Effect of Device Risk Perceptions and Understandability of Data Management Features on Consumers' Willingness to Pay (WTP) for IoT Device Premium Data Management Plan

Ehsan Ul Haque
ehsan.ul_haque@uconn.edu
University of Connecticut
Storrs, Connecticut, United States

Mohammad Maifi Hasan Khan
mohammad.khan@uconn.edu
University of Connecticut
Storrs, Connecticut, United States

ABSTRACT

Prior research has noted that users are willing to pay a premium for higher privacy and security of Internet of Things (IoT) devices. However, it is not clear whether and how users' technical literacy and understandability of data management features impact users' willingness to pay (WTP) for a premium data management plan that gives additional controls over a device's data collection, sharing, and usage for better privacy management. Toward that, we conducted an online study with 159 United States participants. Our results indicate that technical literacy affects users' willingness to pay for a premium plan, mediated by their understandability of the data management features. Further analysis of users' trust perceptions revealed that technical literacy affects consumers' understandability of data management features, leading to lower integrity and benevolence perceptions of Internet of Things manufacturers. Interestingly, our findings noted that offering data management plans, even for a fee, can positively affect users' perceived trustworthiness toward Internet of Things manufacturers. The implications of our findings for user data privacy are discussed in the paper.

CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in HCI**; • **Security and privacy** → **Usability in security and privacy**.

KEYWORDS

WTP for privacy, IoT privacy, Data management plan, Privacy understandability, Technical literary, Trust

ACM Reference Format:
Ehsan Ul Haque and Mohammad Maifi Hasan Khan. 2023. Effect of Device Risk Perceptions and Understandability of Data Management Features on Consumers' Willingness to Pay (WTP) for IoT Device Premium Data Management Plan. In *The 2023 European Symposium on Usable Security (EuroUSEC 2023), October 16–17, 2023, Copenhagen, Denmark*. ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3617072.3617118

EuroUSEC 2023, October 16–17, 2023, Copenhagen, Denmark

ACM ISBN 979-8-4007-0814-5/23/10…$15.00
https://doi.org/10.1145/3617072.3617118

1 INTRODUCTION

Recently, a startup company named Telly has offered to giveaway 500,000 smart televisions for free. However, the "free" television comes with an attached second screen, which will stream non-stop targeted advertisements combined with both viewing data and extensive personal data collected from the household's daily activities through its sensors, including sensors to assess how many people are watching from the couch [24].

The trend of data-oriented business has been accelerated in recent years, where collection and monetization of personal data have become the critical focus for e-commerce [4, 10]. The acceptance of smart home Internet of Things (IoT) devices with the promise of an improved and convenient life have made user data collection more seamless. Not surprisingly, the excessive amount of data collection has raised serious concerns for user data privacy among privacy advocates and end-users [47, 55, 56], which is further exacerbated by poor data collection and usage practices by IoT manufacturers while not correctly informing users about such practices [27, 33, 38, 52]. At the same time, the lack of availability of salient information on sensor data collection and privacy practices makes it hard for consumers to perform informed purchase decisions based on their security and privacy expectations [17].

Prior research revealed that users are willing to pay a premium for higher privacy and security of the IoT devices [9, 16, 17, 22, 34]. However, the lack of such information at the time of purchase often leads users to underestimate the invasiveness of the smart devices' data collection practices [15], which can incentivize IoT manufacturers to refrain from making salient data collection practices readily available at the time of purchase. In addition, even though consumers express willingness to pay a premium for devices with better privacy and security practices, there is still a gap in the literature exploring how users' willingness to pay (WTP) for better privacy management is impacted and whether it creates sufficient incentives for the IoT manufacturers to go for privacy-focused data collection and usage practices while manufacturing IoT devices.

Towards that, in this study, we examine factors that impact users' WTP for a premium data management plan that gives users additional controls over IoT devices' data collection, sharing, and usage practices for better privacy management. This exploration gives us a better understanding of users' willingness to pay for privacy management, revealing the factors that most influence such a decision to pay a premium for managing data privacy. In addition, shedding light on users' willingness to pay for data management features would help clarify whether offering such a data management plan

alongside IoT devices would be a viable and incentivized option for IoT manufacturers to consider.

To understand users' WTP for data management, we developed a hypothetical data management plan offering features to give users control over the IoT manufacturers' data retention, sharing, and usage practices. Our review of the IoT products on Amazon revealed that IoT manufacturers often offer free cloud storage up to a specific limit along with the device. Further, many allow viewing and sharing of data over the cloud as a free basic data management option. Based on this observation, we developed two versions of the data management plan: the basic and the premium. The basic plan included free cloud storage of up to 2 TB alongside the option to view and download cloud-stored data from anywhere. In addition to this feature, the premium plan included three additional features based on user expectations for data management, pointed out in prior works. Work from Emami-Naeini et al. showed that users often expect control over managing IoT devices' data retention, sharing, and usage practices and express willingness to purchase devices with these options included [16, 17]. Based on these prior findings, the additional features offered in the premium data management plan include - *Control over cloud data* - option to delete sensor data stored on the cloud; *Control over data sharing* - option to opt-out from third party data sharing; and *Control over data usage* - option to restrict the IoT manufacturer to use collected data in ways other than keeping the device functional.

To understand users' WTP for the premium data management plan, we informed users that the basic plan is free and included in the device purchase price. In contrast, the premium plan needs to be purchased for an additional yearly subscription fee. We asked them to indicate the fee they are willing to pay for the premium data management plan using Van Westendorp's Price Sensitivity Meter (PSM) [51]. PSM asks for four price points (e.g., a price that is "too cheap", "cheap", "expensive", and "too expensive" to consider the product) for a target product (i.e., the premium data management plan in our case) to determine the optimal price for the product [29]. We used all these four price points to reference users' WTP for the premium plan and to investigate the factors affecting the WTP.

Among the factors that may affect users' WTP, we first considered IoT device risk perceptions. Prior works in the IoT context noted that device risk perceptions impact users' perception and expectations for privacy for smart home IoT devices [16, 17]. For example, an indoor smart home security camera that collects video data raises more privacy concerns regarding the collected data compared to a smart lightbulb with a motion sensor. Hence, expecting that users' perception of privacy risks towards the IoT devices will affect their WTP for the premium plan, we designed the study with two groups, namely, the High-risk (HR) group that offers data management plans for an indoor smart home security camera, and the Low-risk (LR) group that offers data management plans for a smart lightbulb with motion sensor. The devices in the High-risk and Low-risk groups were selected based on prior research [36].

Along with risk perceptions, the understandability of privacy is identified as another important factor that guides informed privacy decision-making. In this vein, Malhotra et al. informed that users' ability to understand privacy mechanisms is crucial for privacy adoption [30]. Recently, Ul Haque et al. showed that users' technical literacy crucially impacts their perception of trust towards the service provider, shaping their decision to adopt or not adopt privacy controls for better privacy protection [50].

Given the interplay of multiple factors towards users' privacy perception and behavior, we incorporated technical literacy, understandability of data management features, and trust perceptions towards IoT manufacturers as factors that we expect to impact users' WTP for the premium data management plan and investigated the following research questions.

RQ1. Does users' willingness to pay (WTP) for the premium data management plan vary based on the risk perception of the IoT device under consideration (i.e., HR vs. LR groups)? Are users likely to choose the premium plan over the basic plan based on the risk perception of the IoT device?

RQ2. How does users' technical literacy impact their understandability of the premium plan features and their WTP for the premium data management plan?

RQ3. How does users' technical literacy and understandability of the premium plan features impact their perception of trust (i.e., integrity, competence, and benevolence) towards IoT manufacturer? How does the perception of trust towards IoT manufacturers impact users' WTP for the premium data management plan?

RQ4. Does offering a premium data management plan with a subscription fee impact users' overall trust perceptions towards the offered IoT manufacturer, and why?

To answer the research questions, we performed a study on Amazon Mechanical Turk (MTurk) platform and collected data from 159 participants. We took strict measures to ensure data quality on MTurk, which we elaborated on in the methodology section. Our results indicate that, even though participants' WTP for the premium plan is higher for the High-risk (camera) group compared to the Low-risk (lightbulb) group, the difference was not statistically significant, implying that, even though users see device risks differently based on the data sensitivity, their willingness to pay for data management features remain somewhat similar, irrespective of the IoT device. Further, regression analysis suggests understandability of the premium plan features is a crucial factor that mediates the relationship between users' technical literacy and their WTP for the premium plan. Our results also suggest a mediating effect of understandability on the relationship between participants' technical literacy and their perception of integrity and benevolence towards the IoT manufacturer; however, these dimensions of trust were not found to be impacting their WTP for the premium plan. The implications of our findings from both the perspective of IoT device manufacturers and consumers are discussed in the paper.

2 BACKGROUND AND RESEARCH HYPOTHESES

In this section, we discuss prior efforts focusing on the factors affecting privacy perceptions, attitudes, and behaviors, and list the research hypotheses investigated in the paper.

2.1 Users' Willingness to Pay for Privacy

A body of work in the security and privacy domain investigated users' willingness to pay for security and privacy across different contexts. In the security context, prior research showed that users

were willing to pay a premium for features such as better and improved phishing detection [39], and reduced risk of identity theft online [41]. In privacy contexts, Tasi et al. informed that, when privacy-related information is made salient, users often indicate a higher willingness to purchase products from retailers that better protect privacy, even if the product requires a higher price, suggesting that privacy may work as a selling point for retailers and businesses [49]. Similarly, prior work in the context of social media noted that users expressed willingness to pay a premium for privacy-preserving features [43].

In IoT contexts, Morgner et al. investigated and noted that security update availability significantly impacts users' purchase decision of the IoT devices [34]. In the same vein, Emami-Naeini et al. noted that users were willing to pay a premium of about 10% to 30% of the base device price when security and privacy information is saliently available at the purchase time [17]. In a more recent study, Emami-Naeini et al. performed an incentive-compatible approach to measure users' WTP for devices with higher security and privacy. They indicated that deidentified data collection, compared to identifiable one, poses the most impact on users' WTP [15]. They further noted that, for IoT devices with no security and privacy information, users often overestimate the devices' practices to be consistent with the average IoT device in the market, indicating a potential incentive for the IoT manufacturers not to make such information saliently available at the purchase time.

Notably, prior works mostly looked at WTP for devices with higher security and privacy or where such information is readily available. In contrast, in this work, we concentrate on consumers' willingness to pay for a premium data management plan that gives users enhanced control over their data privacy management. Users' WTP for such a plan would incentivize the IoT manufacturers to offer such plans alongside their IoT products.

An important factor noted in prior work that affects privacy perception is the perceived risk of the data that the IoT device collects. Morgner et al. noted a higher willingness to pay for IoT devices with better security attributes when the devices' risk perception is high [34]. Prior work also noted differences in the comfort level for data collected by IoT devices with high risk perceptions than those with low risk perception [36]. Based on these results, we expect users' WTP for the premium plan and their likelihood of choosing the premium option over the basic option to be significantly higher for the High-risk group compared to the Low-risk group. Hence, we pose the following hypotheses:

H1a. The likelihood of choosing the premium data management plan will be significantly higher in the HR group compared to the LR group.

H1b. Participants in the HR group will indicate significantly higher WTP for the premium plan (all four price points) compared to the participants in the LR group.

2.2 Users' Technical Literacy and Understandability of Privacy

Literature identifies users' technical literacy as an essential factor in their perception of privacy. For instance, Kang et al.'s work investigated and confirmed differences in the mental models of technical and non-technical participants and suggested that technical participants have a more sophisticated mental model that enables them to better understand privacy-related constructs compared to non-technical users who have comparatively simpler mental models [23]. Malhotra et al.'s work showed that understanding privacy constructs enables users to act more proactively in their privacy decision-making, especially to adopt more privacy-protective measures [30]. Prior research among Facebook users further noted that users' technical literacy does impact their understandability of Facebook's privacy features [12]. In the context of Social Networking Sites (SNS), a similar role of technical literacy on users' understandability and subsequent privacy behavior was also noticed [8, 45]. Based on these prior findings, we expect users' understandability of data management features to be affected by their technical literacy. As understandability of privacy was found to impact protective privacy decision-making, in our study, we expect users' understandability of privacy features to significantly affect their WTP for the premium plan for all four price points. Hence, we pose the following hypotheses:

H2a. Users' understandability of the data management features will positively impact their WTP for the premium plan (all four price points).

H2b. The relationship between users' technical literacy and their WTP for the data management plan (all four price points) will be mediated by users' understandability of the data management features.

2.3 Effect of Trust Perceptions on Privacy Decision-Making

In the context of privacy, the perception of trust comes from users' belief that the service provider is willing to protect user data, which helps reduce their concern about data collection [11, 54]. When combining trust and privacy, a notion of appropriate trust often comes into consideration, as prior works depicted how inappropriate trust may lead to risky privacy behavior. For example, work from Balash et al. showed how trust towards Google inappropriately led to trusting third-party services authorized with Single Sign-On (SSO) services [7].

Regarding factors affecting users' trust perceptions, Ul Haque et al.'s work in the context of Google showed how technical literacy impacts users' perception of trust, especially their perception of integrity and benevolence in Google's context. Even though participants indicated an overall higher integrity and benevolence perception of Google, likely to be influenced by brand trust [32], technical participants indicated significantly lower integrity and benevolence perception of Google compared to non-technical participants [50]. However, technical and non-technical users had similar perceptions of Google's high competence. Hence, we expect technical literacy to negatively impact users' perception of integrity and benevolence toward IoT manufacturers. In addition, we expect the effect of users' technical literacy on their perception of integrity and benevolence to be mediated by their understandability of the data management features. Hence, we pose the following hypotheses:

H3a. Users' technical literacy will impact users' integrity perception towards IoT manufacturers negatively.

H3b. The relationship between users' technical literacy and integrity perception towards IoT manufacturers will be mediated by users' understandability of the data management features.

H4a. Users' technical literacy will impact users' benevolence perception towards IoT manufacturers negatively.

H4b. The relationship between users' technical literacy and benevolence perception towards IoT manufacturers will be mediated by users' understandability of the data management features.

Trust has been studied to be a crucial factor shaping users' perception and adoption of privacy [28]. Lower trust perceptions induce concern over the data collection, leading users towards choosing options that restrict services providers' data collection and usage [50, 54]. Hence, we expected that participants with lower trust perceptions towards the IoT manufacturers will be more interested in the premium plan and will indicate higher WTP. So, we hypothesize:

H5. Users' trust perceptions will negatively impact their WTP for the premium plan (all four price points).

3 METHODOLOGY

We developed a hypothetical data management plan to examine users' WTP for a premium data management plan that provides additional privacy controls and data management functionality for a yearly subscription fee. The following sections detail the study's design and hypothetical data management plan.

3.1 IoT Devices and Purchase Price Considerations

To ensure realism, we used deception to inform participants that the study is being performed on behalf of an IoT manufacturer whose name will not be revealed for anonymity requirements. We further informed them that the IoT manufacturer is planning to offer data management plans along with their IoT devices, and the study aims to evaluate those data management plans. As examples of the IoT devices that the manufacturer is offering, we selected an indoor smart home security camera as the high risk device (for the HR group) and a smart lightbulb with motion sensor as the low risk device (for the LR group) based on prior studies that looked at device risk perceptions [36].

In addition, we showed participants images of the IoT devices as our group manipulation. The images were collected from Amazon product pages and edited out to remove any brand names (presented in the Appendix). Once the data collection was completed, we debriefed participants about the deception used in the study. Our university's Institutional Review Board (IRB) reviewed and approved this deception.

To select the device purchase price, we performed a market analysis on Amazon to determine the prices for our selected IoT devices. We observed that, with frequent discounts available, the average price for similar IoT devices ranges from $20 (USD) to $40 (USD). As such, we selected our study's IoT devices to be $30 (USD) as the purchase price. The prices for both devices (i.e., indoor camera and smart lightbulb) were set at $30 (USD) to avoid any possible confounding effect.

3.2 The Basic and The Premium Data Management Plans

To examine users' WTP for the premium plan, we informed participants that the IoT manufacturer of the study is planning to offer two variants of the data management plan, where the basic plan will be included in the purchase price. However, the premium option requires a yearly subscription fee. We informed participants that this study aimed to develop a realistic price point for the premium data management plan. As subscription-based plans are frequently used in the industry, we refrain from asking for a one-time fee for the plan to make it realistic. In addition, to minimize participants' cognitive burden, we selected the yearly subscription option instead of the monthly subscription.

To enable users to compare the basic and the premium plans and see what features are included in each plan, we showed them a side-by-side comparison chart of the two plans (Figure 1). We used the template for the comparison from the Blink Subscription Plan [1]. Blink is a popular IoT manufacturer that offers IoT devices such as video doorbells and indoor security cameras, and is owned by Amazon [2]. As the design of the comparison charts and the use of color/icons can impact users' decisions, which is not the focus of this study, we decided to use the template used in the industry.

3.3 Variables in the Study

3.3.1 Technical Literacy. We used Kang et al.'s Technical Knowledge of Privacy Tools Scale (TKPTS) to measure participants' technical literacy [23]. Kang et al.'s work validated the scale using a combination of datasets collected from both online and in-person setups [23]. The scale contains six true/false questions to evaluate participants' technical literacy that avoids self-reporting participants' own technical literacy. Based on the answers to the questionnaire, a participant can get a score ranging from 0 to 6. We used participants' scores as a linear scale variable in our analysis.

3.3.2 Trust perceptions towards IoT manufacturers. We used McKnight et al.'s Technology Trusting Belief (TTB) scale to measure participants' trust in the average IoT manufacturer. McKnight's work conceptualizes three dimensions of trust: *Integrity* - trustee's honesty in keeping promises to the trustor; *Competence* - Trustee's ability to do what the trustor needs; and *Benevolence* - trustor's belief on trustee's motivation and care to act on trustor's interest [31]. As trust is a crucial factor in privacy perception and decision-making, the scale is extensively used in prior works concerning users' privacy behavior [13, 25, 50]. As such, we used this scale to see how trust perceptions toward IoT manufacturers impacts users' WTP for privacy in the IoT purchase scenario. We used a 7-point Likert scale (Strongly disagree to Strongly agree) to measure participants' trust perceptions toward IoT manufacturers.

3.3.3 Willingness to Pay for Privacy. To measure users' willingness to pay for the premium data management plan, we used Van Westendorp's Price Sensitivity Meter [51]. The questionnaire consists of users' responses to the four price points to determine the optimal price for the product of interest. The four price points the questionnaire is concerned with are as follows: (i) a price that is perceived to

[1] https://www.amazon.com/dp/B08JHG867P
[2] https://blinkforhome.com/about-us

Features	Basic data management plan (free and included with the device price)	Premium data management plan (purchased separately)
Cloud data management: • Automatic cloud data backup • Free cloud storage of 2 TB • View and download cloud data from anywhere	✓	✓
Control over cloud data: • Option to delete data stored in the cloud		✓
Control over data sharing: • Option to opt-out from third-party data sharing by the IoT manufacturer		✓
Control over data usage: • Option to limit the IoT manufacturer from using collected data for any purposes other than for the purpose of device functionality		✓

Figure 1: Basic and premium data management plan comparison chart displayed in the study.

be "too cheap" where users would not consider buying it as it would question the quality of the product, (ii) a price that is perceived as "cheap" enough for users to consider the price to be a bargain, (iii) a price that is perceived to be "expensive" where users may still consider buying the product, (iv) a price that is perceived to be "too expensive" for users to consider buying the product. In this study, we asked participants in each group to indicate these four price points for the yearly subscription fee of the premium data management plan for the $30 IoT device associated with each group. We gave users these reference points to perform comparisons of the manipulations we introduced in the study.

In the optimal price point calculation, all these four price points are used to determine the optimal price of the product [29]. For our study, we considered participants' answers to all four price points as our reference to compare participants' WTP for the premium data management plan we introduced in the study. As such, a participant p1 giving a higher price valuation for the "too cheap", "cheap", "expensive", and "too expensive" points than another participant p2 would mean that p1's WTP for the premium plan is higher than p2. We refrain from averaging the four price points to get a single price point per participant as the price points are not envisioned as such in the original questionnaire and were not used to get an optimal price point for each different respondent. Instead, all participants' price points and data are used to generate an optimal price point for the product of interest [29, 40].

3.3.4 Understandability of Privacy Features. To evaluate users' understandability of all four features included in the premium data management plan, we asked participants to rate statements related to the features as either true or false. To enable participants to use their intuition while rating the statements, we did not include the option "I am not sure". Adding this option might make participants overly cautious with their answers, while their intuition might say otherwise (either correctly or wrongfully). To evaluate their understandability, we asked participants to rate 20 true/false statements across the four features. The ratio of correct/incorrect statements was set to 1. Meaning, even if a participant rated all 20 statements as true, they would score 10. As we have four features in the data management plan, we presented the features randomly to each participant and presented the statements randomly for each feature. We consider the combined score across all four features as their understandability score and use it as a linear variable in our analysis.

3.4 Participant Recruitment

We recruited participants from Amazon Mechanical Turk (MTurk) platform for this study. Per our eligibility criteria, participants must be at least 18 years or older, currently living in the United States, and proficient English speakers. In addition, participants were required to be familiar with smart home IoT devices to be eligible for the study. The study focused on IoT devices and their perception of privacy, so familiarity with IoT was crucial.

Participants were also asked whether and what IoT devices they use in their households to understand the popular IoT devices that are most commonly used. They were also asked what IoT devices they would like to purchase in the future (if any). However, these questions were not counted as the eligibility criteria, instead helped us understand the state of IoT usage to date.

Recently, Mturk has received criticism for data quality [46]. Keeping the criticisms of the MTurk platform in mind, we have taken extensive measures to maintain the quality of the response. First, we included multiple choice and text-based attention checks based on recent recommendations for study in MTurk [46]. Second, we recruited MTurk workers who completed at least 1000 Human Intelligent Tasks (HITs) with a HIT approval rate of 95% following recommendations from prior research [48]. Third, we took leverage of the Qualtrics Bot Detection feature and removed responses

from the analysis that Qualtrics flagged as either bot or duplicate. Fourth, we introduced five attention check questions related to the features in the data management plans, and participants had to complete all of the answers correctly to proceed to the next steps and eventually complete the survey. Fifth, based on our manipulations related to the IoT device type and the device's price, participants had to answer what device they were assigned to and what the price of the assigned device was while answering the price points for the premium data management plan. Finally, to restrict ineligible participants from attempting multiple times to figure out the prescreening criteria, we asked participants to report their MTurk worker ID at the beginning of the survey and maintained a database of these IDs to cross-verify multiple attempts.

3.5 Survey Flow

Once participants consented to the survey, they went through our prescreening criteria. If a participant was found ineligible, they could not proceed to the main survey and were notified accordingly.

Eligible participants answered the Technical Knowledge of Privacy Tools Scale (TKPTS) and Technology Trusting Belief (TTB) questionnaires first. After that, participants were introduced to the data management plans and asked five attention check questions related to which features belong to which plans. Participants had to correctly answer these five questions to proceed to the next part of the survey. Next, as part of our manipulation, participants in the high-risk (HR) group were mentioned that the data management plan was for the smart home security camera, and in the low-risk (LR) group participants were informed that the plan is for a smart lightbulb with motion sensor.

To increase realism and communicate the purpose of the IoT device, we asked participants to imagine that there were reports of several recent break-ins in their neighborhood, and they made plans to buy the $30 IoT device (Indoor smart home security camera in the HR group and the Smart lightbulbs with motion sensor in the LR group) to monitor the inside of their home. To help participants imagine the product, we showed the picture of the devices where we edited out the brand and manufacturer information. In the HR group, participants were informed that the smart camera can automatically record videos and send notifications to the participants' phones when it detects movement. In the LR group, we informed participants that the lightbulb can automatically turn on and send notifications to their phones when it detects movement.

After the manipulation, participants answered the Price Sensitivity Meter questions for the yearly subscription fee of the premium plan. In the next phase, participants had to answer the manipulation check question related to what device and the price of the device they were asked to imagine.

Next, participants were prompted with the understandability statements for the four features of the premium data management plan. Here, the four features and the understandability statements were presented randomly for each participant to reduce any ordering bias. Each participant answered all of the understandability questions.

Next, participants rated and explained their perceived trustworthiness towards the survey's unnamed IoT manufacturer. Finally, they answered the demographic questionnaire, which concluded the survey.

We randomized the scale items for all the scales to avoid any possible ordering bias. In addition, we put three attention check questions (in the form, "Please select 'Somewhat disagree' for this statement") and filtered out the responses that failed any of these attention checks. After the data collection, we debriefed participants about the deception used in the survey. The survey questionnaire can be accessed using the link in the Appendix A.1.

The survey took approximately 20 minutes to complete (M = 19.74, Mdn = 15.83, SD = 13.46). Each eligible participant was compensated $4 for participation ($12/hour rate). The survey was approved by the university Institutional Review Board (IRB) and was hosted on the university's Qualtrics server.

3.6 Survey Data Analysis

We recorded a total of 272 complete responses. Among them, 15 participants failed at least one of three attention check questions, 8 responses were tagged as bot/duplicate by Qualtrics Bot Detection, 12 responded in less than five minutes, and 90 failed the manipulation check. In total, we remove 113 responses, leaving 159 valid responses for the analysis (87 participants in the HR group and 72 in the LR group). To detect a medium effect size with an expected Power of 0.8 (guided by prior works in the domain of usable privacy [6, 26, 37, 53]), the minimum sample size needed for our analysis (i.e., comparison of means (two groups), multiple linear regression) was 148. Based on this calculation, our sample size of 159 was deemed sufficient for the analysis. We used G*Power for the power analysis [19]. Quantitative analysis was performed using SPSS. In addition, we used the PROCESS macro of SPSS [1, 21] for any mediation analysis. As our dependent variable WTP has four price points, we used Bonferroni corrected $\alpha = 0.0125$ to indicate significance for the tests concerning WTP. For the rest, significance was measured for $\alpha = 0.05$.

For qualitative analysis of participants' open-ended responses, we undertook a content analysis-based approach [42]. The first author independently reviewed the comments for each question to generate the codebook. Another researcher then coded the comments using the codebook independently. Both coders met to resolve any disagreements and updated their codes accordingly.

4 RESULTS

Among the 159 valid responses, there were 110 (69.2%) male and 49 (30.8%) female participants. Participants' age ranged from 22 to 73 years ($M = 37.14, SD = 10.87$).

Chi-squared test showed that there was no significant differences across the groups regarding participants' gender ($\chi^2(1) = 0.004, p = 0.95$). In addition, the Mann-Whitney U test showed that the groups were similar in terms of participants' age distribution ($U = 3458.5, p = 0.247$). Hence, we concluded that groups were similar regarding participants' demographics. However, we noted that our participant distribution was skewed towards male participants, where 69.2% of the total participants were males. Group-wise demographic breakdown of participants is presented in Table 2 in the Appendix.

4.1 Participants' Understandability of the Data Management Plan Features.

Participants' understandability score was measured by asking twenty true/false understandability statements across the four premium plan features. Each statement corresponds to a score of one towards the overall understandability score.

There were six statements for the *cloud data management* feature, contributing to a score of 6 towards the overall understandability score. Participants' mean understandability score was 4.53 out of 6 for this feature ($M = 4.53, Mdn = 5, SD = 1.25$).

There were four understandability statements for the *control over cloud data deletion* feature, contributing to a score of 4 towards the overall understandability score. Participants' reported mean score was 2.25 out of 4 ($M = 2.25, Mdn = 2, SD = 1.28$).

There were five statements for the *control over data sharing* feature, contributing to a score of 5 towards the overall understandability score. Participants' reported mean score was 2.92 out of 5 ($M = 2.92, Mdn = 3, SD = 1.31$).

Finally, there were five statements for *control over data usage* feature, contributing to a score of 5 towards the overall understandability score. Participants' reported mean score was 2.86 out of 5 ($M = 2.86, Mdn = 3, SD = 1.33$).

After combining the understandability of all four features, we found that participants' mean understandability score was 12.56 out of 20. The minimum score was 3 out of 20, and the maximum was 20 out of 20 ($M = 12.56, Mdn = 11, SD = 4.01$). We used the combined score as participants' understandability of the data management features score for our analysis. Mann-Whitney U test showed that groups were similar in terms of participants' understandability scores (HR: $M = 12.7, Mdn = 11.0, SD = 4.13$; LR: $M = 12.39, Mdn = 11.0, SD = 3.87$) ($U = 2995, p = 0.63$)

4.2 Effect of Device Risk Perception on WTP for Premium Data Management Plan (RQ1)

To examine whether our manipulation was successful, we asked participants in both groups to indicate their perception of the sensitivity of the data collected by the IoT device assigned to the group (i.e., indoor smart security camera in the HR group and smart lightbulb with motion sensor in the LR group). Our results indicated that participants in the HR group attributed higher data sensitivity scores ($M = 7.93, Mdn = 8.0, SD = 1.64$) compared to participants in the LR group ($M = 6.81, Mdn = 7.0, SD = 2.31$), which was significant ($U = 2260, p = 0.002$). Hence, our manipulation of the device data risk perceptions was successful.

Given the option to choose from the basic data management plan that is free and included with the device price and a premium data management plan that requires an additional fee, we hypothesized that participants in the HR group would be willing to choose the premium data management plans at a higher rate compared to the participants in the LR group. However, we noted that 68/87 (78.2%) participants in the HR group and 59/72 (81.9%) participants in the LR group indicated somewhat to strong likelihood of choosing the premium data management plan over the basic plan. The groups were not significantly different in their likelihood of choosing the premium data management plan (HR: $M = 3.91, Mdn = 4.0, SD = 1.16$; LR: $M = 4.0, Mdn = 4.0, SD = 1.10$) ($U = 3249.5, p = 0.662$). Hence, H1a was not supported. This result suggests that, even though participants self-reported a higher overall likelihood of choosing the premium data management plan over the basic plan given the option, the risk perception of the IoT device did not impact this likelihood. (**Finding 1**).

We expected participants' WTP for the premium plan to be higher in the HR group than in the LR group. We performed Mann-Whitney U tests to examine the group differences observing a difference in variance between the HR and the LR groups. Mann-Whitney U tests across the groups showed that, even though participants indicated higher WTP for the premium plan in the HR group than in the LR group, the differences in mentioned price across all four price points were not statistically significant (too cheap: (HR: $M = 23.91, Mdn = 20.0, SD = 30.21$; LR: $M = 20.46, Mdn = 20.0, SD = 11.34$) ($U = 3183.5, p = 0.757$) | cheap: (HR: $M = 33.62, Mdn = 25.0, SD = 39.49$; LR: $M = 26.57, Mdn = 25.0, SD = 17.34$) ($U = 2992.5, p = 0.626$) | expensive: (HR: $M = 47.5, Mdn = 30.0, SD = 50.06$; LR: $M = 39.28, Mdn = 30.0, SD = 30.57$) ($U = 2889.5, p = 0.396$) | too expensive: (HR: $M = 73.37, Mdn = 35.0, SD = 96.49$; LR: $M = 51.57, Mdn = 35.0, SD = 49.9$) ($U = 2667.5, p = 0.106$)). Hence, H1b was also not supported. Figure 3 in the Appendix shows participants' WTP for the premium plan for the four price points across both groups. This finding suggests that users' WTP for the premium plan may not be significantly affected by the risk perceptions of the IoT device. (**Finding 2**).

4.3 Impact of Technical Literacy and Users' Understandability of Data Management Features on WTP for Premium Plan (RQ2)

We performed a mediation analysis to test our hypothesis on the relationship between technical literacy, understandability, and WTP of the premium plan. The detailed model statistics are presented in Table 3 in the Appendix. Our analysis shows that technical literacy significantly and positively impacts users' understandability of the premium plan ($coeff = 0.7904, p = 0.0018$).

We noticed that, for price point "too cheap" and "cheap", the models with predictors of understandability and technical literacy were not significant (too cheap: $p = 0.13$; cheap: $p = 0.37$). Hence, no mediation was noted for these two price points. However, the models were found significant for the price points "expensive" and "too expensive" (expensive: $p = 0.0006$, too expensive: $p = 0.0001$), having understandability as the only significant predictor (expensive: ($coeff = 2.749, p = 0.0012$) | too expensive: ($coeff = 6.069, p = 0.0001$))

Looking at the direct and indirect effects of the model for the "expensive" price point, we noted that the direct effect of technical literacy on WTP (expensive) for data management was not significant ($coeff = 3.377, p = 0.208$). However, the indirect effect via understandability was significant ($coeff = 2.173, CI_{95\%} = [0.36, 4.73]$). These interactions indicated a full mediation of the variable understandability on the relationship between technical literacy and WTP's "expensive" price point.

Again, for the "too expensive" price point, technical literacy's direct effect on WTP was not significant ($coeff = 4.711, p = 0.342$). However, the indirect effect via understandability was noted as significant ($coeff = 4.797, CI_{95\%} = [1.03, 9.83]$), indicating another

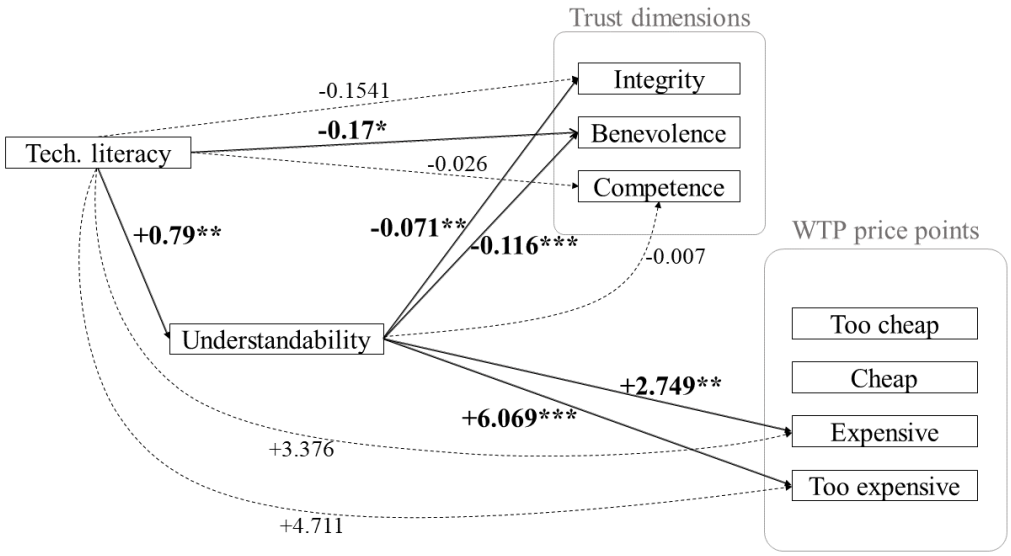

Figure 2: Solid lines indicate significant paths from the mediation analysis. Dotted lines indicate non-significant paths. The detailed statistics of all the regression analysis are presented in the Appendix. *** p < 0.001; ** p < 0.01; * p < 0.05.

full mediation for this price point. Hence, our hypotheses H2a and H2b were partially supported.

Thus, our results suggest that technical literacy positively impacts users' understandability of the data management features. It further positively affects users' willingness to pay for premium data management at higher price points (i.e., "expensive" and "too expensive"). (**Finding 3**).

4.4 Effect of Technical Literacy and Understandability of Data Management Features on Users' Trust towards IoT Manufacturer. (RQ3)

Overall, participants reported higher integrity ($M = 5.35, Mdn = 5.67, SD = 1.25$), competence ($M = 5.54, Mdn = 5.67, SD = 1.11$), and benevolence ($M = 5.2, Mdn = 5.33, SD = 1.27$) perceptions towards the IoT manufacturers, indicating that users hold high trust perceptions towards IoT manufacturers in general.

For the model with integrity, understandability was the only significant predictor ($coeff = -0.071, p = 0.0041$). Mediation analysis showed that the direct effect of technical literacy on integrity perception was not significant ($coeff = -0.1549, p = 0.052$). In contrast, the indirect effect through understandability was significant ($coeff = -0.0564, CI_{95\%} = [-.1122, -.0112]$), indicating a full mediation of the understandability score on the target relationship. The direction of effect indicates that higher understandability of data management features lowers users' integrity perceptions towards IoT manufacturers. Hence, our hypotheses H3a and H3b were supported. These findings indicate that higher technical literacy negatively affects users' integrity perceptions towards IoT manufacturers, mediated by the understandability of the data management features. (**Finding 4**).

Similarly, For the model with benevolence, both technical literacy ($coeff = -0.1698, p = 0.0257$) and understandability ($coeff = -0.1164, p < 0.001$) was significant predictor ($coeff = -0.071, p = 0.0041$), hence, observed both a direct effect of technical literacy and an indirect effect through understandability ($coeff = -0.092, CI_{95\%} = [-.1628, -.0271]$). These interactions indicate a partial mediation of understandability score on the relationship between technical literacy and benevolence perceptions of IoT manufacturers. Hence, our hypotheses H4a and H4b were supported. In summary, technical literacy negatively impacted participants' benevolence perception of IoT manufacturers, mediated by their understandability of data management features. (**Finding 5**). The detailed model statistics of the analysis are presented in Table 4 in the Appendix.

In addition, we generated four regression models for the four price points of the premium plan. In the model, we included six predictors: understandability score, integrity, benevolence, and competence perceptions. We further added participants' age and gender (categorical variable, dummy coded for male vs. female comparisons) as demographic variables. The detailed model statistics are presented in Table 5 in the Appendix.

Consistent with the mediation analysis earlier, the understandability score was the only predictor for the price points "expensive" and "too expensive". Users' integrity, benevolence, and competence perceptions of the IoT manufacturers were not found as significant predictors for any of the four price points. Hence, H5 was not supported. We concluded that IoT manufacturers' integrity, competence, and benevolence did not affect users' WTP for the premium data management plan. (**Finding 6**).

Hypothesis	Statement	Finding
H1a	The likelihood of choosing the premium data management plan will be significantly higher in the HR group compared to the LR group.	Not Supported
H1b	Participants in the HR group will indicate significantly higher WTP for the premium plan (all four price points) compared to the participants in the LR group.	Not Supported
H2a	Users' understandability of the data management features will positively impact their WTP for the premium plan (all four price points).	**Partially supported**
H2b	The relationship between users' technical literacy and their WTP for the data management plan (all four price points) will be mediated by users' understandability of the data management features.	**Partially supported**
H3a	Users' technical literacy will impact users' integrity perception towards IoT manufacturers negatively.	**Supported**
H3b	The relationship between users' technical literacy and integrity perception towards IoT manufacturers will be mediated by users' understandability of the data management features.	**Supported**
H4a	Users' technical literacy will impact users' benevolence perception towards IoT manufacturers negatively.	**Supported**
H4b	The relationship between users' technical literacy and benevolence perception towards IoT manufacturers will be mediated by users' understandability of the data management features.	**Supported**
H5	Users' trust perceptions will negatively impact their WTP for the premium plan (all four price points).	Not Supported

Table 1: Summary of the tested hypotheses and their findings.

4.5 Does Offering Data Management Controls Impact IoT Manufacturers' Perceived Trustworthiness? (RQ4)

We measured users' integrity, benevolence, and competence perceptions towards IoT manufacturers using McKnight et al.'s Technology Trusting Belief scale [31] and reported our findings related to these trust constructs in Section 4.4.

Additionally, based on prior findings that noted that offering privacy features can make a service provider appear more trustworthy [54], we wanted to investigate whether offering the premium data management plan, even if it costs money, would increase users' overall trust perception towards our survey's hypothetical IoT manufacturer compared to other vendors. Towards that, we asked participants, solely based on their interaction with the survey and the survey questionnaire, whether they would feel the study's IoT manufacturer to be more or less trustworthy compared to other IoT manufacturers and why.

Among 159 respondents, 94 participants (59.1%) indicated that they found the survey's IoT manufacturer somewhat to much more trustworthy than average IoT manufacturers. 49 out of 87 (56.23%) participants in the HR group and 45 out of 72 (62.5%) participants in the LR group indicated that they found the concerned manufacturer more trustworthy. The most commonly mentioned reason was the offering of data management features that helped perceive the IoT manufacturer as more trustworthy. For example, P57 and P159 commented respectively:

"They offer plans that give you more control over data usage and storage, which I appreciate."

"It offers a lot of options for privacy. I would have to trust the manufacturer because of this offering."

In contrast, only 25/159 participants (15.72%) across all groups indicated the survey's IoT manufacturer to be somewhat to much less trustworthy (HR group: 13/87 (14.94%); LR group: 12/72 (16.67%)). The rest (40/159, 25.15%) indicated that they would put about the same level of trust in the study's IoT manufacturer. As a reason to put less trust in the survey's IoT manufacturer, P51 mentioned not appreciating data management options, such as cloud deletion requiring a fee.

"The fact that the manufacturer would block essential things such as being able to delete data from the cloud behind a paywall makes me view them as much less trustworthy. I do not trust a company that blocks basic features behind a paywall."

These findings suggest that offering privacy options, even with a fee, can help improve IoT manufacturers' perceived trustworthiness. (**Finding 7**).

4.6 Yearly Subscription Fee for the Premium Data Management Plan

Using Van Westendorp's Price Sensitivity Meter [51], we calculated the optimal yearly subscription fee of our hypothetical premium data management plan in each group. Our analysis revealed that the optimal yearly subscription fee of the premium plan for the indoor smart home security camera was $30 (USD). Comparatively, the optimal yearly subscription fee of the premium plan for the smart lightbulb with motion sensor was found to be $25 (USD). Hence, in both groups, the optimal WTP for the premium plan was, at most, the purchase price of the IoT device. (**Finding 8**).

Van Westendorp's plots are presented in Figure 4 in the Appendix.

5 DISCUSSION

This study investigated the factors that affect users' WTP for a premium data management plan offered for an additional yearly subscription fee. The implications of our findings are discussed below.

5.1 Technical Literacy and Understandability is Important for Informed Privacy Decision-Making

Participants in our study reported a mean understandability score of 12.56 out of 20, with a standard deviation of 4.01. While no prior

efforts attempted to measure the understandability of privacy features, prior works noted that consumers often have misconceptions about the implications of privacy terms and features [14, 16], implying that, even if a privacy feature is known to a consumer, the underlying implications of such a feature towards privacy and data protection may not be easily understood by the end-users.

Our findings confirm that understandability of the data management features is crucial for users' WTP for the premium data management plan, suggesting the variable's important role in privacy decision-making. Our results further suggest that merely making privacy information readily available does not necessarily mean users will be able to make informed privacy decisions unless they can understand the implications of the provided privacy information. This is in line with prior work that showed that, when users were provided with labels for IoT devices, only users who can understand the features included in the labels indicated higher WTP towards devices with better privacy practices [15].

We also found that understandability of the premium plan features mediated the relationship between users' technical literacy and their WTP for the premium plan for two of the four price points examined. This underscores the importance of developing users' technical literacy, which can impact their willingness to pay a price for a data management plan by affecting their ability to understand the implications of the data management features. Hence, designing privacy labels and features should consider users' technical literacy level instead of mindlessly assuming that all consumers will be able to understand privacy-related constructs equally. Researchers should look into effective ways to educate consumers with standard privacy-related terms, construct, and attributes to enable them to make informed privacy decisions independently.

5.2 Implications of Understandability of privacy features for Users' Trust Perceptions

We noticed that users' technical literacy negatively impacted their perception of integrity and benevolence, mediated by the understandability of the data management features. As trust is vital in any provider-consumer relationship [5], our findings imply that it might be of (malicious) interest for the IoT manufacturers to make privacy-related information either not readily available or too obscure for consumers to understand as a mechanism to retain users' trust. Prior efforts confirmed IoT manufacturers' tendency to keep IoT devices' privacy practices unavailable at the purchase time [17], leading consumers to underestimate the invasiveness of the device manufacturers' privacy practices, even for the devices with relatively poor practices [15].

In our study, participants perceived the survey's IoT manufacturer as comparatively more trustworthy than average IoT manufacturers. Qualitative comments suggest that offering the data management plan, even with a fee, positively influences users' trust perceptions of the IoT manufacturer. This finding, combined with the identified effect of understandability on trust perceptions, implies that, from the manufacturers' point of view, it might be in their best interest to offer privacy options that are limited/ineffective in restricting themselves from using the collected data, which can mislead users in terms of overestimating their degree of control over shared data and help build trust. This is further supported by prior efforts indicating that offering privacy options can be manipulative in terms of misleading users towards practices which is beneficial for service providers' data collection while helping to build trust [2, 18, 44].

Given the above concerns, legislators should ensure that IoT manufacturers cannot take advantage of the users by offering ineffective data management plans that do not satisfy the core data privacy requirements. Further, regulations should force IoT manufacturers to make salient privacy information readily available at device purchase time that is easy to understand and empower consumers to make informed purchase decisions considering their privacy preferences. A viable way to ensure the availability of information related to device privacy practices can be requiring IoT manufacturers to provide privacy labels as suggested in prior efforts [16, 34], at the same time educating users about the privacy attributes and their underlying implications in terms of data privacy protections.

5.3 Incentivizing and Guiding IoT Manufacturers towards Offering Control over Data Privacy

Prior work noted that there is not enough incentive for the IoT manufacturers to inform of their privacy practices as consumers tend to underestimate the invasiveness of IoT devices' privacy preferences when such information is not available at the time of purchase [15]. However, investigating users' WTP for a premium data management plan, we noticed that there might be an incentive to offer such a data management plan for an additional fee. Our results showed that consumers are willing to purchase a data management plan to better control their data privacy preferences. Importantly, our results suggest that offering data management options can work as a trust-building strategy, which IoT manufacturers can leverage to earn consumer trust that may, in turn, help increase the adoption of their IoT products.

While offering data management options can help build trust, as discussed above, IoT manufacturers need to be cautious while determining the monetary price of the offered data management plans. In this study, we noticed that, despite indicating interest in paying a premium for the data management plan, users' self-reported yearly subscription fee was less than the device price. This is also supported based on prior findings that showed users' reluctance to pay for privacy features [18]. Further, as asking users to pay for their privacy can hurt trust perceptions for some consumers as well, IoT manufacturers should be careful in choosing the features to be included in the data management plan that is not free. We saw evidence of this in participants' comments where they felt that the option to delete cloud data should not require any additional fee, which caused them to rate the study's hypothetical IoT manufacturer as less trustworthy than average IoT manufacturers.

5.4 Limitations of the Study

We took several measures to ensure the study's internal validity and data quality. Nonetheless, reported findings should be interpreted with the following limitations in mind.

First, we used the Amazon MTurk platform to recruit our study participants who are adults living in the United States. Our participants have the technical ability to use MTurk, which may differ from a general representative population of the United States.

Second, we measured participants' willingness to pay for the hypothetical premium data management plan based on self-reported data. Prior works noted that self-reported data can differ from actual behavior due to hypothetical bias [3, 20], and users' actual WTP can be lower than the hypothetical WTP [35]. Hence, it is possible that our participants might have indicated an overvaluation of their WTP for the premium plan. However, as the primary focus of our study was to investigate factors that affect users' WTP for a premium data management plan and was not to evaluate the optimal WTP for such a premium plan, we believe that self-reported WTP serves the purpose of our study adequately.

Third, the features used in our study as part of the premium data management plan are extracted based on prior research investigating users' expectations regarding IoT device data management in the United States [16, 17]. Therefore, consumers from different geographic locations (e.g., Europe, Asia), subject to different privacy regulations and norms, may have different privacy expectations, and thus may exhibit different attitudes towards the premium plan. For example, manufacturers under GDPR may be required to include some or all of the premium plan features as part of the device price, and this can cause consumers from the EU countries to be unwilling or less willing to pay for such a premium plan if asked. Hence, our findings may not apply to IoT consumers bound to different privacy regulations compared to the United States.

Finally, to keep the study tractable and not overwhelm users with all possible privacy features that might be included in the hypothetical data management plan, we only included four features based on users' privacy exceptions from IoT devices, guided by prior research [16, 17]. As such, WTP may vary based on different data management features, and should be investigated in future efforts.

6 CONCLUSION

In this work, we focused on investigating the factors that affect users' willingness to pay for a premium data management plan offered separately for an additional subscription fee. Our result confirms that users' willingness to pay for premium data management plan is affected by their technical literacy and their understandability of the offered data management plan's features. Furthermore, our work indicates that the understandability of data management features can affect users' trust perceptions toward IoT manufacturers. Based on our findings, we outlined strategies for IoT manufacturers to offer privacy options that can work as a trust-building mechanism. Finally, this work elaborates on how privacy offerings can also be used to misguide users towards higher trust, and calls for action from privacy legislators to ensure user privacy in the IoT world.

ACKNOWLEDGMENTS

This research was supported by a NSF CAREER award to the second author, 1750908.

REFERENCES

[1] Soleman Abu-Bader and Tiffanie Victoria Jones. 2021. Statistical mediation analysis using the sobel test and hayes SPSS process macro. *International Journal of Quantitative and Qualitative Research Methods* (2021).
[2] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514.
[3] Frode Alfnes, Kyrre Rickertsen, et al. 2011. Non-market valuation: experimental methods. *The Oxford handbook of the economics of food consumption and policy* 215 (2011), 242.
[4] Gabe Turner Aliza Vigderman. 2022. The Data Big Tech Companies Have On You. (2022). https://www.security.org/resources/data-tech-companies-have/
[5] Angelo Antoci, Laura Bonelli, Fabio Paglieri, Tommaso Reggiani, and Fabio Sabatini. 2019. Civility and trust in social media. *Journal of Economic Behavior & Organization* 160 (2019), 83–99.
[6] Mehrdad Bahrini, Nima Zargham, Alexander Wolff, Dennis-Kenji Kipker, Karsten Sohr, and Rainer Malaka. 2022. It's Long and Complicated! Enhancing One-Pager Privacy Policies in Smart Home Applications. In *Nordic Human-Computer Interaction Conference*. 1–13.
[7] David G Balash, Xiaoyuan Wu, Miles Grant, Irwin Reyes, and Adam J Aviv. 2021. Security and Privacy Perceptions of Third-Party Application Access for Google Accounts (Extended Version). *arXiv preprint arXiv:2111.03573* (2021).
[8] Lemi Baruh, Ekin Secinti, and Zeynep Cemalcilar. 2017. Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication* 67, 1 (2017), 26–53.
[9] John M Blythe, Shane D Johnson, and Matthew Manning. 2020. What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Science* 9, 1 (2020), 1–9.
[10] Visualcapitalist.com Carmen Ang. 2022. How Do Big Tech Giants Make Their Billions? (2022). https://www.visualcapitalist.com/how-big-tech-makes-their-billions-2022/
[11] Eve M Caudill and Patrick E Murphy. 2000. Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing* 19, 1 (2000), 7–19.
[12] Ralf De Wolf, Koen Willaert, and Jo Pierson. 2014. Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior* 35 (2014), 444–454.
[13] Kenan Degirmenci. 2016. Trust-promoting seals in green information systems: the case of smart meters and privacy. (2016).
[14] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the experts: What should be on an IoT privacy and security label?. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 447–464.
[15] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. [n. d.]. Are Consumers Willing to Pay for Security and Privacy of IoT Devices? ([n. d.]).
[16] 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.
[17] 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*. 1–12.
[18] 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 *USENIX Security Symposium*. 483–500.
[19] Franz Faul, Edgar Erdfelder, Albert-Georg Lang, and Axel Buchner. 2007. G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior research methods* 39, 2 (2007), 175–191.
[20] Glenn W Harrison and E Elisabet Rutström. 2008. Experimental evidence on the existence of hypothetical bias in value elicitation methods. *Handbook of experimental economics results* 1 (2008), 752–767.
[21] Andrew F Hayes, Amanda K Montoya, and Nicholas J Rockwood. 2017. The analysis of mechanisms and their contingencies: PROCESS versus structural equation modeling. *Australasian Marketing Journal* 25, 1 (2017), 76–81.
[22] Nick Ho-Sam-Sooi, Wolter Pieters, and Maarten Kroesen. 2021. Investigating the effect of security and privacy on IoT device purchase behaviour. *computers & security* 102 (2021), 102132.
[23] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User mental models of the internet and implications for privacy and security. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. 39–52.
[24] Jennifer Korn. 2023. Want a free 55-inch TV? The catch: Nonstop ads, less privacy. https://www.cnn.com/2023/05/17/tech/telly-free-television-with-advertisements/index.html.
[25] Hanna Krasnova, Sarah Spiekermann, Ksenia Koroleva, and Thomas Hildebrand. 2010. Online social networks: Why we disclose. *Journal of information technology* 25, 2 (2010), 109–125.

[26] Kiran Kumar, Dapeng Liu, and Lemuria Carter. 2023. Understanding the Adoption of Digital Conferencing Tools: Unpacking the Impact of Privacy Concerns and Incident Response Efficacy. *Computers & Security* (2023), 103375.
[27] Nicole Lindsey. 2019. Smart devices leaking data to tech giants raisesnew IoT privacy issues. (2019). https://www.cpomagazine.com/data-privacy/smart-devices-leaking-data-to-tech-giants-raises-new-iot-privacy-issues/
[28] Emmanuel Elioth Lulandala. 2020. Facebook data breach: a systematic review of its consequences on consumers' behaviour towards advertising. *Strategic System Assurance and Business Analytics* (2020), 45–68.
[29] David W Lyon. 2002. The price is right (or is it?). *Marketing Research* 14, 4 (2002), 8.
[30] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.
[31] D Harrison McKnight, Vivek Choudhury, and Charles Kacmar. 2002. Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research* 13, 3 (2002), 334–359.
[32] Miriam J Metzger. 2006. Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research* 33, 3 (2006), 155–179.
[33] Carrie Mihalcik. 2021. Apple HomePod mini reportedly has a secret sensor for temperature, humidity. (2021). https://www.cnet.com/home/smart-home/apple-homepod-mini-reportedly-has-a-secret-sensor-for-temperature-humidity/
[34] Philipp Morgner, Christoph Mai, Nicole Koschate-Fischer, Felix Freiling, and Zinaida Benenson. 2020. Security update labels: establishing economic incentives for security patching of IoT consumer products. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 429–446.
[35] James J Murphy, P Geoffrey Allen, Thomas H Stevens, and Darryl Weatherhead. 2005. A meta-analysis of hypothetical bias in stated preference valuation. *Environmental and Resource Economics* 30 (2005), 313–325.
[36] 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, 399–412.
[37] Shabnam Najafian, Amra Delic, Marko Tkalcic, and Nava Tintarev. 2021. Factors influencing privacy concern for explanations of group recommendation. In *Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization*. 14–23.
[38] Alfred Ng and Megan Wollerton. 2019. Google calls Nest's hidden microphone an "error". (2019). https://www.cnet.com/news/google-calls-nests-hidden-microphone-an-error/
[39] Kenneth D Nguyen, Heather Rosoff, and Richard S John. 2017. Valuing information security from a phishing attack. *Journal of Cybersecurity* 3, 3 (2017), 159–171.
[40] Oliver Roll, Lars-Hendrik Achterberg, and Karl-Georg Herbert. 2010. Innovative approaches to analyzing the Price Sensitivity Meter: Results of an international comparative study. *Laurea Publications A• 72* (2010), 181.
[41] Brent Rowe and Dallas Wood. 2013. Are home internet users willing to pay ISPs for improvements in cyber security?. In *Economics of information security and privacy III*. Springer, 193–212.
[42] Johnny Saldaña. 2021. The coding manual for qualitative researchers. *The coding manual for qualitative researchers* (2021), 1–440.
[43] Michel Schreiner, Thomas Hess, and Faranak Fathianpour. 2013. On The Willingness To Pay For Privacy As A Freemium Model: First Empirical Evidence.. In *ECIS*. 30.
[44] H Jeff Smith, Tamara Dinev, and Heng Xu. 2011. Information privacy research: an interdisciplinary review. *MIS quarterly* (2011), 989–1015.
[45] Deepesh Kumar Srivastava and Basav Roychoudhury. 2021. Understanding the Factors that Influence Adoption of Privacy Protection Features in Online Social Networks. *Journal of Global Information Technology Management* 24, 3 (2021), 164–182.
[46] Jenny Tang, Eleanor Birrell, and Ada Lerner. 2022. Replication: How well do my results generalize now? The external validity of online privacy and security surveys. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 367–385.
[47] Jennifer Fries Taylor, Jodie Ferguson, and Pamela Scholder Ellen. 2015. From trait to state: Understanding privacy concerns. *Journal of Consumer Marketing* (2015).
[48] Hsin-yi Sandy Tsai, Mengtian Jiang, Saleem Alhabash, Robert LaRose, Nora J Rifon, and Shelia R Cotten. 2016. Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security* 59 (2016), 138–150.
[49] Janice Y Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. The effect of online privacy information on purchasing behavior: An experimental study. *Information systems research* 22, 2 (2011), 254–268.
[50] Ehsan Ul Haque, Mohammad Maifi Hasan Khan, and Md Abdullah Al Fahim. 2023. The Nuanced Nature of Trust and Privacy Control Adoption in the Context of Google. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–23.
[51] Peter H Van Westendorp et al. 1976. NSS Price Sensitivity Meter (PSM)–A new approach to study consumer perception of prices. In *Proceedings of the 29th ESOMAR Congress*, Vol. 139167.
[52] Kaveh Waddell. 2021. Connected devices share more data than needed, study says. (2021). https://www.consumerreports.org/privacy/connected-devices-share-more-data-than-needed-study-says-a7015033345/
[53] Jason Watson, Heather Richter Lipford, and Andrew Besmer. 2015. Mapping user preference to privacy default settings. *ACM Transactions on Computer-Human Interaction (TOCHI)* 22, 6 (2015), 1–20.
[54] Heng Xu, Hock-Hai Teo, and Bernard Tan. 2005. Predicting the adoption of location-based services: the role of trust and perceived privacy risk. (2005).
[55] Tao Zhou. 2011. The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems* (2011).
[56] Moshe Zviran. 2008. User's perspectives on privacy in web-based applications. *Journal of Computer Information Systems* 48, 4 (2008), 97–105.

A APPENDIX

A.1 Survey Instruments

Survey questionnaire for the study can be accessed from https://github.com/ehsan-ashik/WTP-Data-Management-Plan-Study/raw/main/Survey%20Instruments.pdf.

A.2 Demographics Summary

Table 2 shows a group-wise summary of participants' demographics.

A.3 Images of the IoT Devices Used in the Study

Figure 5 presents the edited-out versions of the images of the IoT devices we used in the study. In the HR group, the reference IoT device was an indoor smart home security camera (top), and in the LR group, the reference device was a smart lightbulb with motion sensor (bottom). We edited out all the brand-related information from the images to avoid biasing the participants.

A.4 Van Westendorp Graphs for Optimal Price Point Calculations

Figure 4 shows the Van Westendorp graphs for the HR and the LR groups that indicate the optimal WTP (yearly subscription fee) of the premium data management plan based on participants' answers to the four price points of the Price Sensitivity Meter (PSM). The optimal price point is indicated by the lowest interaction point of the four line graphs representing the four price points of the PSM. In the HR group, the optimal WTP for the premium plan was observed to be about $30 (USD), and in the LR group, this value was observed to be approximately $25. In both groups, the purchase price of the IoT device was mentioned as $30 (USD).

A.5 Regressions Statistics

Detailed statistics for all the mediation and regression analysis performed are presented in Tables 3, 4, and 5.

Metric	Levels	HR Group	LR Group
Age	-	$M = 35.65, Mdn = 32, SD = 9.27$	$M = 38.94, Mdn = 33.5, SD = 12.35$
Gender	Male	60	50
	Female	27	22
	Non-binary	0	0
Education	Less than high school	0	1
	High School graduate or GED	9	0
	Some college	6	3
	2 year degree	1	2
	4 year degree	30	26
	Master's degree	39	37
	Doctoral degree	0	1
	Professional degree	2	2
Income	$1 to $9,999	4	2
	$10,000 to $24,999	5	9
	$25,000 to $49,999	43	21
	$50,000 to $74,999	13	23
	$75,000 to $99,999	19	13
	$100,000 to $149,999	3	1
	$150,000 and greater	0	3
		$N = 87$	$N = 72$

Table 2: Participant demographics by groups.

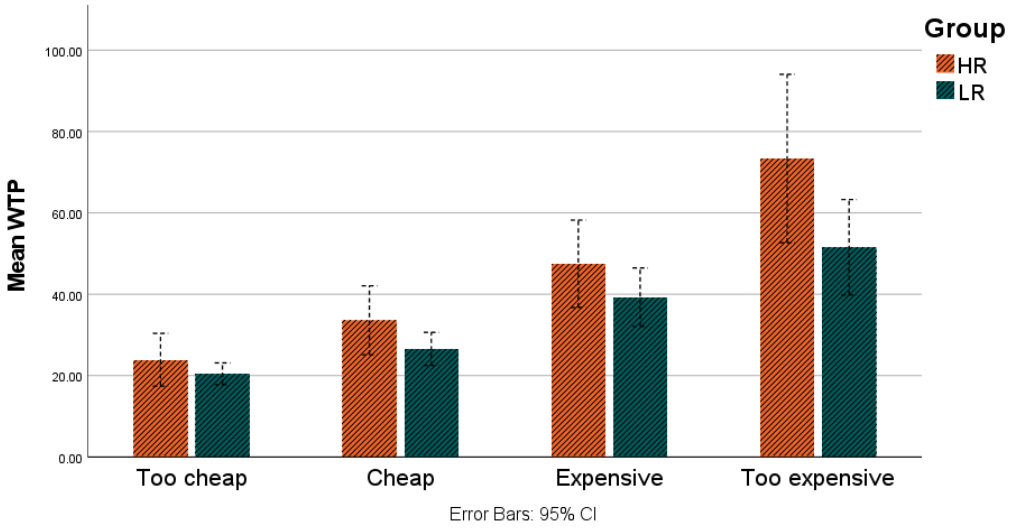

Figure 3: Participants' mean WTP for the premium plan for all four price points across the groups.

OUTCOME VARIABLE: Understandability

Model Summary

R	R-sq	MSE	F	df1	df2	p
.2459	.0605	15.1714	10.1029	1.0000	157.0000	.0018

Model

	coeff	se	t	p	LLCI	ULCI
constant	10.7653	.6435	16.7282	.0000	9.4942	12.0364
Tech. Literacy	.7904	.2487	3.1785	**.0018**	.2992	1.2815

OUTCOME VARIABLE: Too Cheap

Model Summary

R	R-sq	MSE	F	df1	df2	p
.1599	.0256	548.1126	2.0333	2.0000	155.0000	.1344

Model

	coeff	se	t	p	LLCI	ULCI
constant	33.4267	6.4934	5.1478	.0000	20.5997	46.2536
Tech. Literacy	.4439	1.5567	.2851	.7759	-2.6312	3.5189
Understandability	-.9625	.4798	-2.0061	.0466	-1.9102	-.0147

OUTCOME VARIABLE: Cheap

Model Summary

R	R-sq	MSE	F	df1	df2	p
.1125	.0127	986.5938	1.0006	2.0000	156.0000	.3700

Model

	coeff	se	t	p	LLCI	ULCI
constant	23.0190	8.6565	2.6592	.0087	5.9199	40.1180
Tech. Literacy	2.7475	2.0687	1.3281	.1861	-1.3388	6.8338
Understandability	.0937	.6436	.1456	.8844	-1.1776	1.3650

OUTCOME VARIABLE: Expensive

Model Summary

R	R-sq	MSE	F	df1	df2	p
.3011	.0906	1643.9164	7.7746	2.0000	156.0000	.0006

Model

	coeff	se	t	p	LLCI	ULCI
constant	1.5667	11.1741	.1402	.8887	-20.5053	23.6388
Tech. Literacy	3.3763	2.6704	1.2644	.2080	-1.8984	8.6510
Understandability	2.7494	.8308	3.3095	**.0012**	1.1084	4.3904

Total effect of X on Y

Effect	se	t	p	LLCI	ULCI	c_cs
5.5493	2.6692	2.0790	.0392	.2772	10.8214	.1637

Direct effect of X on Y

Effect	se	t	p	LLCI	ULCI	c'_cs
3.3763	2.6704	1.2644	.2080	-1.8984	8.6510	.0996

Indirect effect(s) of X on Y

	Effect	BootSE	BootLLCI	BootULCI
Understandability	2.1730	1.1243	.3581	4.7250

OUTCOME VARIABLE: Too Expensive

Model Summary

R	R-sq	MSE	F	df1	df2	p
.3337	.1114	5622.4725	9.7744	2.0000	156.0000	.0001

Model

	coeff	se	t	p	LLCI	ULCI
constant	-23.5688	20.6650	-1.1405	.2558	-64.3881	17.2506
Tech. Literacy	4.7108	4.9385	.9539	.3416	-5.0442	14.4657
Understandability	6.0690	1.5364	3.9502	**.0001**	3.0342	9.1038

Total effect of X on Y

Effect	se	t	p	LLCI	ULCI	c_cs
9.5075	5.0046	1.8998	.0593	-.3775	19.3924	.1499

Direct effect of X on Y

Effect	se	t	p	LLCI	ULCI	c'_cs
4.7108	4.9385	.9539	.3416	-5.0442	14.4657	.0743

Indirect effect(s) of X on Y

	Effect	BootSE	BootLLCI	BootULCI
Understandability	4.7967	2.2994	1.0334	9.8329

Table 3: Mediation analysis of technical literacy and WTP for data management plan with understandability of the data management features as mediator. Bold values indicate significance with a Bonferroni corrected $\alpha = 0.0125$.

OUTCOME VARIABLE: Understandability

Model Summary

R	R-sq	MSE	F	df1	df2	p
.2459	.0605	15.1714	10.1029	1.0000	157.0000	.0018

Model

	coeff	se	t	p	LLCI	ULCI
constant	10.7653	.6435	16.7282	.0000	9.4942	12.0364
Tech. Literacy	.7904	.2487	3.1785	**.0018**	.2992	1.2815

OUTCOME VARIABLE: Trust Integrity

Model Summary

R	R-sq	MSE	F	df1	df2	p
.3060	.0936	1.4259	8.0559	2.0000	156.0000	.0005

Model

	coeff	se	t	p	LLCI	ULCI
constant	6.5933	.3291	20.0351	.0000	5.9433	7.2434
Tech. Literacy	-.1541	.0786	-1.9590	.0519	-.3094	.0013
Understandability	-.0713	.0245	-2.9142	**.0041**	-.1196	-.0230

Total effect of X on Y

Effect	se	t	p	LLCI	ULCI	c_cs
-.2104	.0780	-2.6967	.0078	-.3645	-.0563	-.2104

Direct effect of X on Y

Effect	se	t	p	LLCI	ULCI	c'_cs
-.1541	.0786	-1.9590	.0519	-.3094	.0013	-.1541

Indirect effect(s) of X on Y

	Effect	BootSE	BootLLCI	BootULCI
Understandability	-.0564	.0258	-.1122	-.0112

OUTCOME VARIABLE: Trust Benevolence

Model Summary

R	R-sq	MSE	F	df1	df2	p
.4402	.1938	1.3094	18.7474	2.0000	156.0000	<.0001

Model

	coeff	se	t	p	LLCI	ULCI
constant	7.0468	.3154	22.3451	.0000	6.4238	7.6697
Tech. Literacy	-.1698	.0754	-2.2525	**.0257**	-.3186	-.0209
Understandability	-.1164	.0234	-4.9653	**.0000**	-.1627	-.0701

Total effect of X on Y

Effect	se	t	p	LLCI	ULCI	c_cs
-.2618	.0784	-3.3406	.0010	-.4165	-.1070	-.2576

Direct effect of X on Y

Effect	se	t	p	LLCI	ULCI	c'_cs
-.1698	.0754	-2.2525	.0257	-.3186	-.0209	-.1671

Indirect effect(s) of X on Y

	Effect	BootSE	BootLLCI	BootULCI
Understandability	-.0920	.0344	-.1628	-.0271

OUTCOME VARIABLE: Trust Competence

Model Summary

R	R-sq	MSE	F	df1	df2	p
.0427	.0018	1.2414	.1424	2.0000	156.0000	.8674

Model

	coeff	se	t	p	LLCI	ULCI
constant	5.6801	.3071	18.4986	.0000	5.0736	6.2866
Tech. Literacy	-.0257	.0734	-.3504	.7265	-.1707	.1192
Understandability	-.0069	.0228	-.3040	.7616	-.0520	.0382

Table 4: Mediation analysis of technical literacy and trust perceptions with understandability of the data management features as mediator. Bold values indicate significance.

OUTCOME VARIABLE: WTP - Too Cheap

Model Summary

R	R-sq	MSE	F	df1	df2	p
.211	.045	648.593	1.176	6.0000	151.0000	.322

Model

	coeff	se	t	p	LLCI	ULCI
constant	35.164	14.059	2.501	.013	7.386	62.942
Trust Integrity	-.594	2.746	-.216	.829	-6.019	4.831
Trust Competence	1.940	2.597	.747	.456	-3.192	7.072
Trust Benevolence	-.044	2.759	-.016	.987	-5.496	5.408
Understandability	-.720	.555	-1.296	.197	-1.817	.378
Gender (Female vs. Male)	-.647	4.319	-.150	.881	-9.180	7.886
Age	-.293	.191	-1.533	.127	-.671	.085

OUTCOME VARIABLE: WTP - Cheap

Model Summary

R	R-sq	MSE	F	df1	df2	p
.159	.025	656.859	.657	6.0000	152.0000	.684

Model

	coeff	se	t	p	LLCI	ULCI
constant	28.014	18.925	1.480	.141	-9.377	65.404
Trust Integrity	-.749	3.696	-.203	.840	-8.051	6.553
Trust Competence	3.428	3.493	.981	.328	-3.474	10.330
Trust Benevolence	-.679	3.714	-.183	.855	-8.018	6.660
Understandability	.543	.748	.727	.468	-.934	2.020
Gender (Female vs. Male)	-.703	5.769	-.122	.903	-12.101	10.695
Age	-.421	.256	-1.641	.103	-.927	.086

OUTCOME VARIABLE: WTP - Expensive

Model Summary

R	R-sq	MSE	F	df1	df2	p
.298	.089	4178.517	2.472	6.0000	152.0000	.026

Model

	coeff	se	t	p	LLCI	ULCI
constant	9.314	24.611	.378	.706	-39.309	57.937
Trust Integrity	-1.199	4.806	-.249	.803	-10.695	8.297
Trust Competence	1.859	4.543	.409	.683	-7.117	10.834
Trust Benevolence	.184	4.830	.038	.970	-9.360	9.727
Understandability	3.222	.972	3.314	**.001**	1.301	5.142
Gender (Female vs. Male)	4.372	7.502	.583	.561	-10.450	19.195
Age	-.328	.333	-.985	.326	-.987	.330

OUTCOME VARIABLE: WTP - Too Expensive

Model Summary

R	R-sq	MSE	F	df1	df2	p
.336	.113	18540.276	3.218	6.0000	152.0000	.005

Model

	coeff	se	t	p	LLCI	ULCI
constant	-5.000	45.436	-.110	.913	-94.768	84.768
Trust Integrity	-.822	8.873	-.093	.926	-18.353	16.709
Trust Competence	2.101	8.387	.251	.802	-14.469	18.672
Trust Benevolence	-1.287	8.918	-.144	.885	-18.905	16.332
Understandability	6.633	1.795	3.696	**<.001**	3.087	10.179
Gender (Female vs. Male)	11.360	13.851	.820	.413	-16.006	38.725
Age	-.512	.615	-.832	.407	-1.727	.704

Table 5: Regression analysis statistics. Bold values indicate significance with a Bonferroni corrected $\alpha = 0.0125$.

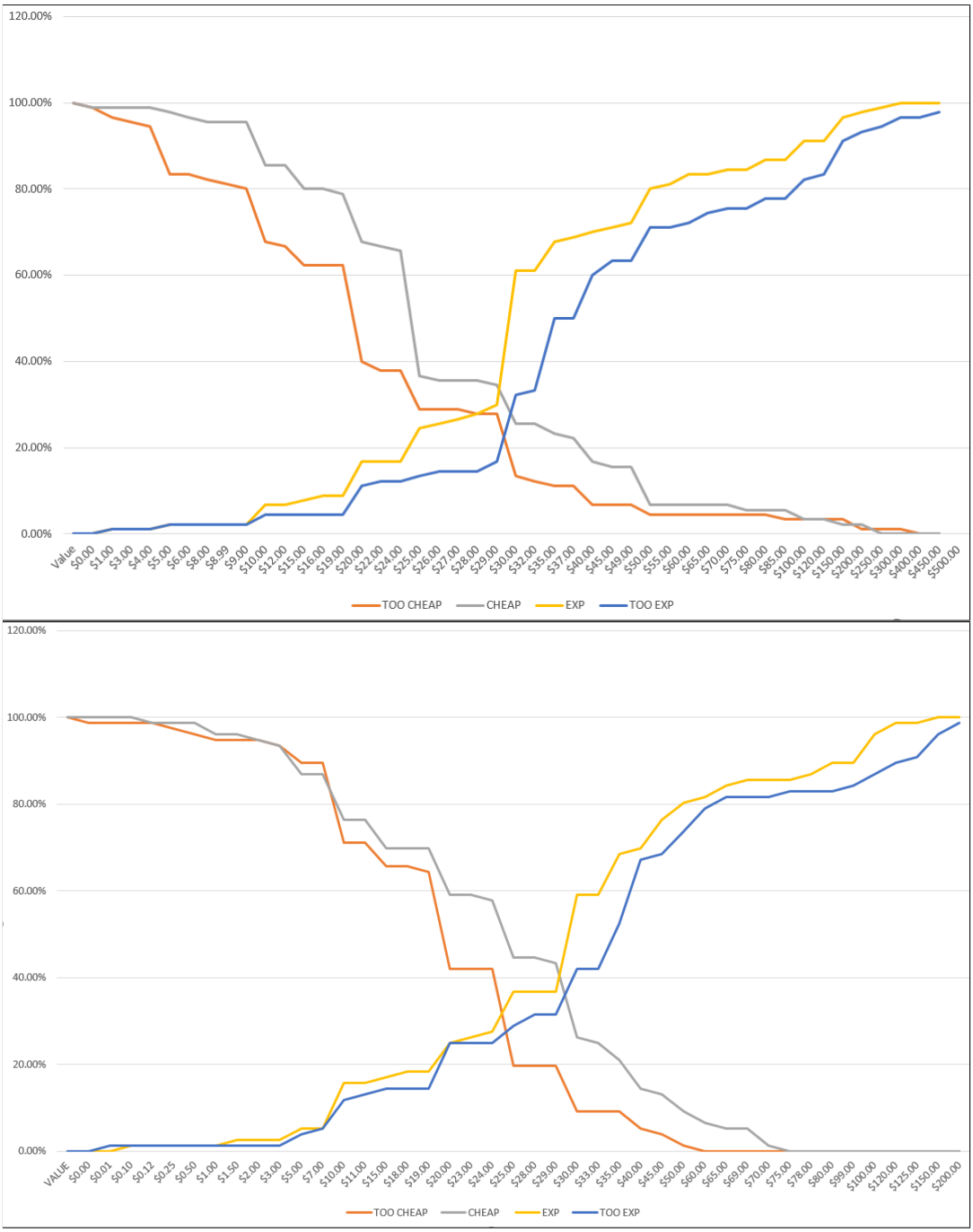

Figure 4: Van Westendorp graphs for calculation optimal yearly subscription fee (WTP) of the premium data management plan for the HR (top) and the LR (bottom) groups.

Figure 5: IoT device images used in the study. Indoor smart-home security camera in the HR group (top) and Smart lightbulb with motion sensor in the LR group (bottom). The brand related information is edited out.