.63% | 0.0005* | 8.33% |
| | TR4-NULL | 0.0008* | 9.2% | 0.0002* | 12.39% |
| | TR5-NULL | 0.0005* | 7.76% | 0.0007* | 11.56% |
| | TR6-NULL | 0.000** | -9.48% | 0.000** | -11.29% |
| | TR7-NULL | 0.0002* | 11.21% | 0.0005* | 10.48% |
| Family Members/ Friends | TR1-NULL | 0.0001* | 8.89% | 0.0001* | 9.9% |
| | TR2-NULL | 0.001* | 8.61% | 0.001* | 6.83% |
| | TR3-NULL | 0.000** | 6.94% | 0.000** | 6.62% |
| | TR4-NULL | 0.000** | 8.61% | 0.000** | 9.18% |
| | TR5-NULL | 0.000** | 7.5% | 0.000** | 8.7% |
| | TR6-NULL | 0.000** | -6.94% | 0.000** | -12.32% |
| | TR7-NULL | 0.005 | 1.94% | 0.0003* | 9.62% |

| Key | Value |
|---|---|
| TR1 | if you have given consent |
| TR2 | if you are notified |
| TR3 | if information used for maintenance of device/feature |
| TR4 | if information is not stored |
| TR5 | if information is stored for duration of 1-3 months |
| TR6 | if information is stored indefinitely |
| TR7 | if privacy policy mentions the {recipient} and the purpose of sharing |

Table 6: Wilcoxon Singned Rank test for influence of TEE on comfort with transmission principles. Reporting p-values for 42 comparisons, * stands for □ ≤ 0.001 and **stands for □ ≤ 0.0001.

## B TABLE FOR INFLUENCE OF TEES ON COMFORT WITH INFORMATION FLOWS BY SUBJECT

| Transmission Principle | Device Owners | | Other Occupants | |
|---|---|---|---|---|
| | □– □ □ □ □□□– □ □ □ □□□– □ □ □ □□□– | | | |
| □ □ □if you have given consent | 38555.0 | 0.014 | 33488.5 | 0.005 |
| if you are notified | 38076.0 | 0.029 | 32310.0 | 0.02 |
| if information is used for maintenance of device | 36856.5 | 0.014 | 34391.5 | 0.009 |
| if information is not stored | 36433.5 | 0.0218 | 33021.0 | 0.005 |
| if information is stored for duration of 1-3 months | 35006.0 | 0.0.006 | 34551.5 | 0.009 |
| if information is stored indefinitely | 34989.5 | 0.0069 | 32535.0 | 0.008 |
| if policy mentions {recipient} and the purpose of sharing | 36846.0 | 0.014 | 33263.0 | 0.05 |
| Recipient | Without TEE | | With TEE | |
| | □– □ □ □ □□□– □ □ □ □□□– □ □ □ □□□– | | | |
| □ □ □Law Enforcement | 37258.5 | 0.0087 | 33304.0 | 0.005 |
| Device Manufacturer | 37316.0 | 0.008 | 33769.5 | 0.007 |
| Other Devices at Place | 35468.0 | 0.005 | 32298.5 | 0.02 |
| Recommendation Services | 35533.5 | 0.0047 | 32796.0 | 0.03 |
| Health Services | 37297.0 | 0.083 | 32080.5 | 0.01 |
| Family Members/ Friends | 36417.5 | 0.021 | 32353.5 | 0.023 |

Table 7: Mann Whitney's U test for subject sensing effect for transmission principles and recipients for both groups device owners and other occupants using between-subject analysis. Reporting values for significant differences. ⍰ stands for □ ≤ 0.004.

| Transmission Principle | Without TEE | | With TEE | |
|---|---|---|---|---|
| | □– □ □ □ □□□– □ □ □ □□□– □ □ □ □□□– | | | |
| □ □ □if you have given consent | 38365.5 | 0.0025⍰ | 29443.5 | 0.003⍰ |
| if you are notified | 37913.5 | 0.003⍰ | 28641.5 | 0.002⍰ |
| if information is used for maintenance of device | 36850.5 | 0.0041⍰ | 30493.0 | 0.0022⍰ |
| if information is not stored | 38869.5 | 0.001⍰ | 3144.0 | 0.0015⍰ |
| if information is stored for duration of 1-3 months | 38299.0 | 0.002⍰ | 33615.0 | 0.004⍰ |
| if information is stored indefinitely | 36674.0 | 0.0018⍰ | 30388.5 | 0.002⍰ |
| if policy mentions {recipient} and the purpose of sharing | 36587.0 | 0.0008⍰ | 29564.5 | 0.0007⍰ |
| Recipient | Without TEE | | With TEE | |
| | □– □ □ □ □□□– □ □ □ □□□– □ □ □ □□□– | | | |
| □ □ □Law Enforcement | 38534.5 | 0.002⍰ | 30605.5 | 0.002⍰ |
| Device Manufacturer | 38130.5 | 0.003⍰ | 30565.5 | 0.002⍰ |
| Other Devices at Place | 38077.5 | 0.003⍰ | 30947.5 | 0.003⍰ |
| Recommendation Services | 37211.0 | 0.0016⍰ | 30450.5 | 0.002⍰ |
| Health Services | 38945.5 | 0.001⍰ | 29942.0 | 0.0012⍰ |
| Family Members/ Friends | 37586.5 | 0.004⍰ | 29865.5 | 0.0011⍰ |

Table 8: Mann Whitney's U test for subject of sensing effect for transmission principles and recipients for both groups with and without TEE using within subject analysis. Reporting values for significant differences. ⍰ stands for □ ≤ 0.004.

## C AVERAGE ACCEPTABILITY SCORES FOR OTHER DEVICES AT PLACE'S

The average acceptability scores are shown in Figure 8

## D DEMOGRAPHICS

The distribution of participants in the survey is shown in Figure 9 by gender, Figure 10 by age, Figure 11 by household income, and Figure 12 by IoT device ownership.

## E IUIPC SCORES

The overall IUIPC scores in both groups is shown in Table 9.

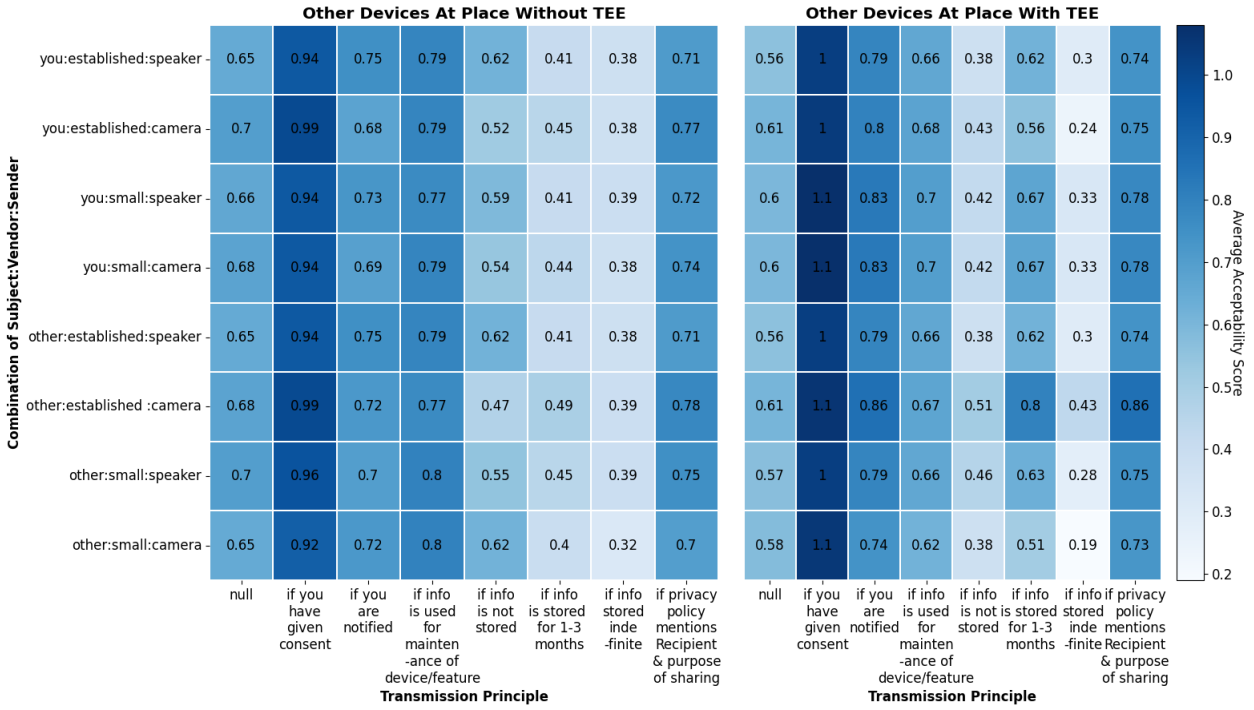



Figure 8: Other Devices at Place's Average Acceptability of information flows grouped by without TEE on left and with TEE on right.

| IUIPC | Without TEE | | With TEE | |
|---|---|---|---|---|
| | Mean(□) | Std.Dev (□) | Mean(□) | Std.Dev(□) |
| IUIPC Control | 5.59 | 2.42 | 5.72 | 2.62 |
| IUIPC Awareness | 5.78 | 2.64 | 5.82 | 2.63 |
| IUIPC Collection | 7.38 | 3.68 | 7.52 | 3.59 |

Table 9: IUIPC scores of participants in both groups without and with TEE. We have reported the mean (□) and the standard deviations (□) of the scores.

# F SURVEY INSTRUMENT

## F.1 SURVEY OVERVIEW

Before presenting the CI question a brief overview was given to participants shown in Figure 13.

## F.2 NULL TRANSMISSION PRINCIPLE QUESTIONS

- Without TEE: A Sender from Vendor records Sender-DataType of Subject in your smart home. In your opinion as the device owner, how acceptable is for the Vendor to send Sender-DataType of Subject to the following recipients?
- With TEE: A Sender from Vendor records Sender-DataType of Subject in your smart home. In your opinion as the device owner, how acceptable is for the Vendor to send Sender-DataType of Subject to the following types of recipients when data processing occurs within a Trusted Execution Environment (TEE)?

The null transmission principle questions for Without TEE group is shown in Figure 14 and for With TEE group shown in Figure 1a.

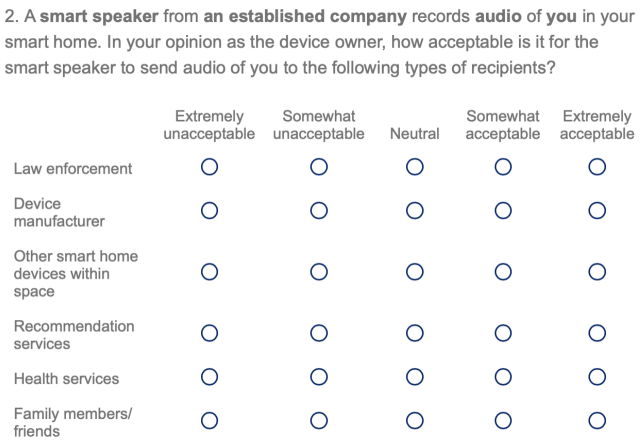
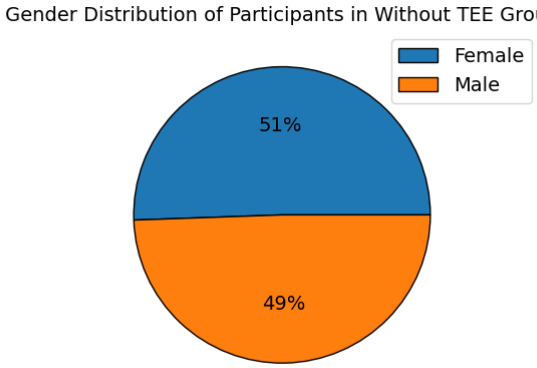
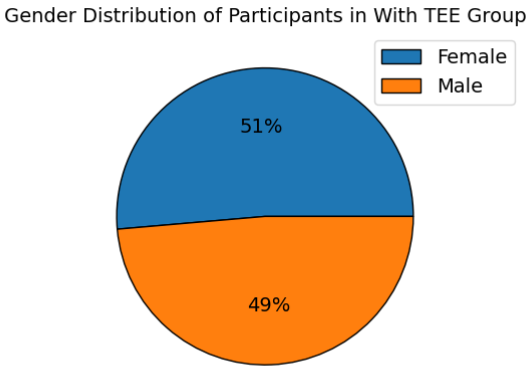



Figure 14: Example of Null Transmission Question Without TEE

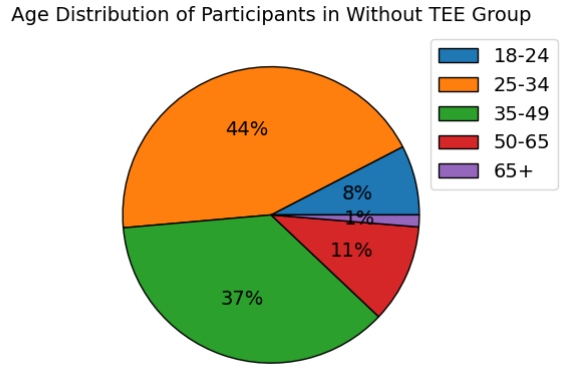



(a) Gender distribution of participants without TEE group

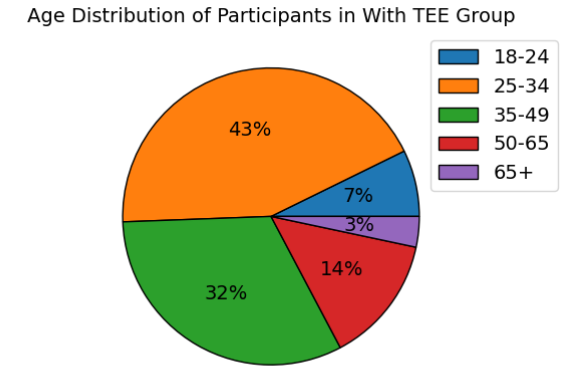



(b) Gender distribution of participants without TEE group

Figure 9: Gender distribution of the participants in the survey. In Figure 9a shows the Without TEE group gender distribution and Figure 9b shows for With TEE group




(a) Age distribution of participants without TEE group




(b) Age distribution of participants with TEE group

Figure 10: Age distribution of the participants in the survey. In Figure 10a shows the Without TEE group age distribution and Figure 10b shows for With TEE group

## F.3 NON-NULL TRANSMISSION PRINCIPLE QUESTIONS

Each recipients was enquired for the non-null transmission principles with its purpose. The Without TEE group non-null transmission principle questions is shown in Figure 15, and for With TEE group shown in Figure 1b.

## F.4 SURVEY SELECTION PARAMETERS

Before presenting the question, the participants were randomly assigned to a group with TEE or without TEE. With TEE group had CI questions with information flows having the TEE and Without TEE group had CI questions regarding the existing information flows. After the group selection a random selection of parameters was done for Sender, Sender's Data Type Vendor, Subject. All parameters were selected from Table 10.

## F.5 QUESTIONERS FOR TEE GROUP AFTER VIDEO

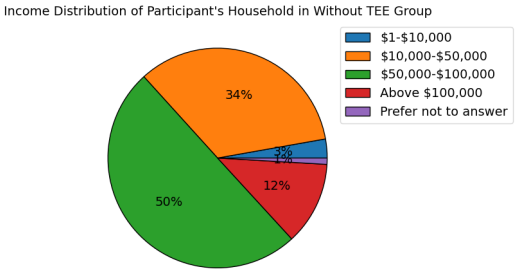
(1) Non-authorized persons can modify/change the nature of the algorithm being used or gain access to the image database.
(2) The Face recognition algorithm can only unlock the video data locked with face recognition algorithm lock. For the rest of the algorithms, the video data remains locked.
(3) After locking the video data, a non-authorized person is able to access or alter the video data.

## F.6 VIDEO LINKS

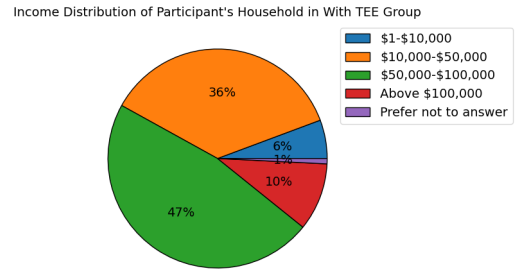
(1) Video shown to cloud-based TEE group: https://youtu.be/RsGSqjsXIiY
(2) Video shown to without TEE group: https://youtu.be/XOT9vfxzz3U

| Group | Sender | Vendor | Subject | Recipient | Purpose | Transmission Principle |
|---|---|---|---|---|---|---|
| Without TEE | Smart Speaker | Small Company | You | Law Enforcement | for investigation into a reported crime | if you have given consent |
| With TEE | Smart Camera | Established Company | Other Occupants | | | if you are notified |
| | | | | Device Manufacturer | for understanding device utilization | if information used for maintenance of device/ feature |
| | | | | Other Devices at Place | to control other smart devices | if information is not stored |
| | | | | Recommen-dation Services | to provide with local offers that are nearby | if information is stored for duration on 1-3 months |
| | | | | Health Services | to monitor health and for emergency responses | if information is stored indefinitely |
| | | | | Family members/ friends | for caregiving / monitoring | if privacy policy mentions the {recipient} and the purpose of sharing |
| | | | | | | null |

Table 10: CI Parameters chosen to generate smart home information flows. The data parameter is not listed as its audio for smart speaker and video for smart camera.

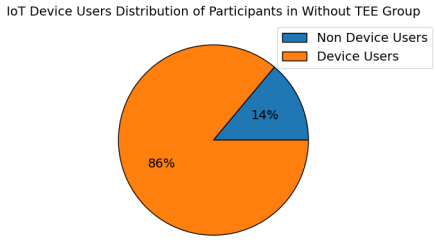



(a) Household Income distribution of participants without TEE group

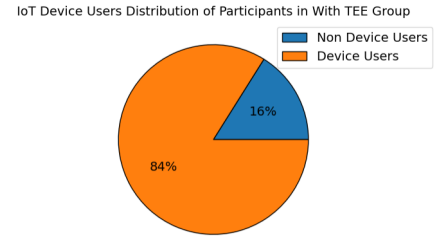



(b) Household Income distribution of participants without TEE group

Figure 11: Household Income distribution of the participants in the survey. In Figure 11a shows the Without TEE household income distribution and Figure 11b shows for With TEE group




(a) IoT device owners/usage distribution of participants without TEE group




(b) IoT device owners/usage distribution of participants with TEE group

Figure 12: IoT device owners/usage distribution of the participants in the survey. In Figure 12a shows the Without TEE IoT device owners/usage experience distribution and Figure 12b shows for With TEE group

**Survey Overview:**

Smart home devices and appliances are becoming increasingly popular. These types of devices often have sensors that collect information about people that own and use them and the spaces within which they are situated. This information may be sent to numerous recipients for a variety of purposes related to the functionality of the device.

As an example, consider a Google Nest Camera installed at the front door of a home. The video feed for this camera may be used for numerous purposes, including:

1. Detecting unknown individuals
2. Activating porch lights at dusk.
3. Get recorded video history.

Many large technology (e.g., Google, Amazon, Apple, etc.) and appliance (e.g., Samsung, LG, GE, etc.) vendors from established companies manufacture and sell smart home devices. However, these devices may also be manufactured by smaller companies or startups with less brand recognition. A key feature of smart devices is the collection and transmission of data outside of the space for processing and enabling value-added functionality within the space, or for space owners.

In the survey, always consider yourself as the owner of the device in each scenario. This survey contains questions about information flows from devices located inside a smart home to various types of recipients that may enable functionalities based upon this data. These devices are either manufactured by an established company or manufactured by a small company. You will be asked whether you think each information flow with the device is acceptable for yourself or occupants other than you that are utilizing the space. Please answer each question as honestly as possible.

Figure 13: Survey Overview

3.1. A **smart speaker** from **an established company** records **audio** of **you** in your smart home. In your opinion as the device owner, how acceptable is for the smart speaker to send audio of you to **Law enforcement** for investigation into a reported crime under the following circumstances?

| | Extremely unacceptable | Somewhat unacceptable | Neutral | Somewhat acceptable | Extremely acceptable |
|---|---|---|---|---|---|
| if you have given consent | ○ | ○ | ○ | ○ | ○ |
| if you are notified | ○ | ○ | ○ | ○ | ○ |
| if information used for maintenance of device/ feature | ○ | ○ | ○ | ○ | ○ |
| if information is not stored | ○ | ○ | ○ | ○ | ○ |
| if information is stored for duration on 1-3 months | ○ | ○ | ○ | ○ | ○ |
| if information is stored indefinitely | ○ | ○ | ○ | ○ | ○ |
| if privacy policy mentions the Law enforcement and the purpose of sharing | ○ | ○ | ○ | ○ | ○ |

Figure 15: Example of Non-Null Transmission Question Without TEE