Investigating Users' Decision-making for Data Privacy Controls in the Context of Internet of Things (IoT) Devices Using an Incentive-compatible Lottery Study

Ehsan Ul Haque
School of Computing
University of Connecticut
Storrs, Connecticut, USA
ehsan.ul_haque@uconn.edu

Mohammad Maifi Hasan Khan
School of Computing
University of Connecticut
Storrs, Connecticut, USA
mohammad.khan@uconn.edu

Abstract

While companies are increasingly moving towards the 'pay for privacy' model, it is unclear how consumers make privacy decisions under this model. Toward that, we conducted an incentive-compatible lottery study on Prolific to understand the factors behind users' choice to have additional data privacy controls. With 265 United States participants across two device risk conditions (High-risk: camera vs. Low-risk: light bulb) and three cash conditions ($9.99 vs. $19.99 vs. $29.99), results reveal that device risk and cash offerings influence participants' lottery choice. We further observed an interaction effect between participants' technical literacy and cash option. Specifically, technical participants chose the data privacy controls instead of cash at a higher rate when the cash condition was $29.99. In contrast, less technical participants favored the privacy option at a higher rate when the cash condition was $9.99. Implications of our findings for user data privacy are discussed in the paper.

CCS Concepts

• **Security and privacy** → **Privacy protections**; • **Human-centered computing** → **Empirical studies in HCI**; **User studies**.

Keywords

Privacy, Internet of things, Incentive-compatibility, Willingness to pay for privacy, Premium data privacy controls, IoT device risk perceptions, Monetary trade-off, Technical literacy

ACM Reference Format:
Ehsan Ul Haque and Mohammad Maifi Hasan Khan. 2025. Investigating Users' Decision-making for Data Privacy Controls in the Context of Internet of Things (IoT) Devices Using an Incentive-compatible Lottery Study. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 22 pages. https://doi.org/10.1145/3706598.3713251

CHI '25, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713251

1 Introduction

The explosive growth toward Internet-based services and the Internet of Things (IoT) signifies a fundamental shift towards a new business model centered around user data. Often, the *smartness* of the IoT hinges on the ability to seamlessly collect and analyze user data and usage patterns, enabling intelligent inferences and actions tailored to individual needs [5, 18]. Undoubtedly, smart devices offer convenience and potentially an improved way of life. However, the pervasive practice of collecting and monetizing user data has raised growing concerns over user data privacy among both privacy advocates and end-users [66, 75, 89, 90]. To mitigate privacy concerns and protect personal data, prior research has revealed users' willingness to pay (WTP) for (a) higher privacy and security of the devices [12, 31, 40, 58] and (b) additional data privacy controls that will strengthen their ability to take control of IoT devices' data collection and usage practices [13, 80]. Consumers' keenness towards privacy and their willingness to pay a premium have created a new trend: service providers charging premiums for limiting data collection and usage. One such recent example is tech-giant Meta's announcement of a subscription-based 'pay for privacy' model, where Facebook and Instagram users are offered the option to opt out of data sharing and usage for a fee [32, 76, 88]. While this model is gaining in popularity among tech and IoT manufacturers, these companies often do not provide adequate information regarding their services' data collection and usage practices [31, 80], which makes it difficult for users to assess actual privacy risks and make informed decisions.

Given the varying privacy risks and monetary costs associated with different IoT devices and services, monetary tradeoffs are often a fundamental component of users' privacy decision-making in this context. For instance, when building a smart connected home that brings convenience while respecting data privacy, at the purchase time, users often face a choice between IoT products with better security and privacy features and those that come with lower security and privacy protection. However, the added security and privacy typically come at a premium price compared to less privacy-protective IoT devices, and IoT devices that collect user data for business purposes are likely to be less expensive than those that limit data collection and usage. In this vein, previous studies suggest that the price of IoT devices is a significant factor in users' privacy decisions [12, 31, 58]. Therefore, understanding users' tradeoff calculations between privacy and money is crucial to comprehend how they make privacy decisions when monetary considerations are involved.

Toward understanding users' tradeoff calculations between privacy and money, we replicated the 'pay for privacy' model with two versions of a hypothetical data management plan. Under this model, the *Basic plan* is free and included with the device price and offers data management controls towards cloud data management, replicating current cloud management offerings observed in the IoT marketplace. On the other hand, the *Premium plan* requires a yearly subscription fee and includes additional controls for protecting data collection, usage, and retention over the cloud. These additional controls were developed based on prior efforts' findings on users' expectations and preferences for data security and privacy in the IoT context [29, 31].

To quantify monetary valuation of security and privacy, prior studies often rely on participants to self-report their WTP in hypothetical scenarios, which are susceptible to a phenomenon known as *hypothetical bias* [4, 16, 39]. Hypothetical bias can lead participants to overestimate their valuation of privacy, significantly diverging from their *true* preferences due to the lack of incentive to reveal it accurately [39, 59].

Consequently, to tackle the shortcomings of hypothetical biases and incentivize users to make genuine choices between privacy and money, we employed incentive compatibility in a lottery-based study setup. To achieve this, we presented participants with the opportunity to enter a lottery pool where they could win an Internet of Things (IoT) device by selecting one of two options. Additionally, participants were screened to include only those who were not current users of the IoT devices used in the lottery. Detailed information on the eligibility criteria and the screening survey is presented in Section 3.3.

Replicating the current data-centric business trend under the 'pay for privacy' model, in the lottery, participants were presented with two options:

1. **Option A: premium plan** - The *device* along with a year-long prepaid subscription of the premium data management plan.
2. **Option B: cash** - The *device* along with the free basic plan, plus a *cash amount* instead of the premium data management plan.

Given the above incentive-compatible lottery framework, the study's treatment conditions were determined based on extant research that focused on factors impacting users' monetary valuations of privacy. Perceived device risk was identified as one such factor. While device risk perception has been noted to be significant toward users' purchase decisions related to privacy [29, 31], there is a notable gap in the literature regarding how perceived risk differences influence users' cognitive processes and behaviors when balancing privacy against monetary costs. This study aims to bridge this gap by utilizing a mixed-methods approach to examine how users calculate their trade-off between privacy and money based on the perceived risk of IoT devices under *high risk* and *low risk* categories. With these considerations, the *device* in the lottery was an indoor smart camera in the *high risk* condition and a smart light bulb with motion sensor in the *low risk* condition. Note that, in our study, the light bulb is considered a low-risk device compared to the smart home camera collecting users' video feeds. However, categorizing the smart light bulbs as a universally low-risk device may not be appropriate, as suggested by Nissenbaum's *Contextual Integrity Framework* [62] and is not the intention of this paper.

Next, to understand how the privacy-money tradeoff unfolds at different price points, we also varied the *cash amount* in the lottery. This approach is built upon prior studies showing that users are willing to pay a premium for increased security and privacy for IoT devices. However, there is a limit to their WTP. Ul Haque et al. found that users' self-reported maximum yearly subscription fee for a premium data plan was, at most, the price of the device the premium plan was offered for [80]. Therefore, our study offers three cash options: one-third, two-thirds, and the full price of the offered $30 IoT device in the lottery.

With these considerations, we designed a 2 (device risk - High-risk: indoor smart home security camera vs. Low-risk: smart light bulb with motion sensor) by 3 (cash option - $9.99 vs. $19.99 vs. $29.99) between subject study to examine the tradeoff between privacy controls and monetary considerations to shed light on the overall dynamics of users' monetary valuation of privacy in the IoT context. In addition, as prior research demonstrates that understandability regarding privacy and security plays a crucial role in privacy-decision making [53, 80, 81], we measured technical literacy as an independent variable to examine its influence on users' tradeoffs between privacy options and money.

These considerations lead to the following research questions:

RQ1. How do device risk (*High-risk: camera* and *Low-risk: light bulb*) and cash option ($9.99, $19.99, and $29.99) impact participants' choice between the premium plan option and the cash option offered alongside the IoT device in the lottery?
RQ2. Does participants' technical literacy impact their consideration of the lottery choice between the premium plan and the cash option?
RQ3. What reasons lead participants to choose between the premium plan option and the cash option in the lottery?
RQ4. How do participants feel about the subscription-based 'pay for privacy' model deployed in the lottery?

We conducted a survey on the Prolific platform to answer these research questions. Analyzing data from 265 U.S. participants recruited through Prolific, our study reveals that device risk and cash option significantly influence participants' choices in the lottery. Participants revealed higher odds of choosing the premium plan option in the lottery in the *High-risk: camera* condition than in the *Low-risk: light bulb* condition. Similarly, the offered cash alternatives also impacted participants' choice between the premium plan option and the cash option offered in the lottery. Interestingly, an interaction between technical literacy and cash option was observed. Higher technical literacy was found to be associated with users' choice of the premium plan over cash significantly more in the $29.99 cash option compared to $9.99 cash option, implying a higher WTP for the premium plan among more technical participants, echoing prior effort's finding [80]. Qualitative analysis provided novel insights both about participants' reasoning behind their lottery choices and their general perception of a 'pay for privacy' model. A closer examination of users' reasoning for choosing between privacy and cash revealed that they often view premium privacy offerings for seemingly low-risk IoT devices negatively.

This negative perception may further contribute to negative attitudes towards IoT manufacturers. In addition, our findings offer valuable insights regarding users' perceptions of and expectations for privacy in the 'pay for privacy' model, revealing a mismatch between IoT providers' data-centric business model and end-users' expectation to have their data privacy protected.

2 Background

2.1 Antecedents of Privacy Decision-Making

Prior literature has explored multiple factors that can impact users' privacy-decision making and their monetary valuations of privacy. One such factor is users' perceived risk. Research has shown that decision-making is often based on users' perceptions of the risk associated with the environment [70, 72, 78, 82]. In the IoT context, users' perception of risk associated with an IoT device was found to impact their security and privacy expectations from that device [12, 29, 31]. When perceived risk is high, users report greater discomfort due to the sensitivity of collected data [60] and a higher WTP for devices with stronger security practices [58].

In addition to risk, price is identified as another influential factor affecting purchase behavior [47, 68]. In the IoT context, even though users are willing to pay a premium for security and privacy, there is a limit, as prior efforts suggest. For example, Emami-Naeini et al. reported that users expressed willingness to pay a premium of 10% to 30% of the device price for better security and privacy practices [31]. Similarly, Ul Haque et al. observed that, in a 'pay for privacy' model, users' maximum premium for a data management plan with additional controls was the base price of the IoT device [80].

Interestingly, technical literacy is noted as an important factor that can influence users' perception of privacy. Specifically, Kang et al. looked at the differences in the mental models of technical and non-technical participants, and suggested that technical participants have a more sophisticated understanding of privacy compared to non-technical participants [46]. Recent work has demonstrated that, despite expressing expectations of privacy in the IoT context, users often have gaps in their understanding of privacy implications [30]. These differences in security and privacy knowledge have important implications as several works have emphasized the importance of understanding privacy constructs in enabling users to make more proactive privacy decisions in different contexts [9, 53, 73]. For instance, research in the context of Social Networking Sites (SNS) has shown that technical literacy impacts the understandability of privacy features [25] and subsequent privacy behavior [9, 73]. Similarly, technical literacy has been found to positively influence users' comprehension of privacy controls, leading to an increased willingness to pay for these controls [80]. While understanding privacy and security is important, Caven et al. argued that simply providing adequate and salient information about manufacturer data practices in security and privacy labels may not be sufficient for users to make informed decisions. In fact, due to gaps in users' perceptions and abilities to understand the information provided [46], additional information can lead to cognitive overload [20]. Their findings challenge the notion that users can make informed decisions when all relevant details are available [21, 35, 43], and motivated us to look at the effect of technical literacy on participants' lottery choice behavior.

2.2 Monetary Valuation of Security and Privacy

Prior work explored user preferences and the monetary valuation of security and privacy in IoT and non-IoT contexts. In non-IoT contexts, research revealed that users are willing to pay premium prices for reduced risk of online identity theft [67] and effective phishing detection [61]. Users' WTP has also been recorded for having privacy-preserving features [48, 71]. Tsai et al.'s work revealed that participants assigned a higher monetary value and showed greater willingness to purchase products that better protect user data privacy, especially when device privacy practices were made saliently available [77].

In the context of IoT, Morgner et al. observed that offering frequent security updates was a crucial factor influencing users' self-reported intention to purchase IoT devices [58]. The relevance of security and privacy information to users' WTP has been noted by previous studies as well [12, 29, 31, 40]. While prior research has identified device risk as a predictor of users' purchase decisions, it has not fully explored how perceived differences in device risk influence users' privacy decisions against monetary costs. For instance, Emami-Naeini et al.'s work observed that users mention security and privacy as crucial to their purchase decisions [31], but the work did not investigate how WTP might vary based on device risk. Similarly, in an attempt to explore factors influencing users' WTP, Ul Haque et al. observed no statistically significant difference when users self-reported their WTP for premium privacy plans across devices with varying risk perceptions [80]. This observed insignificance could stem from the hypothetical nature of these studies, where users lacked incentives to engage in realistic tradeoffs between privacy and money, which are more typical in real purchasing scenarios. Specifically, research has shown that examining users' monetary valuation in a hypothetical setup is prone to 'hypothetical bias' [4, 16], which has the potential downside of significantly diverging from users' actual WTP at the point of purchase, leading to low external validity [39, 52, 59].

To our knowledge, only Emami-Naeini et al.'s work within the IoT privacy context explored users' WTP in an incentive-compatible setup, aiming to mitigate the risk of hypothetical bias [30]. They achieved incentive compatibility by using Multiple Price Lists (MPL), which indirectly estimates WTP based on participants' responses [4, 6, 45]. Their study observed that participants expressed a higher WTP for deidentified data collection compared to identifiable data collection and revealed that users would be willing to pay for higher security and privacy for the IoT device [30]. A key difference between our work and theirs is the focus: their study aimed to identify WTP based on specific security and privacy attribute pairs (e.g., deidentified vs. identified data collection) but did not focus on how different device risks might affect users' preferences for privacy over monetary value. On the other hand, our work explores factors impacting users' tradeoff calculations between privacy and money in a 'pay for privacy' setup with a focus to unfold how device risk, among other factors, may influence users' preference between privacy and money in a mixed-method approach.

Another distinction between our work and Emami-Naeini et al.'s work [30] is the methodical difference in ensuring incentive compatibility. Specifically, in contrast to their indirect approach toward incentive compatibility, we employed a direct lottery-based approach. Prior efforts indicated that indirect approaches like MPL

can introduce potential biases, such as anchoring/order effect based on whether the offered choices are in ascending or in descending order (users' preferences may be anchored on the first revealed price point) [44] and framing effect (where the price lists may encourage users to concentrate on the middle of the table, irrespective of their true preference) [7]. This can lead to divergences from real purchase behavior, despite introducing incentive compatibility [6]. On the other hand, a direct lottery-based approach allowed us to offer users incentivized tradeoffs between privacy and money, potentially mimicking the typical choices users are expected to go through during an IoT device purchase decision. Another potential advantage of our approach over MPL is its compatibility with eliciting behavioral insights following the lottery. Users can respond to the potential reasoning behind their choice through Likert-scale items or open-ended questions. In an MPL-based setup, participants go through several price list items, making it difficult to understand why specific price list items were accepted or rejected [44].

Literature has also explored users' behavior in privacy decision-making when presented with incentives that can potentially nudge them toward revealing personal information. These incentives can be monetary or otherwise. In this context, Happ et al. investigated under what circumstances users can be nudged toward revealing their personal information in the presence of rewards [38]. Their findings showed that offering incentives such as a box of chocolates just before asking to reveal passwords was surprisingly effective in encouraging participants to disclose such information, indicating that social engineering approaches intertwined with behavioral norms, such as the norm of reciprocity [36], can be used to incentivize users toward potentially revealing their personal information [22, 37, 57].

Behavioral economics suggests that monetary incentives (e.g., discount prices) can also be effective in leading users toward releasing their personal information. In the context of privacy, users' willingness to accept (WTA) such rewards is expected to be consistent with their valuation of the requested personal data [1, 2]. Users' WTA for revealing personal information is typically higher than their WTP for protecting their personal information, due to a phenomenon known as the *Endowment* effect [3].

In our study, the sole purpose of the offered cash incentives in the lottery was to provide users with an incentive-compatible tradeoff between privacy and money. However, the offered cash options can be considered as incentives to reveal their personal information by not choosing the premium data privacy controls. Based on previous research, in this setup, participants are expected to act based on the internal valuation of their personal information and their willingness to accept such incentives to reveal this information [2, 3]. Hence, in the lottery, we expect participants to perform the tradeoff calculations based on their internal valuation of the data collected by the offered IoT devices.

3 Methods

To address our research questions, we used two hypothetical data management plans to offer features that grant users control over cloud management along with IoT manufacturers' data retention, sharing, and usage practices. The hypothetical plan was developed to explore participants' willingness to pay (WTP) for the premium plan in a hypothetical setup [80].

The *Basic plan* is based on a review of the offered data management options with IoT devices in the Amazon marketplace. Many IoT devices come with free cloud storage and basic data viewing/sharing options. With these considerations, the *Basic plan* offered free cloud storage up to 2 TB and the ability to view and download cloud stored data. Based on a review of the IoT marketplace, IoT manufacturers offer various cloud storage options, which can significantly differ from traditional storage providers that typically offer small storage options for free. As an example, Google offers 15 GB of free storage for Google users[1]. On the other hand, IoT manufacturers often offer arbitrarily large cloud storage up to a certain time period, such as options to store and see cloud data up to the past 30 days[2]. Hence, in our setup, we chose the cloud storage value to be rather high in order for it to not significantly affect the desirability of the IoT devices offered in the lottery. In addition, the offering of the cloud management feature was included in both the basic plan and the premium plan to make it consistent across both plans to not bias users' choices between the options offered in the lottery.

The *Premium plan* included three additional key features, curated based on prior findings showing users' expectations and preferences to control their IoT devices' data retention, sharing, and usage practices [29, 31]. The additional features in the premium data management plans are: *Control over cloud data retention* - giving the user an option to delete cloud stored sensor data; *Control over data sharing* - giving the user an option to opt-out from third party data sharing; and *Control over data usage* - giving the user an option to restrict collected data to be used for device functionality only.

The premium plan features include data management controls that are usually not offered by service providers and IoT manufacturers. For example, even when there might be a specific data retention period mentioned, it is still not an industry standard common practice to give users control over deleting collected data. Instead, consumers are often given the option to request data deletion from the provider's site at the time of account termination. Even then, data deletion requests are often manually reviewed on a case-by-case basis and are not guaranteed [26, 33, 85]. Note that, the premium plan features are a reflection of users' preferences for the IoT in the United States and can vary due to the applied privacy law in other regions, which is discussed in Section 6.

Participants were informed that the basic plan was free with the device purchase, while the premium plan required an additional yearly subscription fee. This was communicated using a plan comparison chart shown in Figure 1. The same plan comparison chart was used in prior work, measuring users' WTP for the premium data management plan [80]. Using the same versions of the data management plan and the plan comparison chart allowed us to make a direct comparison between the current work's incentive-compatible setup and the prior work's hypothetical setup.

3.1 Study Variables and Groups

The study consists of six groups based on the levels of the independent variable: *device risk* and *cash option*. The variable *device risk* has two levels: *High-risk: camera* and *Low-risk: light bulb*. To ensure

[1] https://support.google.com/googleone/answer/9312312
[2] Kasa Care Plans - https://www.kasasmart.com/us/kasacare

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.

that our manipulation of *High-risk: camera* and *Low-risk: light bulb* devices worked, at a later phase of the study, we asked participants in each group to rate their perceived data sensitivity of the IoT device on a scale from 0 to 10. T-tests showed a significant difference between the perceived data sensitivity of the IoT device in the *High-risk: camera* group ($M = 7.26, Mdn = 7.0, SD = 2.22$) compared to the *Low-risk: light bulb* group ($M = 4.3, Mdn = 5.0, SD = 2.66$), ($t = 9.74, p < .0001$).

The device purchase prices were selected based on a market analysis on Amazon, where we observed that the average price for similar IoT devices ranges from $20 (USD) to $40 (USD) after considering the commonly offered discounts. As such, we set the study's IoT device price to be $29.99 (USD). We used the decimal numbers instead of rounding up to $30 to make the study setup realistic.

Our second treatment variable was *cash option*: the cash alternative that was offered to the participants in the lottery if they chose not to get the premium data management plan option. The cash option values were selected as one-third, two-thirds, and the same as the device price offered in the lottery, based on prior findings [80].

With these, we had a 2 (*device risk*) x 3 (*cash option*) factorial design, leading to six groups in the study. The group distribution is shown in Table 1. Note that while group names included the characters 'A', 'B', and 'C' to distinguish treatment conditions, the use of 'A' and 'B' in lottery options is not associated with the group names.

In addition, we measured participants' technical literacy using Kang et al.'s Technical Knowledge of Privacy Tools Scale (TKPTS), who validated the scale using a combined dataset from both online and in-person setups [46]. The scale contains six true/false questions to evaluate participants' technical literacy to avoid self-reporting of their own technical literacy. Based on the answers to the questionnaire, a participant can get a score from 0 to 6, which was used as a linear variable to observe its impact on participants' lottery choices in the study groups.

3.2 Incentive Compatibility and Ethical Considerations

To achieve incentive compatibility, we informed participants that the study is about understanding users' experience in buying IoT products from the marketplace. After asking questions about their IoT marketplace attitude and experience, we used deception and informed participants that we would host a lottery where participants could win an IoT device worth $29.99. We mentioned that we would choose five random winners from participants. We refrained from informing them how many participants would be in the lottery pool to prevent them from calculating any winning probability, which might have biased their responses.

To make the lottery setup realistic, we showed participants pictures and specifications of the devices they could win. The device images were edited out to remove any brand-related information. The specifications were curated from our analysis of the devices frequently available in the marketplace in this price range. In addition, we added specifications such as compatibility with Amazon Alexa, Google Assistant, and Apple Homekit to make the devices as generic as possible. Figure 4 in the Appendix presents the edited device images shown to the participants.

We opted for a subscription-based model for our premium plan offering. A *subscription model* is a revenue model that focuses on recurring payments, where subscribers are expected to pay a recurring fee, such as weekly, monthly, or yearly [87]. Several key considerations led us to choose a subscription model for our study. First, this model has gained widespread adoption in recent years due to its potential for generating ongoing revenue compared to one-time payments [54, 79]. Offering the premium plan as a subscription would therefore enhance the realism and ecological validity of our lottery. Second, our analysis of the IoT marketplace indicated that IoT manufacturers often offer subscription-based tiered plans for certain services, such as cloud storage. However, to reduce participants' cognitive burden associated with subscriptions, we opted for a yearly payment model while offering the first year of the premium plan as a choice in the lottery. We refrained from explicitly informing participants of any particular value of the yearly subscription fee of the premium plan to allow them to consider the lottery option tradeoff according to their true WTP for the premium plan, based on prior suggestion [86].

After being informed about the two versions of the data management plan, participants were informed about the lottery options between *Option A: premium plan* and *Option B: cash*, which they could choose from based on their preference to enter the lottery pool. In addition, participants were given an option to opt out of entering the lottery pool. The lottery choices were generated to elicit the tradeoff between receiving additional data management controls or accepting a cash amount based on participants' true preferences. Participants' choices in the lottery were used as the dependent variable in our analysis.

Once data collection was complete, we sent out a debriefing statement to all the study participants to inform them about the deception used in the study and the true purpose of the lottery using Prolific's messaging system. In addition, we informed participants that lottery winners will receive the exact amount of money equivalent to the IoT device price instead of the device using Prolific's bonus payment option. We refrained from sending out IoT devices to the participants for two primary reasons. First, sending devices would require collecting participants' sensitive personal information (e.g., their names and addresses). Second, we did not want to give out IoT devices without explicitly assessing their security and

Device Risk Perception	Cash Option	Group ($N = 265$)
High Risk: Indoor smart home security camera	$9.99	1A ($N = 45$)
	$19.99	1B ($N = 43$)
	$29.99	1C ($N = 41$)
Low Risk: Smart light bulb with motion sensor	$9.99	2A ($N = 46$)
	$19.99	2B ($N = 43$)
	$29.99	2C ($N = 47$)

Table 1: Study groups based on different levels of our independent variables.

privacy risks. The lottery winners were compensated $59.98 (USD) ($29.99 device price, plus the highest cash option of $29.99 across all the groups). This was paid in addition to their base payment for participating in the study.

Our University's Institutional Review Board (IRB) reviewed and approved the study design and deceptive elements used.

3.3 Participants and Eligibility Criteria

We recruited study participants from Prolific. Based on prior recommendations [64, 74], we restricted the survey to participants from the United States, who were 18 years or older, had English as their first language, and had completed at least 50 submissions with an approval rate of 95%.

In addition, to recruit participants who were not current users of indoor security cameras or light bulbs, our survey was designed to have two phases. In phase one of the survey, participants were asked to report the types of IoT devices they currently own and the types of IoT devices they currently do not own but would be willing to try out if offered. In this phase, participants who reported owning neither an indoor smart home security camera nor a smart light bulb, alongside being interested in trying out these devices if offered, were invited to complete phase two of the survey containing the lottery.

Further, participants were asked to report whether they had any computer science background to understand its distribution across their IoT usage. This question was not used as a screener to rule out participants to proceed to phase two.

Phase one survey took approximately 3 to 5 minutes, and participants were compensated $1. Participants who were invited to the phase two survey took approximately 8 to 10 minutes to complete this phase and were compensated $2 in addition to the $1 compensation for phase one.

3.4 Survey Flow

After consenting, participants first completed the phase one survey that included study-specific screening questions, the Technical Knowledge of Privacy Tools scale (TKPTS) to measure participants' technical literacy, and demographic questions. Eligible participants were invited to complete the phase two survey based on their answers to the screening questions.

If participants agreed to proceed with the phase two survey, they were randomly assigned to one of the six study groups to avoid potential bias due to skewed distribution across the groups.

Participants first answered the IoT marketplace attitude questions before they came across our lottery-based manipulation. Once participants selected their lottery choice, they did not have the chance to go back and change their lottery choice. Next, we asked a true/false question about the basic and premium plan to ensure participants paid attention to our study's manipulation.

Next, participants were asked to provide a brief reasoning behind their lottery choice to understand their internal reasoning behind it. Afterward, participants were asked to briefly explain how they felt about the business model of a premium offering of privacy options to understand their perceptions of the 'pay for privacy' model. We asked participants to orient their responses towards both the positives and negatives of such a business strategy to be able to extract themes on both sides of the spectrum.

Finally, participants answered multiple 7-point Likert items relevant to the lottery choices that might explain the reasoning behind their responses (e.g., "The premium data management plan is the company's business strategy to extract more money out of the consumer"). We asked these questions after all the open-ended questions to avoid biasing participants' responses. Similarly, participants were asked to rate the perceived data sensitivity of their assigned group's IoT device last so that it does not bias their responses.

We included two attention check questions in the form "Please select 'Strongly disagree' for this statement" to ensure that participants paid attention throughout the survey. The survey instrument for phase one and phase two can be accessed using the link in the Appendix.

3.5 Data Analysis

We recorded responses from 819 participants who completed phase one of the study. Among them, 374 participants were found eligible for and invited to complete phase two of the study. From the invited participants, 341 participants proceeded to phase two, contributing to our final dataset of 341 records across all groups. In the dataset, 8 participants failed at least one attention check question, and 69 failed the manipulation check questions that were asked following their lottery choice. We removed 76 responses who failed our attention and/or manipulation check questions, leading to the final dataset of 265 valid responses across our six study groups. For *High-risk: camera* group 46/129 participants chose lottery *Option A: premium plan*, 78/129 lottery *Option B: cash*, and 5/129 chose not to participate. For *Low-risk: light bulb* group these values are 22/136, 98/136, and 16/136, respectively.

We employed both quantitative and qualitative data analysis to answer our research questions. We built a regression model to

understand the effect of our independent variables (IVs) on the dependent variable (DV). The variables in the model were:

- *device_type*: This IV had two levels: *High-risk: camera* and *Low-risk: light bulb*
- *cash_option*: The IV cash amount offered to the participants with three levels: $9.99, $19.99, and $29.99.
- *tech_literacy*: Participants' technical literacy, was measured using the TKPTS scale [46] and used as a linear IV.
- *lottery_choice*: Dichotomous variable reflecting participants' choices between *Option A: premium plan* and *Option B: cash* in the lottery, which worked as the DV.

Because our DV was a dichotomous categorical variable, we fit Generalized Linear Models (GLM) on the data, with *logit* as the link-function [41, 65]. We leveraged the Akaike Information Criterion (AIC) to assess the model fit [17]. We initially included demographic factors (i.e., age, gender, education, employment, income, prior IoT experience from phase one) and all two-way interactions of our IVs. As the model fit did not improve with the demographic factors included, these factors and some interaction terms were removed in the selection process. The only interaction that improved the model fit was the interaction between *tech_literacy* and *cash_option* and got included in the final model.

We used Welch's t-tests for mean comparisons for the Likert items [24, 27]. To control for False Discovery Rate (FDR) that may arise due to multiple testing, we performed Benjamini-Hochberg correction [11] to the p-values, and reported corrected p-values in the paper. Data were analyzed using SPSS [34] and R [42].

For qualitative data analysis, we employed a bottom-up inductive coding approach [56]. Initially, one researcher coded each open-ended question independently to generate the initial codebook. Another researcher then used the codebook and coded the open-ended questions. Once the two researchers had coded the open-ended questions independently, they met and resolved any conflicts, finalized the codebook, and updated their codes accordingly. For the open-ended questions, we calculated Inter-rater reliability (IRR) using Cohen's Kappa, which ranged from 0.7 to 1, indicating "substantial" or "excellent" agreement between the two coders [49]. We report participants' comments with minor modifications to correct typos and grammatical inconsistencies as needed.

4 Results

Among the 265 valid responses across all groups, there were 153 (57.7%) women, 106 (40.0%) men, and 5 (1.9%) non-binary participants. One participant preferred not to disclose their gender. Participants' ages ranged from 20 to 76 years ($M = 40.26, Mdn = 38.0, SD = 12.95$).

A series of Chi-squared tests revealed no significant differences among the groups based on participants' gender ($\chi^2(15) = 18.41, p = .242$), education level ($\chi^2(35) = 34.05, p = .514$), employment status ($\chi^2(45) = 49.78, p = .289$), and their income level ($\chi^2(40) = 39.03, p = .514$).

The Kruskal-Wallis test showed significant differences among the groups based on participants' age ($H(5) = 11.203, p = .047$). Additional post-hoc tests with Bonferroni correction revealed a difference in age between participants in groups *1C* ($M = 45.61, Mdn = 48.0, SD = 15.63$) and *2B* ($M = 35.65, Mdn = 36.0, SD = 10.15$) ($p = 0.037$), indicating that participants in group *2B* were significantly younger than participants in group *1C*.

To understand if this specific age difference between the two groups impacted the overall model fit, we included the demographic variable age with other demographic factors in the model selection process. However, no demographic factors, including age, impacted participants' lottery choices in the full model. Hence, these factors were removed in the best-fitted reduced model. In addition, we ran the Mann-Whitney U test to observe if there was an age difference between the *High-risk: camera* and the *Low-risk: light bulb* groups. We did not notice any significant age difference between these two groups of participants ($U = 9478.0, p = .257$).

A group-wise demographic breakdown of participants is presented in Table 4 in the Appendix.

4.1 IoT Usage on Prolific

In the phase one survey, participants were asked to report their IoT usage in order for us to get an overview of the current IoT usage on Prolific. Of 804 respondents, 537 (66.8%) reported using IoT devices in their household. Of them, 227 (28.2%) participants reported using three to five IoT devices, and 184 (22.9%) indicated using one to two IoT devices in their household. The rest (126, 15.7%) indicated using more than five IoT devices.

When asked to report the type of IoT devices being used in their households, smart TV (410/804, 50.99%) was reported as the top IoT device used by the participants; followed by smart speaker with voice assistant (367/804, 45.65%) and smart watch (272/804, 33.83%). Smart toothbrush (30/804, 3.73%) and smart smoke detectors (28/804, 3.48%) were mentioned to be the least used IoT devices by our participants. Figure 3 in the Appendix presents participants' household IoT device usage.

Finding Summary: Majority of participants (66.8%) in the phase one survey indicated using IoT devices in their household. Smart TV was found to be the most used in participants' household, followed by smart speakers. Smart toothbrushes and smoke detectors were the least used based on the responses.

4.2 Effect of Device Risk Perception and Cash Option on Lottery Choice (RQ1)

Across all groups, 68/265 (25.7%) participants chose *Option A: premium plan*, whereas 176/265 (66.4%) participants chose *Option B: cash*. Additionally, 21/265 (7.9%) participants chose not to enter the lottery pool. We removed these 21 rows from the data before fitting the model. The model statistics are presented in Table 2.

When looking at the model outcome, we observed a significant effect of the *device_type* on participants' choices in the lottery. Specifically, compared to participants in the *Low-risk: light bulb* condition, participants in the *High-risk: camera* condition indicated increased odds of choosing *Option A: premium plan* over *Option B: cash* ($OR = 2.7349, CI_{95\%} = [1.5026, 5.1109]$). Hence, the IoT device's perceived risk and severity significantly influenced participants' tradeoff calculations between data management options and money.

Row	Model Factor	Estimate	OR	SE	z-value	p-value
1	(Intercept)	-2.11	0.1211	0.53	-3.97	***
	device_type (baseline = smart light bulb with motion sensor)					
2	Device: indoor smart home security camera	1.01	2.7349	0.31	3.23	**
	cash_option (baseline = $29.99)					
3	Cash option: $19.99	0.78	2.1735	0.70	1.10	.29
4	Cash option: $9.99	2.00	7.3977	0.67	3.01	**
	tech_literacy (Continuous)					
5	Technical literacy	0.17	1.1864	0.18	0.96	.34
	tech_literacy * cash_option (baseline = Technical literacy * Cash option: $29.99)					
6	Technical literacy * Cash option: $19.99	-0.36	0.7004	0.26	-1.38	.19
7	Technical literacy * Cash option: $9.99	-0.61	0.5418	0.25	-2.5	*

Model Fit: $\chi^2(6) = 24.7, p < .001$; $Pseudo - R^2 = 0.14$; $AIC = 278.06$ $\quad * p < 0.05$; $** p < 0.01$; $*** p < 0.001$

Table 2: We fitted a GLM using *logit* as the link function to identify the significance of our IVs on our DV. In the model, the DV was the participants' lottery choice: 0 - *Option B: cash*; 1 - *Option A: premium plan. OR* indicates *odds ratio* for participants lottery choice; an $OR > 1$ corresponds to increased odds of choosing *Option A: premium plan* from *Option B: cash*, whereas, an $OR < 1$ corresponds to decreased odds of choosing *Option A: premium plan* from *Option B: cash*.

Similarly, the model outcome indicates that different *cash_option* conditions significantly impacted participants' lottery choices. Compared to participants in the $29.99 cash condition, participants in the $9.99 cash condition revealed increased odds of choosing *Option A: premium plan* over *Option B: cash* ($OR = 7.3977, CI_{95\%} = [2.0774, 28.6985]$). However, participants in $9.99 vs. $19.99 conditions did not reveal significantly increased odds of choosing the data management options over the cash option. A similar observation was noted between the participants in $19.99 vs. $29.99 conditions.

Finding Summary: Based on the model outcome, both device risk perceptions and cash conditions had a significant impact on users' lottery choices. When the IoT devices' perceived risks were considered high, such as for an indoor smart home security camera compared to a smart light bulb with a motion sensor, participants were more likely to choose the additional data privacy controls in the premium plan than taking the cash option. On the other hand, when the offered cash option was $9.99 compared to $29.99, participants were more likely to choose the premium plan option. This finding indicates that higher cash alternatives may influence users to avoid taking the data privacy controls and lure them toward receiving the cash instead. This choice of cash over the premium plan controls is likely dependent on participants' valuation of the additional data privacy controls in the premium plan, as prior efforts suggest [1, 2].

4.3 Interaction of Technical Literacy and Cash Option in Participants' Lottery Choices (RQ2)

Our model outcome reveals a significant interaction between participants' technical literacy and the cash option in their choice of lottery. The visualization of the observed interaction is included in the Appendix (Figure 5).

The model outcome showed that, compared to $9.99 cash condition, in $29.99 cash condition, per unit increase in participants' technical literacy corresponded to increased odds of choosing *Option A: premium plan* over *Option B: cash* ($OR = 0.5418, CI_{95\%} = [0.3307, 0.8697]$). This finding suggested that participants with lower technical literacy scores (i.e., non-technical participants) were significantly more likely to choose *Option A: premium plan* compared to participants with higher technical literacy scores (i.e., technical participants) in the $9.99 cash condition. However, this direction reversed in the $29.99 cash condition, where technical participants seemed more likely to choose *Option A: premium plan* than their non-technical counterparts.

Finding Summary: Based on the model outcome, technical literacy plays a crucial role in users' lottery choices. Higher technical literacy is likely to lead participants toward choosing the additional data privacy controls more than the cash at the higher cash condition of $29.99. This difference in participants' lottery choices based on their technical literacy level is consistent with prior findings showing that higher technical literacy positively leads to a higher monetary valuation of data privacy controls included in the premium plan [80].

4.4 Participants' Post-lottery Responses (RQ3)

We followed a two-step process to shed light on our participants' thought processes when choosing different options in the lottery. First, following participants' responses to the lottery choices, we asked them to briefly explain their reasoning behind their lottery choice, which we qualitatively analyzed to report emerging themes for both categories of participants, namely, participants who chose *Option A: premium plan* vs. participants who chose *Option B: cash*.

In addition to mentioning the reasoning behind their lottery choice, we asked participants to rate five statements (on a 7-point Likert scale - "Strongly disagree" to "Strongly agree") that can be relevant to their thought process for choosing between the lottery options. The research team brainstormed and curated these statements that are likely to illuminate possible reasons behind

participants' lottery choices, especially to reflect on the data privacy controls' *necessity*, *underlying motive*, and *efficacy* in terms of data privacy protection. For example, participants who chose the cash option in the lottery might feel that they do not need the premium plan and its additional controls, as they might believe that the IoT device does not collect enough sensitive data or that they are capable of protecting their personal data, among other reasons.

In this subsection, we report participants' responses to these statements indicating potential reasons behind the lottery choice. In the next section, we present the qualitative analysis of participants' comments to identify recurring themes.

We performed mean comparisons between participants in the *High-risk: camera* and in the *Low-risk: light bulb* groups to determine whether their assigned IoT device's relative risk perception had any impact on their responses. Figure 2 presents participants' responses to the statements based on, (a) their lottery choice (left) and, (b) their assigned group's device risk perception (right).

(i) Participants' responses to the statement *"The premium data management plan is the company's business strategy to extract more money out of the consumer":* Participants choosing both *Option A: premium plan* and *Option B: cash* scored high in their responses to this statement, indicating that participants mostly agreed with the statement. However, participants choosing *Option A: premium plan* ($M = 5.11, Mdn = 5.0, SD = 1.57$) indicated lower scores compared to participants choosing *Option B: cash* ($M = 5.71, Mdn = 6.0, SD = 1.35$), which was found statistically significant ($t = 2.78, p = .011$).

Looking at the differences between participants in different device conditions, we observed that participants in the *High-risk: camera* group ($M = 5.20, Mdn = 5.0, SD = 1.52$) indicated significantly lower ratings for this statement than participants in the *Low-risk: light bulb* group ($M = 5.87, Mdn = 6.0, SD = 1.24$) ($t = 3.87, p = .0004$).

Hence, participants who chose the cash options in the lottery, and those who were assigned to the light bulb conditions, agreed to this statement significantly more than their counterparts, suggesting that they are more likely to believe that offering the premium plan works more toward the company's profit motive rather than offering privacy.

(ii) Participants' responses to the statement *"The premium data management plan does not provide any additional protection to my data privacy":* Participants choosing *Option A: premium plan* ($M = 2.92, Mdn = 3.0, SD = 1.52$) rated significantly lower for this statement than participants choosing *Option B: cash* ($M = 3.59, Mdn = 4.0, SD = 1.63$) ($t = 2.96, p = .0074$), indicating more agreement for this statement among participants choosing the cash option in the lottery.

Similar to the last statement, participants from the *High-risk: camera* group ($M = 3.14, Mdn = 3.0, SD = 1.62$) rated significantly lower for this statement than participants in the *Low-risk: light bulb* group ($M = 3.73, Mdn = 4.0, SD = 1.58$) ($t = 2.97, p = .0073$).

In summary, participants who chose cash in the lottery are more likely to feel that the additional data controls do not add to data privacy protection (i.e., are not effective), which was also true for participants who were assigned to the light bulb group.

(iii) Participants' responses to the statement *"The device does not collect enough personal data that requires an additional premium data management plan":* Similar to the last two statements, participants choosing *Option A: premium plan* ($M = 3.26, Mdn = 3.0, SD = 1.69$) rated significantly lower for this statement compared to participants choosing *Option B: cash* ($M = 4.51, Mdn = 5.0, SD = 1.58$) ($t = 5.23, p = .0004$).

Looking at the differences between participants in different device conditions, we observed that participants from the *High-risk: camera* group ($M = 3.51, Mdn = 4.0, SD = 1.53$) rated significantly lower for this statement than participants in the *Low-risk: light bulb* group ($M = 4.63, Mdn = 5.0, SD = 1.69$) ($t = 5.59, p = .0004$).

These findings indicate that participants who chose the cash options in the lottery were likely to feel that the additional data privacy controls are not of importance as they are likely to believe that the offered IoT devices do not call for additional data management requirements. Similarly, participants assigned to the light bulb condition felt the same way at a higher rate compared to those who were assigned to the indoor smart security camera.

(iv) Participants' responses to the statement *"I doubt that the company's premium data management plan will do what it says it will do":* In contrast to prior statements, we did not notice any significant difference in ratings between participants choosing *Option A: premium plan* ($M = 3.36, Mdn = 3.0, SD = 1.56$) and participants choosing *Option B: cash* ($M = 3.68, Mdn = 4.0, SD = 1.54$) ($t = 1.41, p = .19$). This finding suggests that despite their differences in choosing the lottery option, both groups similarly agreed with the additional data privacy controls' efficacy towards offering heightened protection for data privacy.

However, looking at different device conditions, we found that participants from the *High-risk: camera* group ($M = 3.39, Mdn = 3.0, SD = 1.51$) rated significantly lower for this statement than participants in the *Low-risk: light bulb* group ($M = 3.87, Mdn = 4.0, SD = 1.56$) ($t = 2.53, p = .018$). This suggests that, when additional data privacy controls were offered for the light bulbs in the lottery, participants were more likely to be doubtful regarding the controls' efficacy than when the controls were offered for the smart security camera.

(v) Participants' responses to the statement *"I am capable of protecting my data privacy on my own hence I do not require an additional premium data management plan":* Unlike the previous statement, participants choosing *Option A: premium plan* ($M = 3.09, Mdn = 3.0, SD = 1.62$) rated significantly lower for this statement compared to participants choosing *Option B: cash* ($M = 4.74, Mdn = 5.0, SD = 1.46$) ($t = 7.225, p = .0004$). Hence, participants who chose the cash option were found to overwhelmingly believe that they were capable of protecting their personal data, questioning the necessity of the premium plan offering.

Looking at the differences between participants in different device conditions, though participants from the *High-risk: camera* group ($M = 4.1, Mdn = 4.0, SD = 1.67$) rated lower for this statement than participants in the *Low-risk: light bulb* group ($M = 4.44, Mdn = 5.0, SD = 1.63$), the difference was not statistically significant ($t = 1.65, p = .132$). Hence, participants' beliefs about their capability of protecting their personal information did

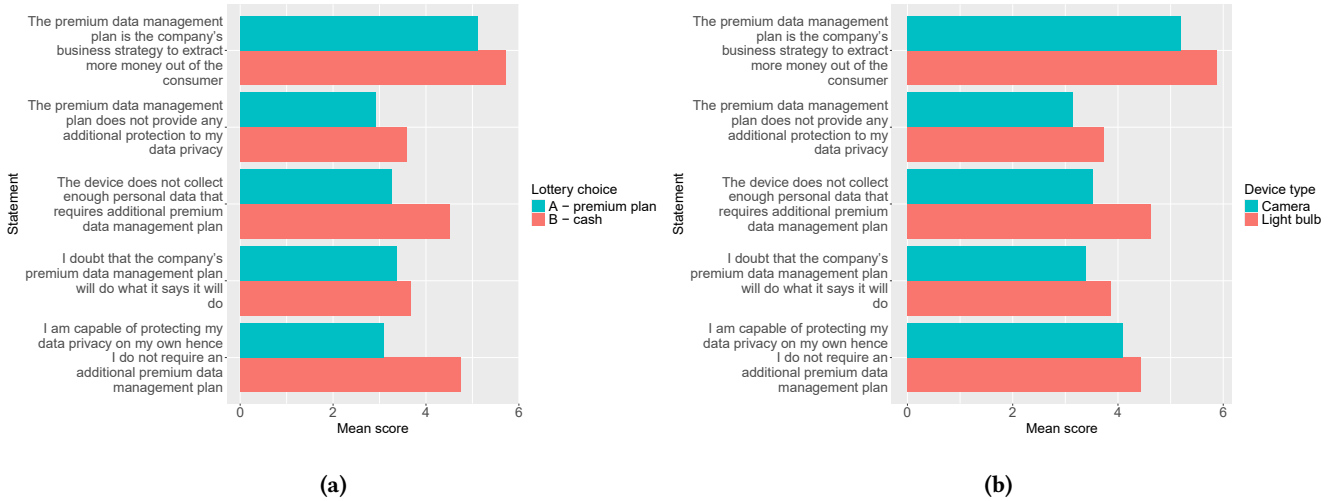

Figure 2: Mean difference of the post-lottery Likert items (a) between participants choosing *Option A: premium plan* vs. *Option B: cash* (left); (b) between participants in the *High-risk: camera* vs. *Low-risk: light bulb* groups (right).

not change significantly based on the device risk condition they were assigned to.

Finding Summary: Among participants choosing between *Option A: premium plan* and *Option B: cash*, considerable disagreement was observed regarding their perceptions of whether IoT devices collect sufficient personal data and their own ability to protect their data privacy. Interestingly, both groups agreed that the premium plan could be the IoT manufacturer's business strategy to extract money from consumers.
A closer look at the differences between the *High-risk: camera* and the *Low-risk: light bulb* groups also revealed surprising observations. Specifically, compared to participants in the *Low-risk: light bulb* group, participants in the *High-risk: camera* group disagreed significantly more on whether the premium plan is a business strategy of the IoT manufacturer or whether it provides any additional protection for user data privacy. This interesting observation suggests that users' perceptions of the premium plan may differ significantly based on their perceived risk associated with the IoT device for which the premium plan is offered.

4.5 Participants' Reasoning behind Choosing *Option A: premium plan* and *Option B: cash* (RQ3)

Qualitative analysis of participants' comments revealed a complete picture of the recurring themes behind participants' lottery choices, which goes beyond the narrow scope of the Likert statements suggesting reasons based on the controls' *necessity*, *motive*, and *efficacy*. The recurring themes both agree with the responses for the Likert statements and identify other vital reasons for or against choosing between the lottery options.

The number of comments for the qualitative data is equal to the distribution of participants' choices between options in the lottery. In particular, 68 participants chose *Option A: premium plan* in the lottery and mentioned their reasons for choosing this option (46 in *High-risk: camera* group and 22 in *Low-risk: light bulb* group), whereas 176 participants chose *Option B: cash* and indicated their reasons for choosing cash option (78 in *High-risk: camera* group and 98 in *Low-risk: light bulb* group). In this paper, example comments are presented with minor corrections to address typos as needed.

4.5.1 Reasons for Choosing Option A: premium plan. Participants' main reasons behind choosing the premium plan option instead of receiving cash are presented below.

(i) Preference to have additional data privacy protection: In total, 26/68 (38.25%) (19 in *High-risk: camera* group and 7 in *Low-risk: light bulb* group) comments indicated participants' preferences for having additional data privacy options to have *control over data*, which worked as their primary reason for choosing the premium data management option in the lottery, as portrayed in the following comment.

"Just made sense, I would rather my data be protected if there is an option for it. $19.99 is nice and all, but if I am using one of these things and it is recording everything about me, I would rather be safe." (GR 2B)

Concerns over data privacy may often lead participants to go for privacy-protective measures, as the following comment suggests.

"The additional features are important to me. I do not appreciate not being able to delete or manage my personal information. It makes me very uncomfortable." (GR 2C)

Participants' responses to the Likert statements further align with this theme, where participants choosing *Option A: premium plan* disagreed significantly more with the statement that suggests the premium plan does not provide additional controls over personal data. Similarly, these participants disagreed with the statement about being capable of protecting their personal data. Hence, they likely prefer having additional data controls offered in the premium plan to protect their data privacy, as suggested by this theme.

(ii) More valuable than the cash alternative:
Many participants felt the premium plan was more valuable and a better deal than the cash offered as the other option. For these participants, their valuation of the premium plan compared to the cash offer was an important consideration when choosing the premium plan option in the lottery. In particular, 25/68 (36.76%) (20 in *High-risk: camera* group and 5 in *Low-risk: light bulb* group) comments reflected this theme, as suggested in the following comment.

"I picked the premium data management instead of the cash because I think that that offers a premium that is much more valuable than the $29.99 I would have received." (GR 1C)

As this comment suggests, offering additional features in the premium plan made it more worthwhile than the cash for some participants.

"Although the cash would be nice, the premium plan has features above the basic plan that I would appreciate and take advantage of." (GR 1B)

(iii) Convenience of trying the plan out without paying first:
For some participants, the convenience of not worrying about paying the subscription fee was essential as the offered option included a prepaid yearly subscription to the premium plan. These participants indicated their preference to experience the plan and its additional features without paying first; hence, they felt that the prepaid one-year subscription offers more benefits than money. In particular, 15/68 (22.06%) (9 in *High-risk: camera* group and 6 in *Low-risk: light bulb* group) comments indicated this reason for choosing the premium plan option.

"I figure if I was lucky enough to be a winner, I would like to see the full experience a new-to-me product can offer and see if it is something I would like to continue after the year is up." (GR 2B)

"I would not have to worry about purchasing the plan or keeping up the payments." (GR 1A)

4.5.2 Reasons for Choosing Option B: cash. Comments reveal some crucial factors behind choosing *Option B: cash* instead of receiving the premium data management plan option, which we elaborate on here.

(i) Questioning the need for the premium plan alongside having preferences for cash:
For a subset of participants, it was unclear why the premium plan option might be necessary. These participants felt that the premium plan was unnecessary, especially when a basic plan was offered with the device, and they would rather have the cash instead. In total, 85/176 (38.29%) (35 in *High-risk: camera* group and 50 in *Low-risk: light bulb* group) comments suggested this theme. This theme echoes their responses to the Likert statements, where participants choosing the cash option agreed more that the premium plan option does not provide any additional data privacy protection. One such comment is presented below.

"I am more interested in a cash payment instead of the premium data management plan since the device already comes with a basic data plan. I am not too picky about third-party sharing or data usage, so the basic plan works for me." (GR 1B)

Many participants, especially in the *Low-risk: light bulb* group, indicated that they do not see the need for any premium offering when it comes to protecting data collected by a light bulb, which also aligns with the Likert statement responses where participants in the light bulb condition rated significantly more that the device does not collect excessive personal data that would require additional protection. Hence, the cash option is preferable, as suggested in the following comment.

"I do not think I need such stringent data management, such as the option to delete cloud data or prevent third parties from accessing it, for data related to light bulbs." (GR 2A)

Some participants felt that managing the premium plan and its additional options would be tiresome, indicating some inconvenience or hassle in managing the additional plans in the settings, especially those who consider themselves 'basic' technology users.

"I understand why control over your own data is a good thing to have, I just do not have the energy to manage that side of things, and would rather have the $29.99 cash" (GR 2C)

Another frequently mentioned reason behind users' choice was that they preferred cash over the premium plan option. Overall, 59/176 (33.52%) (26 in *High-risk: camera* group and 33 in *Low-risk: light bulb* group) comments indicated the notion of *"I'd rather have cash"* or *"Cash is always good!"*, suggesting a general preference for money, especially when offered as an alternative.

"I may not need the premium data management plan, however, I can use the $19.99 for anything else." (GR 2B)

(ii) Trying out the device first before committing to the paid plan:
For a handful of participants, wanting to try out the device before committing to any subscription was crucial behind their choice of the cash option in the lottery. Specifically, 29/176 (16.48%) (18 in *High-risk: camera* group and 11 in *Low-risk: light bulb* group) participants indicated this preference, as shown in one of such comments.

"I am unsure if I will enjoy the light bulb. If I do enjoy the functions I may consider buying the premium service plan separately after using the device for a while." (GR 2A)

Some participants expressed a need for more information about the device and the premium plan offering before committing to the premium offering.

"I would like to do more research on the premium plan and whether or not it would be beneficial to me personally before I decide to try it." (GR 1C)

(iii) Negative sentiments toward subscription-based models:
Some participants indicated a strong negative sentiment towards the subscription-based payment model, which affected their decision. Specifically, 21/176 (11.93%) (9 in *High-risk: camera* group and 12 in *Low-risk: light bulb* group) participants revealed disliking the *hassle* of getting locked into subscription plans, as this comment suggests.

"... I have too many subscriptions and free trials to keep track of as it is. The extra features I would be getting with the premium version are not worth the hassle of a subscription in my opinion." (GR 1A)

(iv) Questioning the efficacy of the data privacy controls:
A few participants (4/176 (2.27%)) (1 in *High-risk: camera* group and 3 in *Low-risk: light bulb* group) seemed to distrust whether the features would work as they suggested, indicating a notion of distrust on manufacturers' commitments for data privacy. This

outlook aligns with participants' responses to the Likert statements, where participants across all groups indicated greater agreement that the premium offerings are nothing but the company's business strategy, especially when their profit model often relies on the monetization of the device collected data.

"I do not really believe that my data would be more protected if I subscribed to the premium plan." (GR 2C)

As pointed out in the following comment, a notion of general distrust over privacy in the era of the interconnected world is also observed.

"Privacy is good, but since when have I really had internet privacy anyways?" (GR 2B)

4.6 Participants' Attitudes towards the Subscription-based 'Pay for Privacy' Model (RQ4)

To understand participants' attitudes towards the *'pay for privacy'* model, we asked participants across all the groups ($N = 265$) to indicate how they feel about the premium data management offering for a fee. Participants' answers shed light on the model's positives and negatives, as described here and summarized in Table 3. An interesting observation was that participants' comments sometimes overlapped with their reasoning for choosing between the lottery choices (as discussed in the previous subsections) and their attitude towards the 'pay for privacy' model. For example, participants' negative attitude towards the subscription-based model was a frequently mentioned reason for not choosing the premium plan in the lottery.

4.6.1 Positive factors towards accepting the 'pay for privacy' model. Participants' comments explored several reasons behind accepting the 'pay for privacy' model, as described below.

(i) Offers choice and flexibility:
Overall, 84/265 (31.7%) (48 in *High-risk: camera* group and 36 in *Low-risk: light bulb* group) participants felt that offering additional privacy options for a fee should give users the flexibility to choose the best option based on their personal needs and preferences. In this way, consumers would choose from several options instead of being forced to pay for the highest tier, especially if a free basic option is available.

"I like when they are sold separately, so that if you do not want the premium plan, you do not have to purchase it. It opens up many more options..." (GR 2A)

Some participants also pointed out that a separate plan should offer users the choice to cancel the plan if they feel the plan is not worthwhile for the money.

"I would rather purchase the data plan separately in case I choose to cancel." (GR 2C)

(ii) Brings cost-effectiveness to the structure:
Some participants felt that separating the device and the plans could make it more cost-effective and make the product more affordable. In total, 24/265 (9.1%) (11 in *High-risk: camera* group and 13 in *Low-risk: light bulb* group) participants reflected on this theme.

"... I guess it makes it more accessible to get the device in the first place. Otherwise, if everything was included but there was no subscription, the device might be super expensive." (GR 1 A)

(iii) Additional protection for products with high data sensitivity:
A total of 11/265 (4.15%) (6 in *High-risk: camera* group and 5 in *Low-risk: light bulb* group) participants' comments indicated that, though the generic offering of such premium plans may not apply to all IoT products, the premium privacy offering should offer additional data privacy options for the IoT devices that collect more sensitive data, as this comment suggests.

"I guess it would be nice to have the extra features but it might really depend on the type of device. I do not really see the benefit of a premium plan for a light bulb, but could perhaps see the benefit for a smart lock for your home." (GR 2C)

4.6.2 Negative factors towards rejecting the 'pay for privacy' model. Participants' comments also went in the other direction in exploring why the 'pay for privacy' model was rejected, as described below.

(i) Data privacy offerings should not be kept behind a paywall:
A total of 57/265 (21.51%) (20 in *High-risk: camera* group and 37 in *Low-risk: light bulb* group) comments reflected that personal data privacy should be free and included and should never be *behind a paywall*, which was the main reason for rejecting the premium offering for an additional fee.

"I feel like the features that are included in the premium data plan should instead be included in the basic plan. Options to stop third parties from collecting your data and the option to delete data from the cloud should be basic options. You should not have to pay for such basic options." (GR 2C)

While expressing their opinions against the model, some participants indicated that under specific regulations, manufacturers might be forced to offer user data privacy for free, pointing out the importance of strict privacy regulations to protect user data privacy.

"I do not normally object to it, but since the premium features were all privacy options it felt a little scummy to me. I feel like in other areas, like the EU, the company would be required to offer those options without additional charge." (GR 1A)

(ii) Potentially contributes towards 'subscription-fatigue':
Towards rejecting the 'pay for privacy,' our participants often indicated being overwhelmed by a substantial 'subscription-fatigue.' A total of 53/265 (20.0%) (28 in *High-risk: camera* group and 25 in *Low-risk: light bulb* group) comments suggested negative sentiments toward subscription-based models, indicating a general dislike towards the trend of subscription-based service offerings in recent years.

"... There is always a 'premium' option for everything these days and I can not afford them. So I do not think about them" (GR 2B)

Some participants also indicated that offering multiple options and a tiered subscription model can be confusing and a hassle for consumers to manage. They would rather have the features included with the device, even if they add up to the overall price.

Positive factors toward accepting 'pay for privacy'	Negative factors toward rejecting 'pay for privacy'	Participants' suggestions towards improving 'pay for privacy'
1. Offers choices and flexibility (31.7%)	1. Data privacy offerings should not be kept behind a paywall (21.51%)	1. Ensuring simplicity and balance between the offered tiers (7.55%)
2. Brings cost-effectiveness to the structure (9.1%)	2. Potentially contributes towards 'subscription-fatigue' (20.0%)	2. Ensuring that device functionality is not tied to the purchase of premium plan (6.79%)
3. Additional protection for products with high data sensitivity (4.15%)	3. Potential for distrust towards manufacturers' data practices (18.49%)	3. Offering free trials of the premium plan before the purchase (5.28%)
	4. Seemingly unnecessary for products with low data sensitivity (10.95%)	

Table 3: Frequent themes mentioned by the participants towards both accepting or rejecting the 'pay for privacy' model alongside offered suggestions towards improving the model's acceptability.

"I think it should just be included for one price. Offer whatever you want for the product and plan and just make it simple." (GR 2C)

(iii) Potential for distrust towards manufacturers' data practices:
A subset of participants (49/265, 18.49%) (23 in *High-risk: camera* group and 26 in *Low-risk: light bulb* group) felt that requiring users to pay for privacy features can make consumers concerned by creating negative feelings and distrust towards the offered manufacturer.

"To me, the premium plan seems to be saying 'give us more money or we will share and sell data we have collected on you.' It turns me off from the product." (GR 2B)

Some participants felt that a 'pay for privacy' model might result from manufacturers' unethical practices of extracting money from consumers by potentially leveraging their privacy concerns, as this comment suggests.

"It feels more like a scam but definitely an opportunity to make money. Many people I know are concerned about privacy when it comes to IoT devices." (GR 1A)

(iv) Seemingly unnecessary for products with low data sensitivity:
For many participants, especially in the *Low-risk: light bulb* group, having a separate premium plan seemed unnecessary. They seemed to have a hard time justifying why the premium plan and additional data management features were necessary for a light bulb, which was also found to be a common reason for choosing the cash option in the lottery. In total, 29/265 (10.95%) (4 in *High-risk: camera* group and 25 in *Low-risk: light bulb* group) comments reflected on this theme.

"I cannot see the value in such plans personally, especially for something as simple as a pack of smart bulbs. I do not know why anything other than maybe an extended warranty or protection plan being needed." (GR 2C)

4.6.3 Users' expectations and suggestions toward improving 'pay for privacy' model's acceptability: Participants' comments sometimes included suggestions or guidelines regarding what they feel should be ensured to make the premium privacy offerings worthwhile. These suggestions often reflected on their expectations from such a model in order for them to consider accepting it.

(i) Ensuring simplicity and balance between the offered tiers: Some participants pointed out that the tiered architecture should be balanced, respect users' various needs and expectations, and be simple and easy to use. In addition, the price differences between the tiers should be reasonably set to make it attractive to users. Overall, 20/265 (7.55%) (9 in *High-risk: camera* group and 11 in *Low-risk: light bulb* group) participants indicated this theme in their comments.

"... It needs a good balance between options and simplicity for users to work well." (GR 1A)

"... I definitely like 'tiers' of plans that offer different things for different price points so I can kind of pick and choose which additional services are worth it for me." (GR 1C)

(ii) Ensuring that device functionality is not tied to the purchase of premium plan:
In total, 18/265 (6.79%) (11 in *High-risk: camera* group and 7 in *Low-risk: light bulb* group) participants felt that, despite the offering of premium options requiring a fee, manufacturers must make sure that the device remains fully functional even if consumers do not purchase the premium offering.

"As long as the device functions properly, for its entire product lifecycle, without the need for a premium subscription, I am fine with the concept. If I have to pay for a product upfront and then I am forced to pay a subscription to benefit from the product, I will not use the product. For instance, I wanted to buy an Oura ring, but with their new pricing model you have to pay for the product and a subscription to benefit from it, which is untenable to me." (GR 2B)

(iii) Offering free trials of the premium plan before the purchase:
Some participants (14/265, 5.28%) (5 in *High-risk: camera* group and 9 in *Low-risk: light bulb* group) suggested that the premium offering of additional features should include a free trial so that users can experience them before deciding to ultimately pay for it, as these comments point out.

"My preference would be for it to be made available with purchase, without additional cost, for at least a trial period." (GR 1A)

"... I would need to see how it fits in my life before considering paying extra for the plan" (GR 2A)

5 Discussion and Design Recommendations

5.1 Mismatch between Businesses' Profit Motive and User Expectation for Data Privacy

The ubiquity of IoT devices and the potential for privacy breaches due to excessive data collection have been extensively documented in previous research [31, 66, 90]. A key takeaway from research looking at users' expectations to mitigate these concerns is that users are generally willing to pay premium prices for data security and privacy, aligning with the 'pay for privacy' model, which can incentivize IoT manufacturers to ask a premium price for enhanced security and privacy features [30, 58, 80]. This suggests an apparent alignment between IoT producers and consumers: manufacturers can offer premium data protection services, and users will willingly pay for these options, appreciating the effort toward improved security and privacy.

However, our incentive-compatible study revealed that 66.4% of participants chose the cash option in the lottery rather than opting for additional data privacy controls under the premium plan. Qualitative findings revealed reasons that may lead consumers to reject the 'pay for privacy' model altogether. Hence, despite the offering of premium data management controls in a 'pay for privacy' model, data collection and usage by service providers are likely to remain unchanged for many, posing a significant threat to user data privacy. This discrepancy highlights a mismatch between the data-centric profit models of service providers and IoT manufacturers and consumers' expectations for data privacy protection.

To understand this potential mismatch and its implications for privacy, we must examine it from the perspectives of both stakeholders. From the service provider's standpoint, user data is a crucial asset for business growth, especially in the current era of data-driven profit models [5, 18]. In such models, the utilization of user data is essential for revenue and business expansion, requiring IoT manufacturers to collect data. Previous studies support this assertion, finding that IoT manufacturers often employ poor data collection and usage practices [50, 55, 84] and fail to provide clear information about what data is collected and how it is used [31, 80]. Given that monetization of user data is one of the major revenue sources in a data-oriented business model, offering effective privacy controls that genuinely restrict data collection is expected to include a premium price in a 'pay for privacy' model, which aligns with prior findings showing that users would be willing to pay for such offerings.

While our participants' preference for cash over additional controls might seem to align with the concept of the 'privacy paradox,' a closer examination from the consumer's perspective reveals a different explanation. The 'privacy paradox' suggests that, despite expressing concerns about privacy, users often engage in behaviors that can compromise their privacy [15, 63]. However, in our study, one of the primary reasons participants rejected the 'pay for privacy' model was their belief that data security and privacy should be free and inclusive. This internal belief likely led them to view 'pay for privacy' as a violation of personal rights, causing them to reject the model even when the offered privacy controls could potentially mitigate the pervasive use of device-collected data. The dichotomy between the controls' intended purposes and the business's profit motive may have further contributed to this rejection, as indicated by participants' comments. This finding echoed prior efforts demonstrating that even when privacy controls are offered at no cost, users may still question their effectiveness if data collection is a major contributor to a business's revenue structure [81]. Therefore, regardless of whether a 'pay for privacy' model is implemented, users' rejection of privacy controls is a plausible scenario, leading to no substantial change in manufacturer data collection and potentially violating privacy. The observed results suggest that the current dynamics not only empower service providers to continue data collection but also place a cognitive burden on consumers by offering unprecedented choices despite their preferences for data privacy, as illustrated by this participant's comment:

"The fact that I can not delete and control data use on the basic plan is terrifying to me. My privacy concerns make the premium plan mandatory if I use the camera and that feels bad. I hate like I am being extorted to use the product the way I think any reasonable consumer would want it to be able to be used." (GR 1C)

We argue that the most effective solutions to address this power imbalance between service providers and consumers require legislative intervention. New and revised regulations should mandate that service providers and IoT manufacturers offer effective means for data privacy protection. Moreover, our findings suggest that policymakers must ensure that fundamental data privacy controls cannot be manipulated or restricted behind a paywall, safeguarding users' rights to data privacy. Additionally, regulations should prevent service providers from manipulating choice architecture as a trust-building strategy while maintaining data collection, as previous studies have demonstrated [13, 81].

Furthermore, we believe that the HCI community, particularly privacy researchers, has a responsibility to assist users in making informed privacy decisions. Our results indicate that users often struggle to understand the implications of data privacy controls, questioning their efficacy and necessity, especially when the controls are offered for seemingly low-risk IoT devices. To mitigate these challenges, privacy researchers should develop and validate strategies for effective privacy risk communication and educate users about the implications of privacy controls. While current suggestions for offering privacy notices and labels can be helpful in informing users about device data practices [20, 21, 28, 69], however, these notices standalone may not be enough for the concerns users' have regarding the contradictory nature of the manufactures' profit model and offering of data security and privacy. Towards this end, empowering users with tools and education to reduce cognitive overload while making privacy decisions remains an ongoing challenge that requires careful attention.

5.2 Tradeoff between Data Privacy Controls and Money

Our incentive-compatible lottery study reveals an interplay of several factors influencing users' choices between receiving additional data privacy controls and money. We observed that participants' decision to choose the premium plan over receiving money was impacted by the underlying risk factors and data sensitivity associated with the IoT device. Compared to the *Low-risk: light bulb* condition, participants in the *High-risk: camera* condition exhibited

a significantly increased likelihood of choosing the premium plan instead of receiving money.

Interestingly, Ul Haque et al.'s work in the hypothetical setup found that participants' WTP for the premium data management plan did not vary significantly between the *High-risk: camera* vs. *Low-risk: light bulb* conditions [80]. In comparison, our incentive-compatible study revealed that, when participants calculate the tradeoff between choosing additional data management options or receiving money by giving up additional data management controls, the perceived risk of the data collected by the IoT device of interest plays a crucial role. This aligns with prior efforts indicating that users perceive risks associated with different IoT devices differently, impacting their privacy expectations and preferences [29]. Our results further unfold the nuances of users' decision-making process, especially when a monetary tradeoff for privacy is present. We found that participants often viewed IoT manufacturers and their privacy offerings negatively when considering low-risk devices, such as the smart light bulbs in our study. This challenges prior findings that users are consistently willing to pay for data privacy [30, 31], highlighting the importance of context and conditions when evaluating privacy against monetary costs. Our findings, supported by qualitative evidence, provide clarity on these critical scenarios.

Furthermore, irrespective of their assigned IoT device, participants in the $9.99 conditions were significantly more likely to choose the premium plan than the $29.99 conditions. Qualitative data further complemented this finding by revealing that participants' valuation of the premium plan features often influenced them to choose the premium plan instead of receiving money. These findings suggest that participants performed monetary valuations of the yearly subscription fee of the offered premium data management plan and decided to choose the premium data management option at a higher rate when the offered cash option was at a lower price point, irrespective of the IoT device. Hence, the cash option of $9.99 is likely lower than their monetary valuation of the premium plan. In contrast, the cash option of $29.99 is likely higher than their valuation of the premium plan for a $29.99 IoT device. This is likely based on their *true* valuation of the premium plan, as prior effort suggests [86].

We observed an interaction between participants' technical literacy and the offered cash option, which likely corresponds to the difference in WTP between technical and non-technical participants. Towards that, Ul Haque et al.'s effort revealed participants' technical literacy to be a significant predictor of their self-reported WTP for the yearly subscription fee of the premium data management plan, mediated by the understandability of the data management plan features [80]. Higher technical literacy was found to be impacting participants' understandability of the premium plan features, which might led to a higher WTP for the premium plan, especially for the higher price points of the WTP (i.e., "expensive" and "too expensive" price points [80]). Hence, technical participants are likely to have a higher understanding of the premium plan features, leading to an overall higher monetary valuation than non-technical participants. This likely caused technical participants to choose *Option A: premium plan* at a significantly higher rate in the $29.99 condition.

5.3 Challenges in Eliciting Users' True Preferences for Privacy

Exploring the monetary valuation of privacy at the time of purchase is a significant focus in HCI research. However, replicating users' true behavior at the point of purchase is challenging. To address the difficulty in measuring users' preferences, studies often use hypothetical approaches, such as contingent valuation [12, 83], where participants report their hypothetical WTP for a product. As discussed in Section 2.2, hypothetical measures can deviate significantly from actual WTP due to hypothetical bias and lack of incentives [39, 59].

To investigate genuine user preferences, researchers should implement incentive-compatible approaches. The selection of such an approach should be tailored to the study's goals. For instance, Emami-Naeini et al. [30] used a Multiple Price List (MPL) method, enabling the quantification of WTP for privacy constructs. MPL is straightforward and easy to implement but has limitations: it relies on discrete choices, which, if too broad, can be cognitively taxing, and if too narrow, may miss true WTP ranges [6]. Additionally, as an indirect method, MPL might differ from the real purchase process.

In contrast, our direct lottery-based incentive-compatible approach offered the choice between privacy and money, closely replicating the considerations users face when purchasing an IoT product with a trade-off between privacy and money. As users are familiar with lottery setups, the setup required minimal familiarization. Another advantage of the setup was its potential for explaining participants' thought processes, potentially revealing behavioral insights and the reasoning behind their choices, as illustrated in post-lottery choice responses. This is particularly difficult in a setup like MPL due to the presence of multiple price point considerations, which can obscure the reasons for accepting or rejecting certain points.

Nonetheless, ensuring the effectiveness of our approach required careful considerations. Although the overall lottery setup is intuitive, we needed to verify that the premium plan option and its feature offerings were clearly explained and understood. To do that, we included a manipulation check question after the lottery choice to confirm participants' comprehension of the basic and premium plans. Participants who failed the check were removed. Also, we wanted to ensure that our participants were interested in the offered rewards, which we addressed by pre-screening participants and only included those who were not current users and were interested in receiving the offered IoT devices.

Despite the advantages of our setup and its effectiveness for our specific research target, there are some drawbacks to consider when determining its suitability for a given research need. For instance, this method can be resource-intensive, necessitating careful planning and significant budgets (e.g., payments for the lottery). Further, precise WTP quantification remains difficult and may require narrower price intervals, similar to MPL. If quantifying users' WTP for a specific product is the primary research goal, other direct incentive-compatible WTP elicitation methods, such as the Becker-DeGroot-Marschak (BDM) method [10], may be more suitable. Nonetheless, researchers should be cautious about

the potential limitations of these approaches. For instance, the auction component of BDM may necessitate strategic maneuvers that participants may find difficult to grasp [14].

5.4 Disconnection between Perceived and Actual Risks associated with IoT

Our findings demonstrate that users' perceived risks associated with the IoT devices under consideration significantly influence both their perception of the additional controls in the premium plan and their choice in the lottery. Specifically, we observed that participants in the *Low-risk: light bulb* condition were significantly more likely to choose the cash option and indicated in their post-lottery Likert responses that the device (i.e., light bulbs) does not collect sensitive data that would necessitate the premium plan controls.

This perception of smart light bulbs as seemingly benign and low-risk suggests a disconnect between users' perceived risks associated with these IoT devices and the actual risks they may pose, which likely has implications for data privacy as well. As the contextual integrity framework suggests, these seemingly benign smart devices deployed in users' private settings can potentially violate both the *Appropriateness* and *Distribution* norms, implying a breach of data privacy [62]. For example, sensor data collected by smart light bulbs can be used to infer sensitive behavioral patterns related to users' behavior and personal spaces (e.g., their home), such as when they leave the house and return, when they go to bed and wake up, among other things. Access to these patterns by malicious actors can lead to data privacy breaches and physical security threats.

Therefore, it is crucial to educate consumers about how seemingly low-risk devices can pose potential privacy risks. Risk communication approaches focusing on bridging the gap between perceived and actual privacy risks can be effective in achieving this goal.

5.5 Difficulty in Defining 'Premium' Features

Our results suggest that reaching an agreement between consumers and service providers regarding what should be considered premium features and included in a 'pay for privacy' model may be challenging. While offering additional controls over third-party data sharing and usage can directly impact service providers' data-oriented businesses and thus be considered premium features for which they may charge a fee, participants' responses indicated that they view these data privacy controls as fundamental and should be free.

Our findings indicate that achieving such consensus may not be straightforward. For example, our participants often found data deletion behind a paywall to be the most intrusive option and voiced their opposition, likely stemming from their perception of their right to personal data. On the other hand, participants frequently questioned the need for additional controls for light bulbs, which collect data that is perceived to be of low risk and sensitivity, and, therefore, not worthy of a premium offering.

Hence, to reach a consensus on the definition of premium features, both legislative guidance defining users' rights for data privacy and the underlying context in which the premium plan is deployed should be considered.

5.6 Design Recommendations for 'Pay for Privacy'

To establish a balance between users' privacy preferences and businesses' needs to incorporate the model into their revenue structures, we curated a list of recommendations for the existing 'pay for privacy' model based on our findings. These recommendations also emphasize the importance of respecting user data privacy and maintaining a healthy provider-consumer relationship.

First, businesses should make fundamental privacy options, such as options to delete cloud stored data, free and inclusive with the product offering, while more advanced features can be included as premium tiers. This aligns with our participants' strong negative reactions to encountering basic privacy options locked behind a paywall. While this strategy may not directly contribute to profit, it can potentially lead to perceived goodwill among users. Our participants pointed out that monetizing basic privacy rights can lead to doubts and distrust about the company's intentions, potentially causing participants to decline services and choose alternatives [51]. Therefore, including certain built-in privacy options in the product offering should help build trust with the user base, which has been shown to be crucial for business sustainability and growth [8, 19].

Second, While participants expect fundamental options like the right to delete cloud-stored data inclusive, features that enhance utility without compromising the right to privacy should be considered premium. For instance, personalized services that leverage user data beyond basic device functionality to offer convenience and value could be premium offerings. For smart security cameras, premium features might include offering dynamic and person-specific privacy zones - where users can create personalized zones that adapt to specific events, or where a camera can detect individual family members and automatically blur their faces in recordings. Offering personalized privacy shields where sensitive activities can be automatically detected, and recording can be paused might also be a premium option for indoor security cameras. These personalized features align with the user's suggestion that premium options should not restrict core device functionality.

Third, businesses should carefully consider the risks and benefits of employing a subscription-based 'pay for privacy' model. Despite the popularity and excessive inclusion of subscription-based premium tiers in company business models, our results suggest that participants dislike being locked into subscriptions and feel burdened by the notion of everything becoming a subscription service, contributing to the phenomenon known as 'subscription fatigue.' Hence, depending on the characteristics of the features, offering certain premium features as a one-time price increase for the device could be more appealing to users, as indicated by participant feedback.

Finally, a "one-size-fits-all" approach to the 'pay for privacy' model should be avoided. Our study finding suggests that user sentiment towards the premium offering significantly differed based on the associated IoT device. Hence, the device context and perceived risks should factor into the curation of features in a premium offering. For instance, deidentified cloud storage could be a premium plan feature only if deidentification of device-collected data is guaranteed. In the case of smart security cameras that capture users' videos and facial information, deidentification might not be feasible.

Instead, providing local file storage options could be a more suitable option.

To address this, when developing a tiered 'pay for privacy' model, it is crucial to consider several important aspects carefully. For instance, the tiered offering should cater to different user needs through distinct levels, including offering a free or minimally priced basic option and allowing users to opt out of higher tiers. Additionally, these tiers should offer users the choice and flexibility to select a plan based on their specific needs. Further, even with a tiered premium model, manufacturers should ensure the device remains fully functional for users who do not purchase the premium offering. Finally, offering users a free trial of the premium plan can be effective, allowing them to experience the product before committing based on their individual needs and preferences.

6 Limitations of the Study

We took several measures, such as screening and employing attention and manipulation checks, to ensure the study's internal validity and data quality. However, the reported findings should be interpreted while considering the following limitations.

First, our study recruited participants through the Prolific platform who are adults residing in the United States. These participants possess the technical ability to use Prolific and participate in online surveys, which may not be representative of the general population of the United States.

Second, we conducted an incentive-compatible lottery study to prevent participants from self-reporting their preferences between privacy and money. However, despite having incentive compatibility in place, participants' responses to the lottery may not directly correlate with participants' privacy vs. money tradeoff calculations at the point of the purchase in real life, which needs to be investigated.

Third, the features included in our study's premium data management plan were drawn from prior research investigating user expectations regarding IoT device data management in the United States [29, 31, 80]. Consequently, consumers from different regions (e.g., Europe, Asia) with varying privacy norms and regulations (e.g., General Data Protection Regulation (GDPR) applicable for EU countries [23]) may hold different privacy expectations and exhibit different attitudes toward the premium plan.

Fourth, our work incorporated multiple demographic factors (e.g., age, gender, income level) in the statistical model but observed no significant effect. However, to limit the scope of the study, we could not consider all possible factors in our study (e.g., Big-five personality factors, risk-taking tendency) that might be relevant to privacy decision-making, but were not explored to keep the study tractable. However, as participants were assigned to different groups randomly, these factors are likely to be evenly distributed across the groups, hence, not impacting the group differences observed in the study. Future efforts can expand on our findings to explore whether and how users' personality traits and attributes affect participants' privacy decision-making.

Finally, to avoid overwhelming participants, we incorporated only four data privacy controls in our data management plans, curated based on prior research on users' privacy exceptions from IoT devices [29, 31]. As such, user perceptions may vary depending on a different set of data management controls, and further research is warranted to investigate the influence of such variations.

7 Conclusion

This study investigated users' choices between premium data management offerings and monetary options in an incentive-compatible lottery study. Our findings revealed that factors such as the risks associated with an IoT device and the cash conditions play significant roles in users' calculations when weighing the tradeoff between additional privacy options and money. Additionally, participants' technical literacy significantly interacted with their choices. By qualitatively analyzing participant responses, we identified users' reasons behind their lottery choices, as well as their reasoning behind accepting and rejecting the 'pay for privacy' model, and discussed the implications of our findings for user data privacy.

Acknowledgments

This research was supported by a NSF CAREER award to the second author, 1750908. We would like to thank the anonymous reviewers for their valuable feedback and suggestions that helped to improve the paper. We would also like to thank Zhelun Rong for his assistance with the data analysis.

References

[1] Alessandro Acquisti and Jens Grossklags. 2005. Uncertainty, Ambiguity and Privacy.. In *WEIS*.
[2] Alessandro Acquisti and Jens Grossklags. 2007. What can behavioral economics teach us about privacy? In *Digital privacy*. Auerbach Publications, 363–378.
[3] Alessandro Acquisti, Leslie K John, and George Loewenstein. 2013. What is privacy worth? *The Journal of Legal Studies* 42, 2 (2013), 249–274.
[4] 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.
[5] Gabe Turner Aliza Vigderman. 2022. The Data Big Tech Companies Have On You. (2022). https://www.security.org/resources/data-tech-companies-have/
[6] Steffen Andersen, Glenn W Harrison, Morten Igel Lau, and E Elisabet Rutström. 2006. Elicitation using multiple price list formats. *Experimental Economics* 9 (2006), 383–405.
[7] Steffen Anderson, Glenn W Harrison, Morten I Lau, and Rutstrom E Elisabet. 2007. Valuation using multiple price list formats. *Applied Economics* 39, 6 (2007), 675–682.
[8] 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.
[9] 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.
[10] Gordon M Becker, Morris H DeGroot, and Jacob Marschak. 1964. Measuring utility by a single-response sequential method. *Behavioral science* 9, 3 (1964), 226–232.
[11] Yoav Benjamini and Yosef Hochberg. 1995. Controlling the false discovery rate: a practical and powerful approach to multiple testing. *Journal of the Royal statistical society: series B (Methodological)* 57, 1 (1995), 289–300.
[12] 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.
[13] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced confidences: Privacy and the control paradox. *Social psychological and personality science* 4, 3 (2013), 340–347.
[14] Sarah Brebner and Joep Sonnemans. 2018. Does the elicitation method impact the WTA/WTP disparity? *Journal of behavioral and experimental economics* 73 (2018), 40–45.
[15] Barry Brown. 2001. Studying the internet experience. *HP laboratories technical report HPL* 49 (2001).
[16] Magdalena Brzozowicz et al. 2018. Hypothetical bias and framing effect in the valuation of private consumer goods. *Central European Economic Journal* 5, 52 (2018), 260–269.

[17] Kenneth P Burnham and David R Anderson. 2004. Multimodel inference: understanding AIC and BIC in model selection. *Sociological methods & research* 33, 2 (2004), 261–304.

[18] 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/

[19] 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.

[20] Peter Caven, Zitao Zhang, Jacob Abbott, Xinyao Ma, and L Jean Camp. 2024. Comparing the Use and Usefulness of Four IoT Security Labels. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–31.

[21] Claire C Chen, Dillon Shu, Hamsini Ravishankar, Xinran Li, Yuvraj Agarwal, and Lorrie Faith Cranor. 2024. Is a Trustmark and QR code enough? The effect of IoT security and privacy label information complexity on consumer comprehension and behavior. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–32.

[22] Robert B Cialdini. 2009. *Influence: Science and practice*. Vol. 4. Pearson education Boston.

[23] European Commission. 2018. EU Data Protection Rules. (2018). https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

[24] Joost CF De Winter and Dimitra Dodou. 2010. Five-point Likert items: t test versus Mann-Whitney-Wilcoxon. *Practical assessment, research & evaluation* 15, 11 (2010), 1–12.

[25] 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.

[26] deleteme.com. 2023. How to Request to Delete Personal Data. (2023). https://joindeleteme.com/blog/how-to-request-to-delete-personal-data/

[27] Ben Derrick and Paul White. 2017. Comparing two samples from an individual Likert question. *International Journal of Mathematics and Statistics* 18, 3 (2017), 1–13.

[28] 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.

[29] 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.

[30] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. 2023. Are Consumers Willing to Pay for Security and Privacy of IoT Devices? (2023).

[31] 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.

[32] Giulia Torchio epc.eu. 2023. Meta's 'Pay or Okay': Is this the final challenge for EU GDPR? (2023). https://www.epc.eu/en/publications/Metas-Pay-or-Okay-Is-this-the-final-challenge-for-EU-GDPR~5672dc

[33] Asunción Esteve. 2017. The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. *International Data Privacy Law* 7, 1 (2017), 36–47.

[34] Andy Field. 2013. *Discovering statistics using IBM SPSS statistics*. sage.

[35] Vaibhav Garg. 2021. A Lemon by Any Other Label. *ICISSP* (2021), 558–565.

[36] Alvin W Gouldner. 1960. The norm of reciprocity: A preliminary statement. *American sociological review* (1960), 161–178.

[37] Christopher Hadnagy. 2010. *Social engineering: The art of human hacking*. John Wiley & Sons.

[38] Christian Happ, André Melzer, and Georges Steffgen. 2016. Trick with treat–Reciprocity increases the willingness to communicate personal data. *Computers in Human Behavior* 61 (2016), 372–377.

[39] 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.

[40] 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.

[41] Joel L Horowitz and NE Savin. 2001. Binary response models: Logits, probits and semiparametrics. *Journal of economic perspectives* 15, 4 (2001), 43–56.

[42] Ross Ihaka and Robert Gentleman. 1996. R: a language for data analysis and graphics. *Journal of computational and graphical statistics* 5, 3 (1996), 299–314.

[43] Harris Interactive. 2019. Consumer internet of things security labelling survey research findings. *Google Scholar Google Scholar Navigate to* (2019).

[44] B Kelsey Jack, Kathryn McDermott, and Anja Sautmann. 2022. Multiple price lists for willingness to pay elicitation. *Journal of Development Economics* 159 (2022), 102977.

[45] Daniel Kahneman, Jack L Knetsch, and Richard H Thaler. 1990. Experimental tests of the endowment effect and the Coase theorem. *Journal of political Economy* 98, 6 (1990), 1325–1348.

[46] 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.

[47] 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.

[48] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 3393–3402.

[49] J Richard Landis and Gary G Koch. 1977. The measurement of observer agreement for categorical data. *biometrics* (1977), 159–174.

[50] 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/

[51] 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.

[52] Jayson L Lusk, Deacue Fields, and Walt Prevatt. 2008. An incentive compatible conjoint ranking mechanism. *American Journal of Agricultural Economics* 90, 2 (2008), 487–498.

[53] 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.

[54] Nick Mehta, Dan Steinman, and Lincoln Murphy. 2016. *Customer success: How innovative companies are reducing churn and growing recurring revenue*. John Wiley & Sons.

[55] 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/

[56] Matthew B Miles and A Michael Huberman. 1994. *Qualitative data analysis: An expanded sourcebook*. sage.

[57] Kevin D Mitnick and William L Simon. 2003. *The art of deception: Controlling the human element of security*. John Wiley & Sons.

[58] 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.

[59] 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.

[60] 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.

[61] 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.

[62] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[63] Patricia A Norberg, Daniel R Horne, and David A Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of consumer affairs* 41, 1 (2007), 100–126.

[64] Eyal Peer, David Rothschild, Andrew Gordon, Zak Evernden, and Ekaterina Damer. 2022. Data quality of platforms and panels for online behavioral research. *Behavior Research Methods* (2022), 1.

[65] Rindang Bangun Prasetyo, Heri Kuswanto, Nur Iriawan, and Brodjol Sutijo Suprih Ulama. 2020. Binomial regression models with a flexible generalized logit link function. *Symmetry* 12, 2 (2020), 221.

[66] Cpi pymnts.com. 2024. Privacy Advocates Urge European Regulators to Oppose Meta's No-Ads Subscription Model. (2024). https://www.pymnts.com/cpi_posts/privacy-advocates-urge-european-regulators-to-oppose-metas-no-ads-subscription-model/

[67] 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.

[68] Naveed Saif, Nasir Razzaq, Muhammad Amad, and Sajid Gul. 2012. Factors affecting consumers' choice of mobile phone selection in Pakistan. *European Journal of Business and Management* 4, 12 (2012), 16–26.

[69] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In *Eleventh symposium on usable privacy and security (SOUPS 2015)*. 1–17.

[70] Bruce Schneier and B Schneier. 2003. *Beyond fear: Thinking sensibly about security in an uncertain world*. Vol. 10. Springer.

[71] 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.
[72] Lennart Sjöberg, Bjorg-Elin Moen, and Torbjorn Rundmo. 2004. Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research. *Rotunde publikasjoner Rotunde* 84 (2004), 55–76.
[73] 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.
[74] 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.
[75] Jennifer Fries Taylor, Jodie Ferguson, and Pamela Scholder Ellen. 2015. From trait to state: Understanding privacy concerns. *Journal of Consumer Marketing* (2015).
[76] techxplore.com. 2023. Rise of the web's 'pay for privacy' model. (2023). https://techxplore.com/news/2023-12-web-pay-privacy.html
[77] 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.
[78] Monique Mitchell Turner, Christine Skubisz, and Rajiv N Rimal. 2011. Theory and practice in risk communication: A review of the literature and visions for the future. *The Routledge handbook of health communication* (2011), 174–192.
[79] T Tzuo. 2018. Subscribed: Why the Subscription Model Will Be Your Company's Future-and What to Do About It.
[80] 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 *Proceedings of the 2023 European Symposium on Usable Security*. 68–85.
[81] 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.
[82] Ehsan Ul Haque, Mohammad Maifi Hasan Khan, Md Abdullah Al Fahim, and Theodore Jensen. 2023. Divergences in Blame Attribution after a Security Breach based on Compliance Behavior: Implications for Post-breach Risk Communication. In *Proceedings of the 2023 European Symposium on Usable Security*. 27–47.
[83] Lingappan Venkatachalam. 2004. The contingent valuation method: a review. *Environmental impact assessment review* 24, 1 (2004), 89–124.
[84] 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/
[85] Tatum Hunter washingtonpost.com. 2021. Companies are hoarding personal data about you. Here's how to get them to delete it. (2021). https://www.washingtonpost.com/technology/2021/09/26/ask-company-delete-personal-data/
[86] Klaus Wertenbroch and Bernd Skiera. 2002. Measuring consumers' willingness to pay at the point of purchase. *Journal of marketing research* 39, 2 (2002), 228–241.
[87] Wikipedia contributors. 2024. Subscription business model — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Subscription_business_model&oldid=1241951474 [Online; accessed 13-September-2024].
[88] Morgan Meaker wired.com. 2023. Facebook Finally Puts a Price on Privacy: It's $10 a Month. (2023). https://www.wired.com/story/meta-facebook-pay-for-privacy-europe/
[89] Tao Zhou. 2011. The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems* (2011).
[90] 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 the following URL: https://raw.github.com/ehsan-ashik/wtp-lottery-study/main/survey_instrument.pdf.

Metric	Levels	Gr 1A	Gr 1B	Gr 1C	Gr 2A	Gr 2B	Gr 2C
Age	-	M = 40.58 SD = 10.57	M = 37.93 SD = 12.36	M = 45.61 SD = 15.63	M = 40.0 SD = 12.22	M = 35.65 SD = 10.15	M = 41.87 SD = 14.5
Gender	Man	16	15	17	20	25	13
	Woman	27	28	23	25	17	33
	Non-binary	2	0	1	0	1	1
	Prefer not to Answer	0	0	0	1	0	0
Education	Less than high school	0	0	0	0	1	2
	High School graduate or GED	7	9	5	6	5	4
	Some College	16	7	12	9	14	12
	2-year degree	3	4	6	4	2	8
	4-year degree	15	13	11	17	16	16
	Master's degree	3	9	5	9	4	4
	Doctoral degree	0	0	0	1	1	0
	Professional degree	1	1	2	0	0	1
Employment	Employed full time	28	19	19	24	21	19
	Employed part time	4	8	4	5	4	4
	Self-employed	3	5	6	4	8	3
	Care-provider	0	0	1	1	0	0
	Homemaker	2	1	3	4	1	8
	Retired	2	2	4	2	0	5
	Student	2	4	1	1	0	2
	Disabled	2	1	0	1	2	4
	Unemployed, not looking for work	0	0	0	0	1	0
	Unemployed, looking for work	2	3	3	4	6	2
Income	$0	0	0	0	3	2	1
	$1 to $9,999	9	6	6	4	7	11
	$10,000 to $24,999	9	7	8	5	5	12
	$25,000 to $49,999	12	7	9	14	11	10
	$50,000 to $74,999	4	8	11	6	6	7
	$75,000 to $99,999	3	5	3	7	3	3
	$100,000 to $149,999	5	8	3	4	4	1
	$150,000 and greater	3	1	1	2	4	2
	Prefer not to answer	0	1	0	1	1	0
		N = 45	*N = 43*	*N = 41*	*N = 46*	*N = 43*	*N = 47*

Table 4: Participant demographics by groups.

A.2 Demographics Summary

Table 4 shows a group-wise summary of participants' demographics.

A.3 IoT Usage Statistics

Figure 3 reports participants' household IoT device usages in the Prolific platform.

A.4 Images of the IoT Devices Used in the Study

Figure 4 presents the edited-out versions of the images of the IoT devices we used in the study. In the *High-risk: camera* group, the reference IoT device was an indoor smart home security camera, and in the *Low-risk: light bulb* group, the reference device was a smart light bulb with motion sensor. We edited out all the brand-related information from the images to avoid biasing the participants.

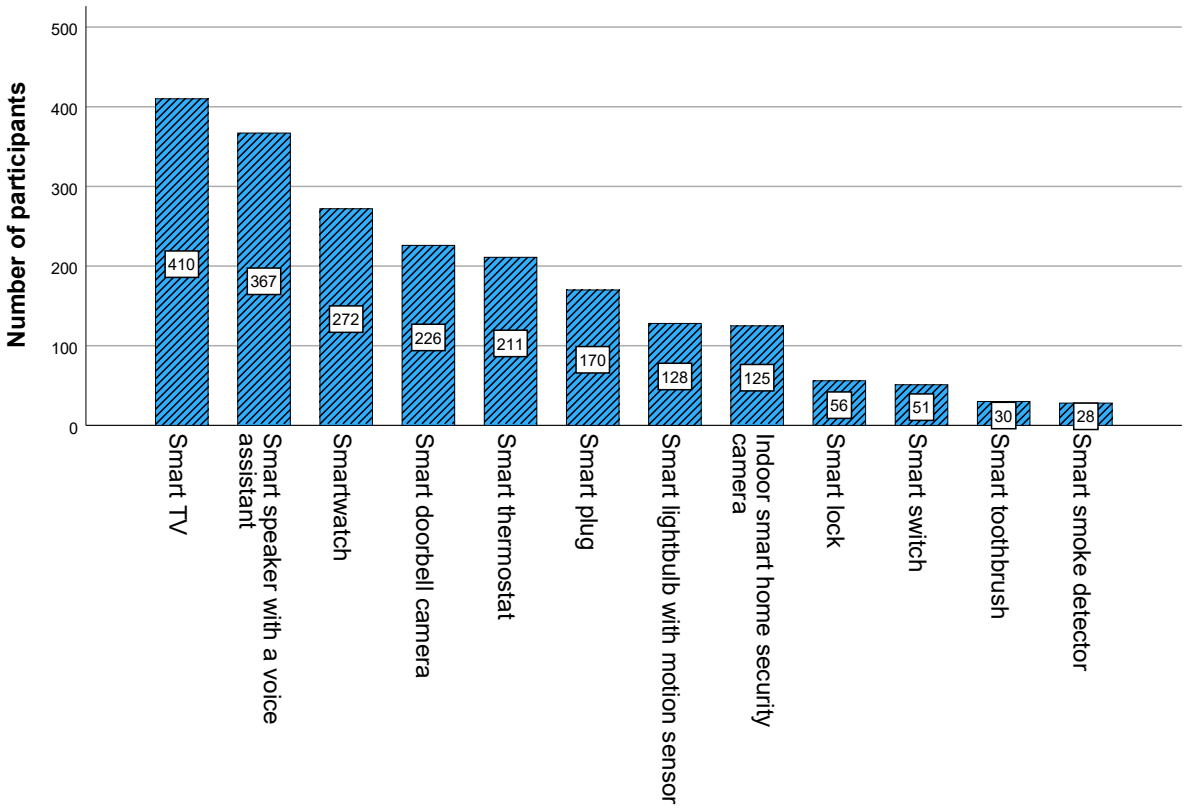

Figure 3: IoT device usages reported by our participants in phase one study.

Figure 4: IoT device images used in the study. Indoor smart-home security camera in the HR group (top) and Smart light bulb with motion sensor in the LR group (bottom). The brand related information is edited out.

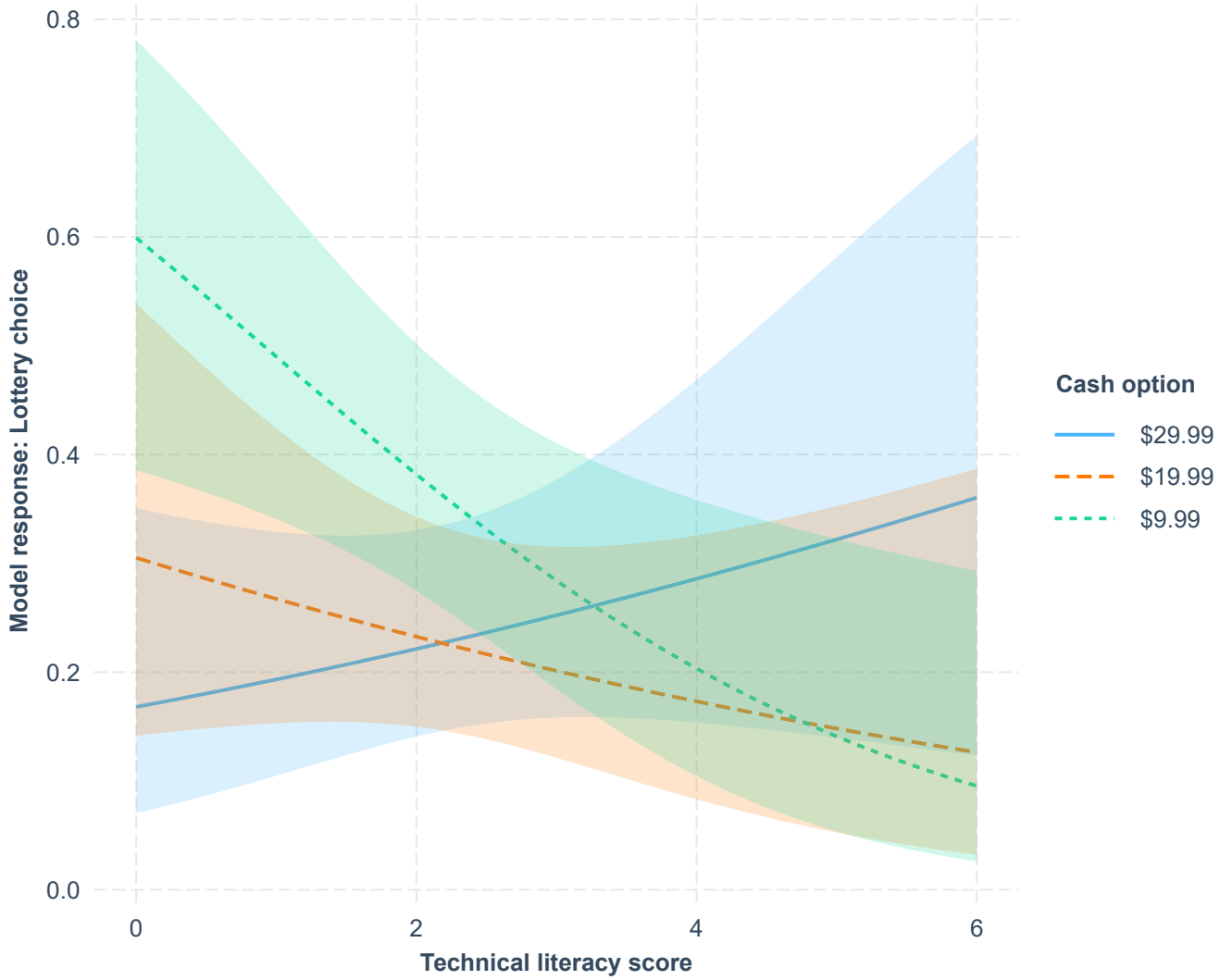

Figure 5: Interaction plot of technical literacy and cash options from the model.

A.5 Visualization of Observed Interaction

Figure 5 shows the plot indicating the interaction of technical literacy and cash option, predicted by the model and described in Section 4.3.