User Perceptions and Experiences with Smart Home Updates

Julie M. Haney[§] and Susanne M. Furman[§]
National Institute of Standards and Technology
Gaithersburg, MD, USA
{*julie.haney, susanne.furman*}*@nist.gov*

***Abstract*—Updates may be one of the few tools consumers have to mitigate security and privacy vulnerabilities in smart home devices. However, little research has been undertaken to understand users' perceptions and experiences with smart home updates. To address this gap, we conducted an online survey of a demographically diverse sample of 412 smart home users in the United States. We found that users overwhelmingly view smart home updates as important and urgent. However, relationships between update perceptions and security and privacy perceptions are less clear. We also identify problematic aspects of updates and gaps between current and preferred update modes. We then suggest ways in which update mechanisms and interfaces can be designed to be more usable and understandable to users.**

***Index Terms*—smart homes, internet of things, security, privacy, human computer interaction**

1. Introduction

About half of all households in the United States (U.S.) have at least one Internet of Things (IoT) smart home device, with adoption on the rise [28] [41]. As the market continues to expand, more consumers will need to protect their devices from security or privacy exposures and attacks. However, smart home users may not be security-savvy and seldom have professional support to maintain their smart home devices [23]. They must manage and secure the devices on their own, including performing maintenance tasks like updates. These tasks may become especially burdensome for users who own multiple smart home devices.

Smart home updates may add or fix functionality but are also a critical mechanism by which manufacturers can distribute patches to remediate security vulnerabilities. Moreover, updates may be one of the few tools that consumers have to secure their smart home devices since other configurable security options are limited or unavailable [13]. Failure to install updates may leave devices vulnerable.

Despite the importance of updates, users do not always apply updates in a timely fashion. In related research about software updates, studies have found that users may hesitate to apply updates for a variety of reasons, including not understanding the purpose and importance of updates and the disruptions updates may cause [26] [48]. However, no large-scale study has investigated experiences with *smart home* updates through the eyes of home users. In addition, it is unclear as to whether the same obstacles encountered with software updates also apply in the smart home domain. These gaps result in little substantive, evidence-based guidance that can be provided to smart home device manufacturers and other stakeholders (e.g., standards developers, regulators, consumer advocacy groups) to improve consumers' update experiences.

To better understand consumer perceptions about and experiences with smart home updates, we conducted an online survey of a demographically diverse sample of 412 U.S. smart home users. We targeted participants who were active users of smart home devices in five categories of interest: virtual voice assistants, smart thermostats, smart security devices, smart environment sensors, and smart lighting. We sought to answer the following research questions:

RQ1: What do users think are the main reasons to update their smart home devices?
RQ2: What do users think about the importance and urgency of smart home updates? What differences exist between device categories and demographic groups?
RQ3: What issues/problems with smart home updates do users encounter?
RQ4: What update installation and notification modes do users' smart home devices currently support? What would be preferred?
RQ5: What are users' perceptions of smart home security and privacy and how do those relate to perceptions of update importance and urgency? What differences exist between device categories and demographic groups?

Our study makes several contributions. We extend prior research on user experiences with software updates into the smart home domain, identifying areas of similarity and divergence. We discover differences in consumers' update experiences and perceptions depending on device category and demographics and how update perceptions relate to security and privacy perceptions. We also identify problematic aspects of smart home updates and gaps between what devices currently provide and what users would prefer. Finally, we propose suggestions to help guide efforts

§. Designated as co-first authors

undertaken by the smart home community – manufacturers, standards developers, regulators, security and privacy consortia, consumer advocacy groups – to implement usable update mechanisms and interfaces that could also result in improved device security.

2. Related Work

2.1. Software Updates

Prior discoveries about user behaviors and challenges with updates of traditional software are valuable as an initial frame of reference for smart home update behaviors. Researchers found that users were more likely to install updates perceived as "major," for example a new operating system version or a security fix [25]. However, they had had a difficult time determining the value of an update because they often lacked information about what the update did and why it was needed, especially when the system or application seemed to be working well without the update [11] [26] [48]. Users may never become aware that an update is needed due to inconsistent or non-automated notification methods, confusion about how automatic updates work or if they are turned on, or concern that notifications are a scam [49] [50]. Moreover, because of the lack of information, some users had a difficult time understanding the relationship between software updates and security, which may result in a decreased sense of urgency to apply updates [11]. Users also may lack an accurate mental model of what updates are doing, especially when applied automatically [50]. The disruptive nature of updates also contributes to hesitance to apply updates, as updates may interrupt computing activities and have unknown installation times [14] [26].

While some users preferred automatic updates, others desired more control [14] [49]. In the smartphone context, users most often activated automatic updates for convenience and for software to stay current [14] [24]. Those who avoided automatic updates tended to have less tolerance for risk, less trust in the applications, and prior negative update experiences [25] [24] [48]. For example, if an automatic update does something unexpected or unwanted, users felt betrayed and lost trust in automatic updates.

Ultimately, users must balance risks and costs of updating against potential benefits [49]. They want to know what the update involves to determine whether they want the changes [24] [49]. Therefore, it is recommended that manufacturers make it easy for users to find update information, communicate the importance, and provide a recovery path should updates cause unintended consequences [11] [25] [49]. To further improve usability, users could be provided the ability to customize update modalities, for example, setting updates to install automatically or configuring the frequency of update notifications [14] [25].

2.2. Internet of Things Updates

As a foundation for our study, we discuss the current state of and prior publications about IoT updates.

2.2.1. State of IoT Updates. A number of critical security vulnerabilities for IoT devices have been identified in recent years, highlighting the need for timely updates [2]. Government regulatory organizations, such as the U.S. Federal Trade Commission (FTC) [22] and the U.S. Consumer Product Safety Commission [5], view IoT device updates as important consumer protections for security, privacy, and safety reasons.

Despite the criticality of IoT updates, inducing consumers to regularly update devices may still pose a challenge. Beyond issues experienced with traditional software updates, there are unique usability challenges for IoT updates [15]. IoT manufacturers may be new to the connected devices market and inexperienced with designing usable and secure update mechanisms. While users have grown accustomed to computer and mobile device operating systems that are typically updated regularly and automatically, there are no such routine update services for many IoT devices [13] [23]. Furthermore, IoT update-related information available to users may be lacking and inconsistently provided [13] [15].

Update modes (updates being automatic or requiring manual intervention) have also been found to be inconsistent across smart home devices. A 2019 report from the National Institute of Standards and Technology (NIST) described a lab analysis of security mechanisms (including update modes) in consumer smart home IoT devices [13]. NIST examined three different smart home devices in several device categories, including categories aligned with our categories of interest: security cameras/doorbells, lightbulbs/lighting, and thermostats. They found that, while all lighting devices required manual updates, thermostats and security devices had a mix of automatic and manual updates.

Since RQ4, in part, was aimed at identifying current and preferred update modes, we supplement the NIST research with a brief, more-recent analysis of popular (based on market share) smart home devices as a point of comparison. For each of our five device categories of interest, we surveyed the update options of three devices from three different manufacturers by conducting internet searches and hands-on examination when possible (Table 1). We found varying update mode options, with manual updates being more common for sensors and lighting devices and some devices only offering automatic updates. While our brief market analysis cannot fully capture the diversity of smart home devices and manufacturers, it does provide more recent evidence that update modes are inconsistent across devices.

2.2.2. IoT Update Research. Few research efforts addressed smart home updates from the end-user perspective. Investigating which privacy and security attributes might impact IoT purchases, one group found that some users misinterpreted the need for updates as indicating poor product security [7]. They also found that users thought automatic updates decrease risk, but many would like to know the details of updates and desire more control over which updates are installed. In an interview study [17], researchers discovered that users were frequently confused about how and

TABLE 1. UPDATE MODES FOR A SAMPLE OF POPULAR SMART HOME DEVICES

Category	Device*	Update Mode
Voice assistants	Device 1	A
	Device 2	B
	Device 3	B
Thermostats	Device 1	B
	Device 2	A
	Device 3	B
Security devices	Device 1	A
	Device 2	B
	Device 3	B
Sensors	Device 1	A
	Device 2	M
	Device 3	M
Lighting	Device 1	B
	Device 2	M
	Device 3	M

Update Mode: A=automatic only; M=manual only; B=both automatic and manual options available.
* Per our institutional policy, names of device manufacturers or models are not included.

if smart home updates are applied, were concerned about updates causing compatibility issues with other products, and seldom linked updates to security. Another study found that their German participants did not consider updates for smart consumer devices to be as important as updates for their smartphones, largely because they did not understand how changes to the consumer devices might be beneficial [14]. To address IoT update shortfalls, recommendations from researchers and standards organization included: increasing transparency about update purpose and importance; providing options for configuring preferences for update notifications and installation; and applying updates with little or no user intervention [8] [10] [9] [12] [14] [17] [23].

While helpful for beginning to identify update challenges, these papers were not primarily focused on smart home updates, with qualitative results (as in [17]) not generalizable to the U.S. smart home user population. Our study addresses this gap through a larger-scale, quantitative, and update-focused survey of demographically diverse smart home users from across the U.S.

2.3. Demographic Influences

For RQ2 and RQ5, we wanted to know the influences of participant demographics. In choosing specific demographic groups of interest, we consulted prior work that identified potential influences on technology attitudes and behaviors. Past research revealed that older adults may be less likely to adopt new technologies [29], are often challenged to implement security measures [36] [38], and may be more fearful of privacy and security exposures [37]. Women have displayed less confidence in privacy protections [3] [30] and less security and computer self-efficacy [1]. Education has been observed to influence smart home trust perceptions and ratings of the likelihood of device security or privacy being compromised [3]. A prior study observed differences in the routinization of smart home usage depending on length of experience [3]. Additionally, marked differences have been observed in the sophistication and accuracy of security and privacy mental models and risk understanding between experts and non-experts [20] [45]. Based on these studies, we selected the following demographic attributes for our analysis: gender; age; education level; prior work experience or education in an Information Technology (IT), cybersecurity, or privacy field; and smart home experience (length of time participants had used smart home devices).

3. Methodology

In April 2021, we conducted an online survey to understand smart home device users' perceptions and experiences with smart home device updates. Our institution's Research Protections Office approved the study.

3.1. Survey Development

The survey focused on five device categories:

- ***virtual voice assistants/smart speakers*** (e.g., Amazon Echo/Alexa, Google Home, Apple HomePod)
- ***smart thermostats*** (e.g., Nest, Ecobee)
- ***smart security devices*** (e.g., security cameras, video doorbells, door locks, garage door openers)
- ***smart sensors*** (e.g., smoke and leak detectors)
- ***smart lighting*** (e.g., light bulbs, lighting systems)

As a shorthand, we refer to these categories as voice assistants, thermostats, security, sensors, and lighting.

We selected these categories because they are among the most popular in U.S. households [28] [41] and represent varying levels of sophistication. Based on prior research [44] [51] [52], we also predicted these categories would elicit a range of security and privacy concerns. For example, users may be less concerned about security and privacy of smart light bulbs as compared to devices with audio and video components (e.g., voice assistants, security cameras). Entertainment devices (e.g., smart televisions), although popular in the U.S., were not included. Since most modern televisions now have smart functionality, purchase of these may not represent a deliberate choice to have a smart home device.

Our research questions, informed by prior work, initially guided the development of the survey instrument. To ensure survey content and construct validity, we performed three rounds of reviews. An IoT security expert with prior experience in researching user software update behaviors provided feedback on technical content, alignment of survey questions to research questions, and possible missing items (questions and response options). A survey expert then reviewed the instrument with a focus on clarity, language appropriateness for the target survey population, format, and alignment of response options to questions. As a pilot to ascertain if questions were being interpreted correctly, we conducted two cognitive walk-throughs with individuals representative of our target survey population. After each review phase, we refined the survey instrument based on collected feedback.

The final survey[1] included select-all-that-apply, select one answer, Likert scales, and open-ended questions. For some questions, to explore differences between device categories, participants answered the same question for all device categories they owned. Survey topics included:

- Categories and number of smart home devices owned
- Reasons to update
- Importance and urgency of updates
- Update issues/problems
- Current and preferred update modes and notifications
- Concerns about the loss of manufacturer support (not included in this paper)
- Smart home security and privacy concerns/perceptions
- Participant demographic questions

3.2. Sample Size and Participant Recruitment

To determine an appropriate sample size, we conducted a power analysis. In 2020, about 37% [40] of the approximately 128.45 million U.S. households [46] had smart home devices (47.52 million households). Using the Qualtrics sample size calculator [35], we determined we needed a sample size of at least 385 for a 95% confidence level.

We hired an independent research company to recruit survey participants using the Prodege non-probability, online opt-in sample panel provider [33]. Prodege maintains a panel of individuals agreeing to be contacted for research opportunities. With millions of panelists and thousands of demographic and behavioral attributes, Prodege fit our sampling needs better than other commonly-used research recruitment pools (e.g., Amazon Mechanical Turk, Prolific) since it allowed for granular demographic targeting and recruitment that could be adjusted on a daily basis to fill gaps in desired demographics as the survey timeframe progressed. Prodege also had a smart home ownership attribute that facilitated efficient sample targeting. To be eligible for the survey, prospective participants had to meet the following criteria:

- Adults (18+ years old) living in the U.S.
- Active users of smart home devices in at least two of the five device categories of interest
- Administrators of their smart home devices, i.e., those responsible for device setup and maintenance

To recruit a demographically diverse sample from across the U.S., the research company developed soft quotas (optional targets) to guide recruitment for U.S. region, income, level of education, race/ethnicity, and urbanicity. Quotas were largely based on data published by the U.S. Census Bureau's Current Population Survey Basic Monthly October 2020 survey [47] and the Pew method for using the 2018 American Community Survey to categorize urbanicity [31].

3.3. Data Collection

The survey was fielded for two weeks, with survey invitations sent out incrementally. Panel members received notification of the survey opportunity, and, if interested, completed a short screening questionnaire to determine eligibility. Once deemed eligible, panelists were provided with the survey link. Given the anonymous nature of the survey, in lieu of informed consent, survey participants were provided a study information sheet on the first screen of the survey. The information sheet described the study purpose, the survey procedure, and how confidentiality and data would be protected. Survey responses were collected without personal or machine identifiers. A total of 412 participants completed the survey with an average completion time of just under 17 minutes. After finishing the survey, participants received a $12.50 (USD) gift card.

1. Survey available at: https://cms.csrc.nist.gov/csrc/media/Projects/usable-cybersecurity/documents/Update_survey_questions.pdf

3.4. Data Analysis

To analyze data, we calculated descriptive statistics to report frequencies of survey question responses and inferential statistics to explore relationships and influencing factors.

3.4.1. Device category and demographic influences. We looked for potential differences in responses based on device category and influences of demographic attributes of interest (see 2.3) for questions about update importance, update urgency, and security and privacy perceptions. To do so, we utilized Cumulative Link Mixed Models (CLMM) with a logit link function to analyze our repeated measures data, which were unbalanced since participants may have answered questions for anywhere between two and five device categories [16] [27]. This model enabled us to analyze ordinal and categorical data while allowing for the use of random effects. The device categories and five demographic factors were entered as fixed factors and individual participants were treated as random factors. For statistically significant models (α = 0.05), we performed post-hoc pairwise comparisons for the device categories, adjusting for multiple comparisons by using the Bonferroni correction (α = 0.01).

3.4.2. Relationships between question responses. Lastly, we used the non-parametric Kendall rank correlations to determine whether responses of certain questions may be related to responses of other questions. Specifically, we wished to know if participants' security/privacy perceptions for each device category were related to how they ranked update importance and urgency. We also examined if security and privacy perceptions were associated with whether participants viewed improving security/privacy as a top reason to update smart home devices. Reported correlations are significant at α = 0.05.

4. Participants and Devices

4.1. Participant Demographics

Participants completed a series of demographic questions at the end of the survey. For each demographic attribute, we report the counts of participants choosing a

response (n) and the rounded percentage out of the total number of participants (N = 412). Demographic responses are summarized in Table 2. As a comparison point, when available, we also include the estimated percentage of adults in the U.S. with each demographic attribute (Pop %).

Compared to the national population, our sample had a greater representation of those in the 35-44 age group, a larger percentage of females, and more racial and ethnic diversity. Our participants were also more highly educated (51% having a bachelor's or graduate degree compared to 34% nationally) and skewed to households with incomes in the $50,000-$99,999 range. Differences between our sample and the U.S. population are in line with prior reporting of consumers most likely to own smart home technologies: those in the 30-40 age group [39]. However, our slightly female-heavy sample differs in that men are typically more likely to adopt smart home devices [39].

Participants lived in 47 U.S. states (all but Alaska, Hawaii, and Vermont) and one U.S. territory (Puerto Rico). We grouped states into regions, finding that our sample had more participants from the Northeast and South but less from the Midwest and West as compared to national numbers. Over half lived in a suburban area, and 80% owned their homes.

To make a partial determination of participants' technology experience, we asked if they currently or previously had worked professionally or were educated in a field related to IT, cybersecurity, or privacy. Just 16% of survey respondents indicated that they had. We also asked how long they had been using smart home devices, with 66% having used the devices for three or more years.

TABLE 2. PARTICIPANT DEMOGRAPHICS (N = 412)

Demographic	Sub-category	n	%	Pop %*
Age Range (years)	18 - 24	35	9%	10%
	25 - 34	55	13%	16%
	35 - 44	107	26%	16%
	45 - 54	37	9%	15%
	55 - 64	71	17%	18%
	65+	107	26%	25%
Gender	Male	169	41%	48%
	Female	241	58%	52%
	Prefer to self-describe	2	<1%	-
Race	White	289	70%	81%
	Black	73	18%	10%
	Asian	29	7%	6%
	Pacific Islander	2	<1%	<1%
	American Indian	4	1%	1%
	Multi-racial	12	3%	2%
	No answer	3	<1%	-
Ethnicity	Hispanic or Latino	71	17%	13%
	Not Hispanic or Latino	335	81%	87%
	No answer	6	<2%	-
Education Level	Less than high school	11	3%	9%
	High school degree	62	15%	30%
	Some college	83	20%	17%
	Associate's degree	47	11%	10%
	Bachelor's degree	148	36%	21%
	Graduate degree	60	15%	13%
Household Income	Less than $50,000	145	35%	37%
	$50,000 - $99,999	161	39%	33%
	$100,000+	102	25%	30%
	No answer	4	1%	-
U.S. Region	Northeast	86	21%	16%
	Midwest	71	17%	20%
	South	167	41%	37%
	West	84	20%	27%
	U.S. Territory	1	<1%	-
	No answer	3	<1%	-
Urbanicity	Rural	68	17%	14%
	Suburban	213	52%	55%
	Urban	131	32%	31%
Home Ownership	Own	330	80%	-
	Rent	78	19%	-
	Other	2	<1%	-
	No answer	2	<1%	-
IT, Security, Privacy Job Experience	Yes	65	16%	-
	No	347	84%	-
Smart Home Experience	Less than 1 year	15	4%	-
	1 - 2 years	122	30%	-
	3 - 5 years	198	48%	-
	6+ years	76	18%	-
	No answer	1	<1%	-

*Pop % (population %) is based on U.S. Census Bureau's CPS Basic Monthly October 2020 survey. Only demographics for adults (18+ years) are included. Items without values were not available in that data set. Urbanicity is based on Pew's method for using the 2018 American Community Survey data.

4.2. Smart Home Devices

Among the five device categories of interest, voice assistants were owned by the most survey participants (83%, n = 341). Security devices were owned by 65% (n = 268), sensors by 52% (n = 215), lighting by 50% (n = 204), and thermostats by 43% (n = 177).

We also asked what other types of devices participants owned. Smart entertainment devices were most common (71% of 412 total participants), with fewer owning smart appliances (35%), smart plugs/outlets (33%), domestic robots such as smart vacuums (30%), or smart hubs like Samsung SmartThings or Hubitat Elevation (20%). Participants specified the number of individual smart home devices they owned, averaging 9 devices, with 34% owning 2-5 devices, 31% with 6-9 devices, and 35% owning 10 or more devices.

5. Results and Discussion

In this section, we report on the results of our survey organized by research question. Results include summary statistics (rounded to the nearest whole percentage) and significant inferential statistics results. All CLMMs were statistically significant; therefore, we performed post-hoc pairwise comparisons to check for significant differences between device categories. Table 3 shows the results of these comparisons and will be referenced throughout this section. Appendix A contains detailed model results.

Our study was exploratory in that it applies an existing area of study (user perceptions, experiences, and behaviors related to *software* updates) to a new context (*smart home* updates) [42]. As such, at the end of each subsection, we situate high-level takeaways within related software update

TABLE 3. DEVICE CATEGORY PAIRWISE COMPARISONS (z-STATISTIC REPORTED)

Categories	Update Importance	Update Urgency	Security Concern	Device Security	Privacy Concern	Device Privacy
voice assistants vs. thermostats	-0.31	-1.8	**4.99***	**-5.2***	**6.87***	**-4.26***
voice assistants vs. security	**-2.8***	**-4.93***	0.55	**-2.77***	1.3	**-5.42***
voice assistants vs. sensors	-1.17	-2.44	**3.53***	**-3.94***	**7.0***	**-5.35***
voice assistants vs. lighting	**5.55***	1.72	**7.52***	**-6.18***	**8.41***	**-4.59***
thermostats vs. security	-2.02	-2.45	**-4.38***	**2.81***	**-5.71***	-0.39
thermostats vs. sensors	-0.71	-0.47	-1.61	1.38	-0.23	-0.75
thermostats vs. lighting	**4.88***	**3.01***	2.01	-0.61	1.13	0.0
sensors vs. security	-1.35	-2.06	**-2.92***	1.42	**-5.78***	0.43
sensors vs. lighting	**5.89***	**3.65***	**3.81***	-2.07	1.41	0.79
security vs. lighting	**7.36***	**5.72***	**6.7***	**-3.56***	**7.03***	0.41

* Significant results at α = 0.01 (adjusted with Bonferroni correction).

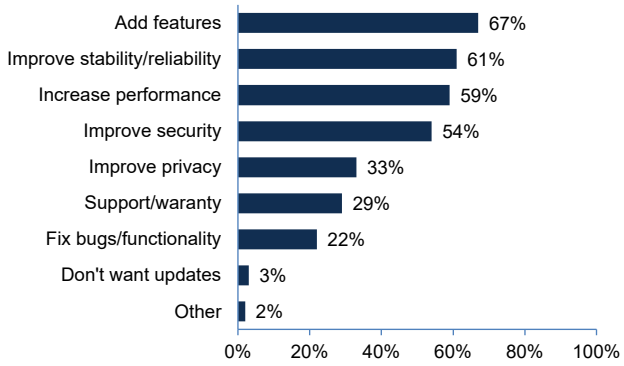

Figure 1. Reasons to update (n = 412)

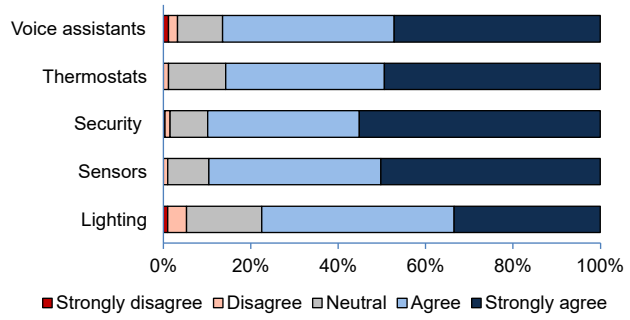

Figure 2. Agreement with statement: "It is important for smart home devices to be updated."

literature as part of an integrated discussion.

5.1. RQ1: Reasons to Update

To determine what participants thought were the biggest drivers for updating their smart home devices, participants selected their top four reasons from a list (see Fig. 1). The answer choices were informed by prior literature that identified reasons people choose to update their software [11] [25] [49] and smart home products [17].

Adding new features or removing outdated ones, providing better stability and reliability, increasing device performance, and improving security were selected by over half of participants. Improving privacy, ensuring manufacturer warranty, and the fixing of non-security bugs were chosen as a top reason by less than a third, while 3% said they did not want updates for their devices.

RQ1 Takeaways: The top three reasons to update (adding features, improving reliability, increasing performance) were focused on adding more or better capabilities, rather than fixing problems. Improving security, although not as commonly selected, was viewed as one of the top four reasons by over half of participants, echoing prior study findings of security being an important driver for software updates [25] [49]. However, our result demonstrated an awareness of the link between updates and security not previously found in IoT-specific studies [14] [17]. Furthermore, we found that participants less frequently viewed privacy improvement as a top reason. This might be because people perceive privacy features as built-in, unchanging aspects of the device.

5.2. RQ2: Update Importance and Urgency

5.2.1. Importance. We asked participants to rate their agreement that smart home device updates are important on a 5-point scale from strongly disagree to strongly agree for each of the device categories they owned (Fig. 2). Updates for security devices were rated as most important (strongly agree or agree) by 90% of participants, followed closely by sensors at 89%, voice assistants at 86%, and thermostats at 85%. Lighting devices were the lowest rated, although still viewed as important by 77%. Across all responses and categories, 86% thought updates were important.

Pairwise comparisons revealed that participants were significantly less likely to agree that lighting updates were important as compared to all other categories (see "Update Importance" column in Table 3). In addition, voice assistant updates were rated significantly less important than security device updates. We also found several demographic influences. As compared to participants who were 65+ years

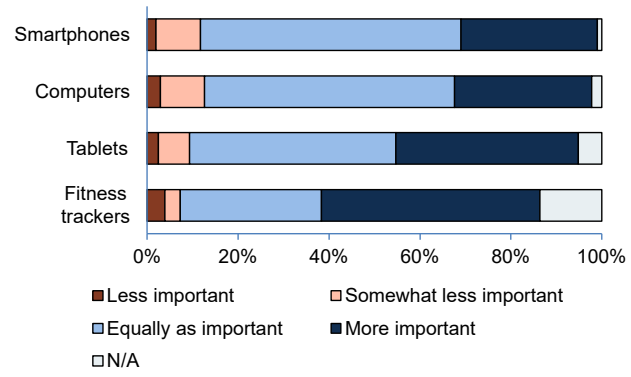

Figure 3. Smart home update importance compared to other technology updates

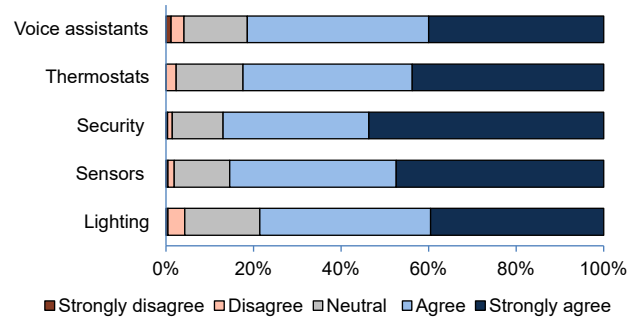

Figure 4. Agreement with statement: "It is urgent that my smart home devices be updated when updates are made available."

of age, those in the 35-44 and 55-64 groups were more likely to rate update importance higher (z = 2.47 and z = 2.64, respectively). Those with prior experience in an IT field had higher ratings as compared to those without this experience (z = 2.07). In addition, participants with less than a year of experience using smart home devices rated update importance lower as compared to participants with 6+ years of experience (z = -2.33). Table 6 in Appendix A shows the detailed results of the CLMM for update importance.

Participants also rated the importance of smart home device updates as compared to other technologies: smartphones, laptop/desktop computers, tablets, and fitness trackers. Response options were on a 4-point scale from less important to more important. If a participant did not own a specific technology, they selected "Does not apply" (N/A). Fig. 3 shows the responses. Among those who owned each type of technology (i.e., excluding N/A responses), smart home updates were overwhelmingly rated as equally or more important, ranging from 92% among owners of fitness trackers to 87% for laptop/desktop computers.

5.2.2. Urgency. Participants rated their agreement that smart home device updates are urgent (Fig. 4). Eighty-three percent of participants agreed that updates were urgent across all responses and device categories, with security devices and sensors again receiving the highest percent of agreement (87% and 85%), thermostats 83%, voice assistants 81%, and lighting the lowest (79%).

Exploring differences in categories, we found that participants were less likely to agree that lighting updates were urgent as compared to updates for thermostats, sensors, and security devices (See "Update Urgency" column in Table 3). In addition, security device updates were viewed as more urgent than voice assistant updates. There was only one demographic influence for update urgency ratings. Compared to participants 65+ years old, those in the 55-64 age group were more likely to rate update urgency higher (z = 2.56). Table 7 in Appendix A shows the detailed results of the CLMM for update urgency.

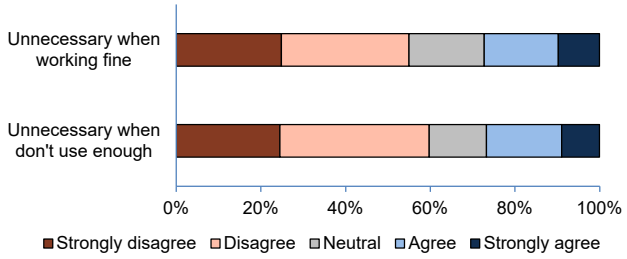

Figure 5. Agreement with statements about when updates are unnecessary

5.2.3. Necessity. Related to importance and urgency, we asked participants to rate their agreement for the following two statements: 1) "Updates are unnecessary when my smart home devices are working just fine without them" and 2) "Updates are unnecessary when I don't use my smart home devices enough." These statements were inspired by survey items in a prior study on software updates [26].

Few thought that updates were unnecessary when devices are working fine (18% agree/strongly agree) and that updates were unnecessary when the device is not used enough (17% agree/strongly agree). Fig. 5 shows the agreement ratings.

RQ2 Takeaways: An overwhelming number of study participants thought smart home updates were both important and urgent. Unlike findings in Mathur et al.'s software updates survey [26], the majority in our survey thought updates were still necessary even if devices were working fine or not often used. Most participants also believed smart home updates were no less important than updates for other types of computing devices. These findings were in contrast to Fassl et al.'s survey [14] in which smart consumer device updates, with the exception of safety-related updates for smart cars, were not generally viewed as important, especially when compared to smartphones [14]. However, divergence in the two studies may be due to the types of IoT devices surveyed in each study. While Fassl et. al. found these differences for a smart appliance and smart shoes, we were focused only on smart home devices.

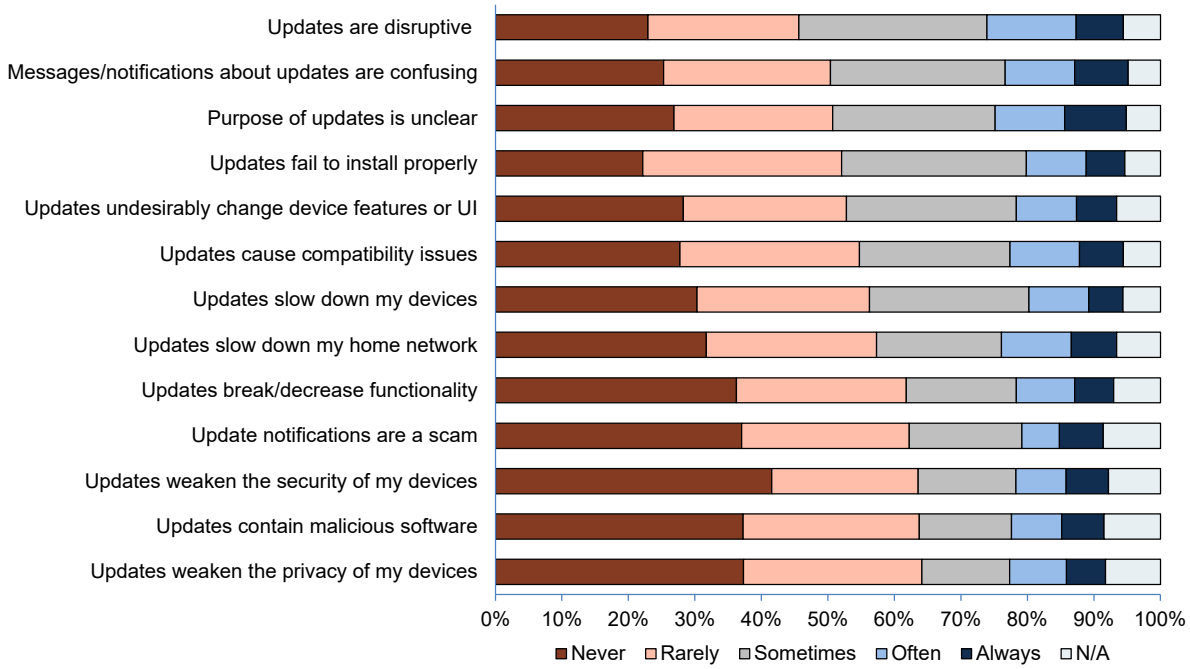

Figure 6. Frequency with which update issues are encountered

Updates for lighting devices were often rated as less important and urgent, perhaps due to lack of obvious safety consequences or perceived simplicity of functionality. Also likely attributed to perceived safety implications, there was a marked difference between voice assistants and security devices for both importance and urgency.

5.3. RQ3: Update Issues

Participants rated how often various update issues had been true for them (from never to always with an N/A option). The update issues included in our survey were informed by two prior surveys about software updates [11] [26] and an interview study identifying challenges with smart home updates [17]. Fig. 6 shows the rating frequencies, sorted in order from those issues most frequently encountered (sometimes, often, or always) to those least encountered. For all possible issues, over half of participants had experienced the issue only rarely or not at all.

RQ3 Takeaways: The top six most frequently encountered issues (at least 40% of participants) centered on impediments to device operation (disruption to current tasks, installation failure, undesirable changes, or compatibility issues) or lack of clarity (unclear update purpose and confusing notifications). These issues were often cited in qualitative studies as reasons for software update hesitancy [25] [48] [49]. Although similarly experienced by participants in quantitative inquiries about software updates [26] [11], our participants encountered these issues less frequently. For example, we found that 44% of participants experienced smart home update purposes being unclear and 40% had compatibility issues, while over 60% had these issues with software updates [26]. A possible explanation for this difference may be that software updates may require more explicit actions on the user's part, and therefore, may be more noticeable [17].

5.4. RQ4: Current and Preferred Update Installation and Notification Modes

A section of the survey was dedicated towards discovering how smart home updates are currently handled and participants' preferences. In this paper, we focus on identifying the *gaps* between current and preferred.

5.4.1. Update modes. We asked participants about the *current* update modes for each device category they owned. Possible select-one responses included: automatic, manual (users initiate update installation), both automatic and manual, or "I don't know/I'm not sure." If they had multiple device models/brands in the same category with some having automatic and some having manual updates, participants were instructed to select the "both" option. Participants also indicated their *preferred* update modes for each device category by selecting one of the following: automatic, manual, both automatic and manual, and no preference.

Notably, depending on device category, an appreciable number of participants did not know how updates are currently being handled: lighting 21%, voice assistants 15%, sensors 14%, and both thermostats and security devices at

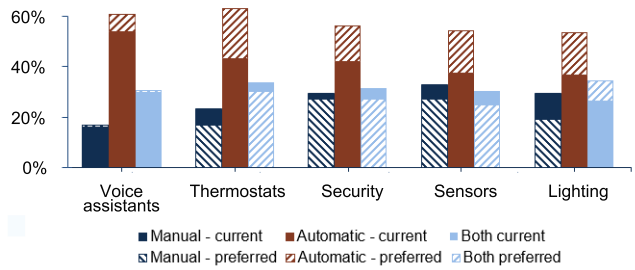

Figure 7. Current and preferred update modes. Instances in which striped bars are placed on top of solid bars indicate that more participants prefer that mode than what they currently have available.

13%. Only 1-5% had no preference regarding update mode (lowest for thermostats, highest for sensors and lighting).

To determine behaviors with manual updates, we asked a follow-up question for those who indicated that their devices in at least one category had manual updates. Of the 238 participants to which this question applied, 56% indicated that they usually install manual updates as soon as available, 38% said that they eventually install manual updates (but not right away), 5% said they rarely install manual updates, and 1% said they never install manual updates.

Fig. 7 shows the current versus preferred update modes for each device category, excluding "don't know" and "no preference" responses. Automatic updates were most commonly implemented for all categories. However, these were only preferred for voice assistants and thermostats. Manual updates were most preferred for security devices and sensors, while owners of lighting devices would most like to be able to choose between automatic and manual updates.

5.4.2. Update availability notifications. We asked participants how they *currently* find out an update is available. More than one notification method could be selected. For the current notification method, few selected "I don't know/I'm not sure": 10% for voice assistants, 8% for thermostats, 1% for security devices, none for sensors, and 1% for lighting. We also asked what notification method they would *prefer*.

Fig. 8 shows the current versus preferred update availability notification methods for each device category ("I don't know" responses excluded). Receiving a message in the device companion app was most selected for both current and preferred notifications across all device categories. Email was the second most preferred for all categories. Of particular interest, for each device category, about a quarter of participants had to seek out update information on their own via websites or other means (e.g., online forums or social media) or wait to hear from family or friends, even though they would generally prefer not to. In addition, across all categories, there were fewer participants who preferred not to be notified about available updates (5%) than those who said they are not currently notified (10%).

5.4.3. Wish list. Participants selected update-related actions they would like to be able to take from a list based on

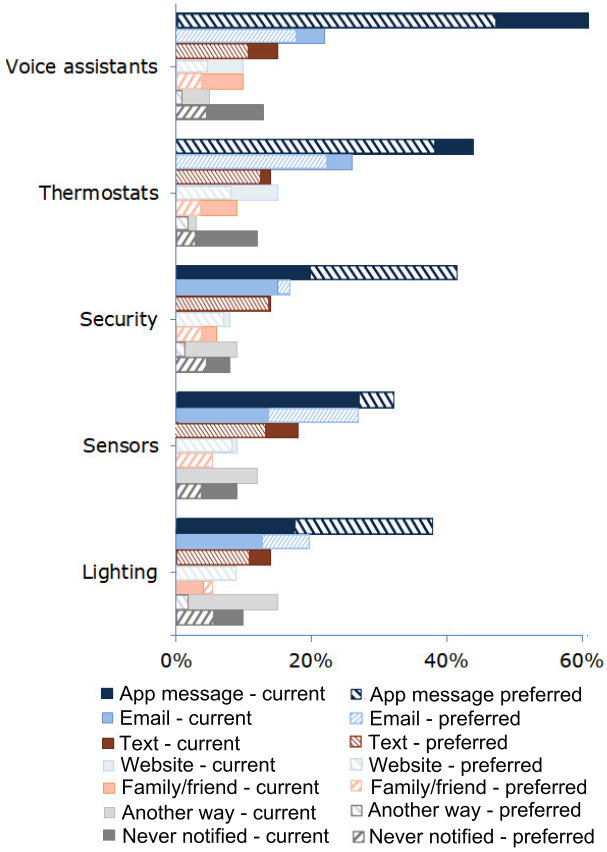

Figure 8. Current and preferred update availability notifications.

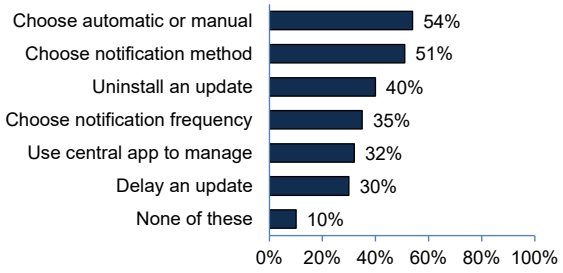

Figure 9. Update wish list (n=409)

findings and recommendations from prior update-focused papers [11] [17] [25] [49]. Fig. 9 shows the response frequencies. Over half would like to have the ability to choose between automatic and manual updates and choose how to receive update notifications. The third most selected action was being able to uninstall an update, with using an application to centrally manage updates and the ability to delay an update selected by less than a third of participants.

RQ4 Takeaways: Participants indicated that automatic updates were most common for all device categories. This

differs from real-world observations (Table 1 and [13]) in which *manual-only* updates were most common for sensors and lighting. In addition, two-thirds of our market-surveyed voice assistants, thermostats, and security devices offer users the option of turning automatic updates on or off, yet survey participants less-frequently mentioned having both options. These discrepancies may be due to memory recall issues, not knowing that they have an option to change default behaviors (which are most commonly set to automatic), or mistakenly thinking they are getting updates automatically when they are not actually receiving any updates.

We found that there were gaps between current modes and user preferences for both update modes and notifications, often dependent on the type of device. While the majority desired automatic updates for certain device categories (voice assistants and thermostats), others wanted more control via options to configure manual updates, especially for security devices, sensors and lighting. This mixed preference was also found in other studies on both software [49] and IoT updates [14]. Additionally, as also found or recommended in prior work, an appreciable number of participants wanted more control over several other aspects of updates, including notification method and frequency [11] [25] and update rollback [21] [25] [13]. A more in-depth discussion on increasing user agency via the customization of update preferences is included in section 6.

5.5. RQ5: Security and Privacy Perceptions

We asked participants about their perceptions of the security of their smart home devices and the privacy of the data collected by the devices. In addition to looking for differences between responses for each device category and demographics influences, we also examined potential correlations between these perceptions and perceptions of update importance and urgency for each category.

5.5.1. Security Concern. Participants rated their level of security concern on a 5-point scale from "not at all concerned" to "extremely concerned." Security devices had the highest level of concern, with 43% of participants moderately or extremely concerned, followed by voice assistants (38%), sensors (35%), and thermostats (33%). Participants were least concerned about lighting (28%). Figure 10 shows the security concern ratings.

We found participants had significantly lower security concern levels for lighting as compared to voice assistants, sensors, and security devices (see "Security Concern" column in Table 3. Both voice assistants and security devices had higher levels of security concern than thermostats and sensors. Considering demographic influences, as compared to participants who were 65+ years of age, those in the 18-24 and 35-44 groups were more likely to have a higher level of security concern (z = 2.23 and z = 2.71, respectively). Participants with a Bachelor's degree had lower levels of security concern as compared to those with a graduate degree (z = -2.42). Table 8 in Appendix A shows the detailed results of the CLMM for security concern.

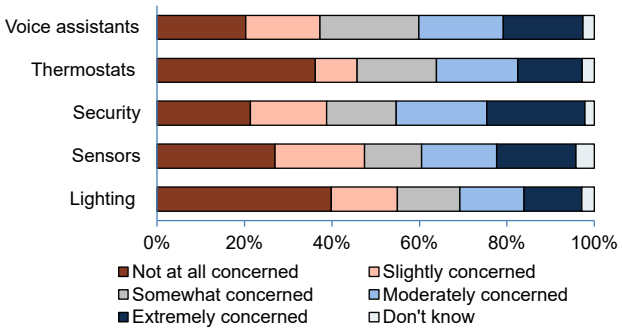

Figure 10. Level of security concern with smart home devices

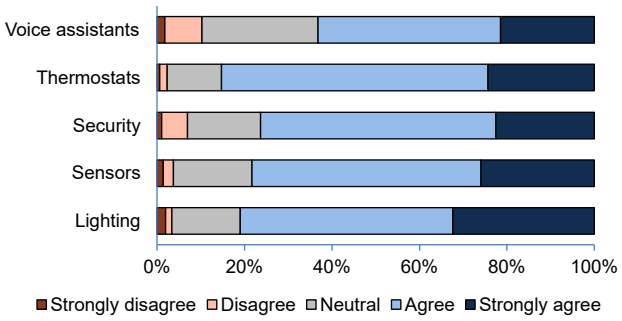

Figure 11. Agreement with the statement: "I think that most smart home devices in this category are secure."

Significant, though weak, correlations were found for the lighting device category between security concern and update importance (τ = 0.1908) and update urgency (τ = 0.2003). In other words, as the level of security concern for lighting increases, the ratings of importance and urgency for lighting updates also increase. Higher levels of security concern were also associated with participants having chosen "Improve security of the device" as a top reason to update (see section 5.1) only for voice assistants (τ = 0.1664).

5.5.2. Device security. We then asked participants to rate their agreement on whether devices in each category are secure (Fig. 11). The majority agreed or strongly agreed that their devices were secure: 85% for thermostats, 81% for lighting, 78% for sensors, 76% for security devices, and 63% for voice assistants. Across all categories, 75% thought their smart home devices were secure.

Voice assistants were perceived as significantly less secure than all other device categories (see "Device Security" column in Table 3). Additionally, security devices were rated as significantly less secure than both thermostats and lighting. Considering demographic influences, participants in the 35-44 age group were more likely to rate their devices as being secure as compared to those in the 65+ age group (z = 2.24). Additionally, participants who had used smart home

TABLE 4. DEVICE SECURITY AGREEMENT CORRELATIONS ($p < 0.05$)

Category	Update Importance (τ)	Update Urgency (τ)
Voice assistants	0.3176	0.3229
Thermostats	0.3938	0.3776
Security devices	0.1863	0.2211
Sensors	0.1622	0.2372
Lighting	0.2161	0.2839

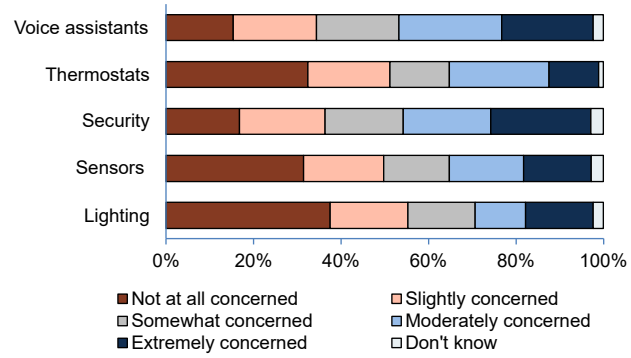

Figure 12. Level of privacy concern for smart home devices

devices for less than a year were less likely to think their devices were secure as compared to those with 6+ years of experience (z = -3.34). Table 9 in Appendix A shows the detailed results of the CLMM for device security.

There were significant, but weak, positive correlations for all device categories between security agreement and update importance and urgency ratings, with the strongest correlations for voice assistants and thermostats (Table 4). There were no significant correlations between level of agreement and choosing "Improve security of the devices" as a top reason to update.

5.5.3. Privacy concern. Level of privacy concern was, overall, higher than security concern, with 44% moderately/extremely concerned about voice assistants, 43% for security devices, 34% for thermostats, and 32% for sensors. Lighting devices again had the lowest rankings of concern at 27%. See Fig. 12.

Participants had significantly higher levels of privacy concern for both voice assistants and security devices as compared to thermostats, sensors, and lighting (see "Privacy Concern" column in Table 3). For demographics, participants in the 18-24, 25-34, 35-44, and 55-64 age groups had lower levels of privacy concern as compared to those in the 65+ age group (z = 2.67, z = 2.33, z = 3.32, z = 2.43, respectively). In addition, participants with some college education had lower levels of privacy concern as compared to those with graduate degrees (z = -1.99). Table 10 in Appendix A shows the detailed results of the CLMM for privacy concern.

Similar to security concern, there were significant, but weak correlations, for the lighting category between privacy

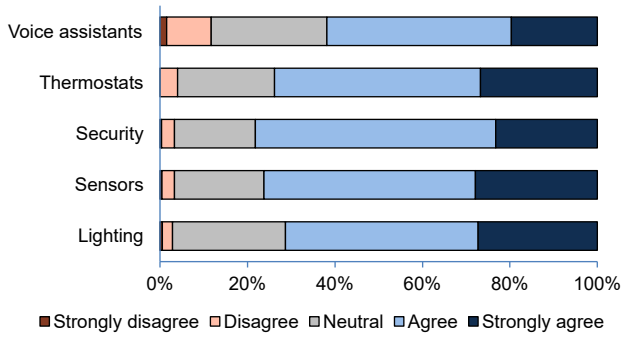

Figure 13. Agreement with the statement: "I think most smart home devices in this category protect my privacy."

concern and update importance (τ = 0.19484) and update urgency (τ = 0.2551). In other words, as the level of privacy concern for lighting increases, the ratings for importance and urgency of lighting device updates also increase. Higher levels of privacy concern were weakly correlated with having chosen "Improve privacy of the devices" as a top reason to update (section 5.1) for four device categories: thermostats (τ = 0.1552), security (τ = 0.1191), sensors (τ = 0.1669), and lighting (τ = 0.1368).

5.5.4. Devices protect privacy. For each device category, we asked participants to rate their agreement that the devices protect their privacy. Across all device categories, 71% of participants agreed or strongly agreed that devices protect their privacy. However, these percentages were lower overall as compared to security perceptions: 78% for security devices, 76% for sensors, 74% for thermostats, 68% for lighting, and 62% for voice assistants. Fig. 13 shows the distribution of responses.

We found that voice assistants were perceived to be significantly less privacy-protecting than devices in all other categories (see "Device Privacy" column in Table 3). With respect to demographic influences, participants in the 25-34 and 35-44 age groups were more likely to agree their devices were private as compared to those in the 65+ age group (z = 2.18, z = 3.06, respectively). In addition, participants with a high school education level rated their devices as more privacy-protecting as compared to those with graduate degrees (z = 2.01). Finally, participants who had less than one year or 1-2 years of experience using smart home devices rated their devices as less privacy-protecting as compared to those with 6+ years of experience (z = -3.1, z = -2.64, respectively). Table 11 in Appendix A shows the detailed results of the CLMM for device privacy.

Similar to the corresponding security question, significant, although weak, correlations were found for all device categories between privacy agreement and perceptions of update importance and urgency, with the strongest correlations for voice assistants and thermostats (see Table 5). There were no significant correlations between agreement and choosing "Improve privacy of the devices" as a top

TABLE 5. DEVICE PRIVACY AGREEMENT CORRELATIONS ($p < 0.05$)

Category	Update Importance (τ)	Update Urgency (τ)
Voice assistants	0.3235	0.327
Thermostats	0.3563	0.3086
Security devices	0.2091	0.2136
Sensors	0.2646	0.3019
Lighting	0.2641	0.2994

reason to update.

RQ5 Takeaways: Overall, we found few relationships between participants' perceptions of smart home security and privacy and their corresponding opinions about update importance and urgency. Security and privacy concerns were only related to update importance and urgency for the lighting category. However, perceptions of update importance and urgency were positively correlated with participants' views that their devices were secure and privacy-protecting. This was surprising since we would expect that updates would have been viewed as important and urgent in order to rectify security and privacy shortcomings in the devices. This unexpected observation might be because participants think updates are important and urgent mostly for non-security or non-privacy motivations, as demonstrated by the top three responses for reasons to update (features, stability, performance) reported in section 5.1.

Since smart home security and privacy perceptions were included in our study for the purpose of determining relationships to update perceptions, we offer only brief thoughts on the results of the individual security and privacy survey items. Overall, we observed a high sense of confidence in the security and privacy of smart home devices (as also found in [18]) and low levels of security and privacy concern. While security and privacy concerns are often cited by smart home *non-adopters* as reasons not to buy these devices [34], our participants were smart home *adopters* whose concern levels were obviously not high enough to prevent them from owning these devices. Additionally, consumers are typically not well-versed in security or privacy implications and may view device ownership as a trade-off in which the benefits are greater than any potential risks [44] [51]. This trade-off may be especially pronounced for voice assistants and security devices, which we found to elicit more security and privacy concern, likely due to their always-listening/watching nature and perceived mysteriousness of their data usage and privacy policies [43].

6. Implications

Exploratory research is meant to "produce new ideas and hypotheses" but not to come to concrete conclusions [42]. As such, for our exploratory study, we do not make definitive recommendations. Rather, based on our results, we offer suggestions for practical ways in which users' update experiences and awareness might be improved while acknowledging areas that could benefit from further investigation.

6.1. Facilitating Understanding and Awareness of Updates

A substantial number of participants were unsure about update purpose, messages, and how updates were being handled on their devices. To alleviate this confusion, manufacturers could provide users with more informative and easy-to-find information on updates, for example within the device companion apps or via product labels [7]. As also recommended by other standards and government organizations [6] [9] [12] [15], manufacturers could be more transparent about their update model so that users know how they can gain awareness of update availability and installation, what actions they should take to install updates, and the availability (if any) of update configuration and notification options. Since we found that over half of participants viewed security fixes as a top reason to update their devices, providing security-related information in update notifications (e.g., that the update provides a security improvement or information about the severity and consequences of the security vulnerability/threat) may be valuable in encouraging users to quickly apply the updates.

Our study results may also reflect gaps in users' understanding and have implications for where manufacturers and third parties might need to focus consumer education efforts. As discussed in section 5, we observed differences among device categories that suggest users may place higher value on some device types depending on functionality and *perceived* security/privacy exposure, thus potentially being less likely to apply timely updates to those devices. This could possibly be because the data collected by devices in these categories are viewed as having lower value [44] or the devices have limited capabilities. In addition, these devices lack audio or video components, which are often viewed with more concern [51].

Therefore, there may be a need for increased consumer education about the importance of updates in mitigating security and privacy risks for *all* smart home devices, regardless of type. Awareness efforts could also be targeted at demographic groups that have less understanding of update importance and associated security/privacy implications, such as older, less-educated, less-experienced, and non-IT expert consumers, as identified in our results.

6.2. Enabling User Agency

Beyond increasing transparency and awareness, since our participants had differing update preferences, we also explore potential benefits of allowing users the ability to customize and control their update experience.

6.2.1. Allowing for Customization. To support the range of preferences expressed by our participants, manufacturers could provide configurable options, for example, allowing choice between automatic and manual updates or permitting users to set the delivery method and frequency of notifications. These suggestions are in line with prior research suggesting that an increase in update control may positively

impact consumers' intent to purchase an IoT product [7]. Increased user agency may also mitigate frustrations with update disruption in that users could potentially postpone installations to a more convenient time or uninstall updates that cause functionality or compatibility issues [25].

As evidenced by our participants, consumers may own and manage many smart home devices. A centralized app or hub enabling update coordination (as also recommended in [17] and [25]) could alleviate user burden by consolidating update notifications and allowing for quick review and customization of update settings. However, while device management is often centralized for products from the same manufacturer (e.g., Apple HomeKit and Google Nest Home), support for diverse devices would require a new update standard to allow device-app communication. Future research would also be needed to design a usable interface.

6.2.2. Debating Automatic vs. Manual Updates. As illustrated by our market analysis and participant responses, some devices allow users to choose the update mode while others are constrained to either manual or automatic updates only. Forcing automatic updates is a common approach to reduce user burden while ensuring devices remain secure. This viewpoint was shared by researchers who recommended a reduction in user involvement, with devices always updating automatically [23] and update notifications avoided [14].

However, one-size-fits-all solutions may not be appropriate. While automatic updates may be beneficial in some cases, there has been debate on whether users should be deprived of choice. Over half our participants explicitly said they would like to be able to choose between automatic and manual updates (section 5.4.3). Several researchers suggested that offloading updates entirely to the system, while being advantageous for some users, may be detrimental for others and actually result in poorer security outcomes [50] or increased discomfort due to a perceived loss of agency [14] [25]. As suggested in Wash et al.'s study on automatic software updates [50], a lack of user involvement and awareness of updates may result in the development of inaccurate update mental models. These gaps in understanding may, in turn, lead to an inability of users to act in situations that require manual updates, for example, when using devices that do not offer automatic updates or when the automatic update process fails.

Allowing options for users who want more control is also supported by several IoT security standards groups. While baseline standards often call for devices to implement automatic updates by default, several go beyond that, recommending that users have the option of automatic or manual updates depending on the context [10] [12], the ability to "approve, authorise, or reject updates" [10], and notification that an update is required [9]. Update notifications may especially be important for automatic updates in order to encourage more accurate update mental models and ensure consumers do not mistakenly believe that updates are being automatically applied when they are indeed not being applied at all.

In light of this debate, we believe more research is warranted to investigate how to design smart home update mechanisms to best balance a range of user preferences while ensuring security, functionality, and reliability are maintained.

6.3. Addressing Study Limitations

Our study has several limitations. First, we acknowledge the potential of participant reporting of current update and notification modes not always reflecting reality. This may especially be the case given the observed differences between participant responses about current update modes, prior NIST research [13], and our market analysis. In addition, prior research findings indicate that users may mistakenly believe that automatic updates are available when they are not [50]. With our current data set, we do not know whether responses might have been impacted by memory recall issues or simply by a lack of awareness. These unknowns could be addressed with future research involving direct observations of update mode and notification settings (e.g., as done in a study on smartphone update behaviors [14]).

We also recognize that the reported intentions to update implied by perceptions of update importance and urgency do not necessarily mean that users actually install updates in a timely fashion [50]. However, prior research has shown that perceptions do influence behaviors [32], including within the security context (e.g., [4] [19]). Moreover, the goals of our exploratory survey, in part, were to identify perceptions (not accuracy), which may reveal areas of misunderstanding or areas of particular importance for participants. A field study that directly monitors user update behaviors (e.g., via update logs as done in [50]) could address this limitation.

Significant correlations identified in our study showed only weak associations. Therefore, further investigation would be valuable. Finally, the experiences and perceptions of smart home users in the U.S. may differ from those in other countries, which could be addressed by a replication study in other regions.

7. Conclusion

As smart home devices become pervasive in households and security and privacy threats evolve, the timely installation of updates is becoming increasingly important. Towards facilitating the installation of these updates, we conducted a survey of 412 U.S. smart home owners to better understand their smart home update experiences and challenges. Based on our results, we offer suggestions for increasing consumer understanding and awareness of updates and implications for customizing the update experience with a goal of empowering consumers to do their part in protecting the security and privacy of their smart home devices.

Disclaimer

Certain commercial companies or products are identified in this paper to foster understanding. Such identification

does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the companies or products identified are necessarily the best available for the purpose.

Acknowledgements

We would like to thank the anonymous reviewers and our colleagues Gregory Haber, Yee-Yin Choong, and Michael Fagan for their valuable input that helped improve the paper. This research was internally funded and did not receive any specific grant from other funding agencies.

References

[1] Mohd Anwar, Wu He, Ivan Ash, Xiaohong Yuan, Ling Li, and Li Xu. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69:437–443, 2017.

[2] Bitdefender. The IoT threat landscape and top smart home vulnerabilities in 2018. https://www.bitdefender.com/files/News/CaseStudies/study/229/Bitdefender-Whitepaper-The-IoT-Threat-Landscape-and-Top-Smart-Home-Vulnerabilities-in-2018.pdf, 2019.

[3] Sara Cannizzaro, Rob Procter, Sinong Ma, and Carsten Maple. Trust in the smart home: Findings from a nationally representative survey in the UK. *PLOS ONE*, 15(5):e0231615, 2020.

[4] Yan Chen and Fatemeh Mariam Zahedi. Individuals' internet security perceptions and behaviors. *MIS Quarterly*, 40(1):205–222, 2016.

[5] Consumer Product Safety Commission. Status report on the Internet of Things (IoT) and consumer product safety. https://www.cpsc.gov/s3fs-public/Status-Report-to-the-Commission-on-the-Internet-of-Things-and-Consumer-Product-Safety.pdf, 2019.

[6] Department for Digital, Culture, Media and Sport. Code of practice for consumer IoT security. https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security, 2018.

[7] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. 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)*, pages 1937–1954, 2021.

[8] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into IoT device purchase behavior. In *CHI Conference on Human Factors in Computing Systems*. ACM, 2019.

[9] European Telecommunications Standards Institute (ETSI). Cyber security for consumer internet of things - ETSI technical specification 103 645 v1.1.1. 2. https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf, 2019.

[10] European Union Agency for Network and Information Security (ENISA). Baseline security recommendations for IoT in the context of critical information infrastructures. https://www.enisa.europa.eu/publications/baseline-securityrecommendations-for-iot, 2107.

[11] Michael Fagan, Mohammad Maifi Hasan Khan, and Ross Buck. A study of users' experiences and beliefs about software update messages. *Computers in Human Behavior*, 51:504–519, 2015.

[12] Michael Fagan, Katerina N. Megas, Karen Scarfone, and Matthew Smith. NISTIR 8259 Foundational cybersecurity activities for IoT device manufacturers. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf, 2020. National Institute of Standards and Technology.

[13] Michael Fagan, Mary Yang, Allen Tan, Lora Randolph, and Karen Scarfone. Draft NISTIR 8267 Security review of consumer home Internet of Things (IoT) products. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8267-draft.pdf, 2019. National Institute of Standards and Technology.

[14] Matthias Fassl, Michaela Neumayr, Oliver Schedler, and Katharina Krombholz. Transferring update behavior from smartphones to smart consumer devices. In *27th European Symposium on Research in Computer Security (ESORICS)*, 2021.

[15] Federal Trade Commission. Internet of things privacy and security in a connected world. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf, 2015.

[16] Ralitza Gueorguieva and John H. Krystal. Move over ANOVA: progress in analyzing repeated-measures data and its reflection in papers published in the archives of general psychiatry. *Archives of General Psychiatry*, 61(3):310–317, 2004.

[17] Julie M. Haney and Susanne M. Furman. Work in progress: Towards usable updates for smart home devices. In *10th International Workshop on Socio-Technical Aspects in Security*, pages 107–117, 2020.

[18] Harris Interactive. Consumer internet of things security labelling survey research findings. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798543/Harris_Interactive_Consumer_IoT_Security_-Labelling_Survey_Report.pdf, 2019.

[19] Tejaswini Herath and H. Raghav Rao. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2):154–165.

[20] Iulia Ion, Rob Reeder, and Sunny Consolvo. "...no one can hack my mind": Comparing expert and non-expert security practices. In *11th Symposium on Usable Privacy and Security*, pages 327–346, 2015.

[21] IoT Security Foundation. Secure design best practice guides. https://www.iotsecurityfoundation.org/wp-content/uploads/2019/11/Best-Practice-Guides-Release-2.pdf, 2019.

[22] Ari Lazurus. Update your software now. https://www.consumer.ftc.gov/blog/2019/06/update-your-software-now, 2019. Federal Trade Commission.

[23] Huichen Lin and Neil Bergmann. IoT privacy and security challenges for smart home environments. *Information*, 7(3):44, 2016.

[24] Arunesh Mathur and Marshini Chetty. Impact of user characteristics on attitudes towards automatic mobile application updates. In *13th Symposium on Usable Privacy and Security*, pages 175–193, 2017.

[25] Arunesh Mathur, Josefine Engel, Sonam Sobti, Victoria Chang, and Marshini Chetty. "They Keep Coming Back Like Zombies": Improving software updating interfaces. In *12th Symposium on Usable Privacy and Security*, pages 43–58, 2016.

[26] Arunesh Mathur, Nathan Malkin, Marian Harbach, Eyal Peer, and Serge Egelman. Quantifying users' beliefs about software updates. In *Workshop on Usable Security (USEC)*, 2018.

[27] Vilmos F. Misangyi, Jeffery A. LePine, James Algina, and Francis Goeddeke. The adequacy of repeated-measures regression for multilevel research: comparisons with repeated-measures ANOVA, multivariate repeated-measures ANOVA, and multilevel modeling across various multilevel research designs. *Organizational Research Methods*, 9(1):5–28, 2006.

[28] NPD Group. Half of U.S. consumers own at least one smart home device. https://www.npd.com/news/press-releases/2021/half-of-u-s-consumers-own-at-least-one-smart-home-device-reports-npd/, 2021.

[29] Katherine E. Olson, Marita A. O'Brien, Wendy A. Rogers, and Neil Charness. Diffusion of technology: frequency of use for younger and older adults. *Ageing International*, 36(1):123–145, 2011.

[30] Yong Jin Park. Do men and women differ in privacy? Gendered privacy and (in) equality in the internet. *Computers in Human Behavior*, 50:252–258, 2015.

[31] Pew Research Center. Prior to COVID-19, urban core counties in the U.S. were gaining vitality on key measures. https://www.pewsocialtrends.org/2020/07/29/prior-to-covid-19-urban-core-counties-in-the-u-s-were-gaining-vitality-on-key-measures/, 2020.

[32] William T. Powers. *Behavior: The control of perception*. Aldine, 1973.

[33] Prodege. Prodege: world class marketing and consumer insights. https://www.prodege.com/, 2022.

[34] PwC. Smart home, seamless life. https://www.pwc.fr/fr/assets/files/pdf/2017/01/pwc-consumer-intelligence-series-iot-connected-home.pdf, January 2017.

[35] Qualtrics. Sample size calculator. https://www.qualtrics.com/blog/calculating-sample-size/, 2022.

[36] Anabel Quan-Haase and Isioma Elueze. Revisiting the privacy paradox: concerns and protection strategies in the social media experiences of older adults. In *9th International Conference on Social Media and Society*, pages 150–159, 2018.

[37] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. "Woe is me": examining older adults' perceptions of privacy. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–6, 2019.

[38] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. Why older adults (don't) use password managers. In *30th USENIX Security Symposium*, 2021.

[39] Smiljanic Stasha. An in-depth view into smart home statistics. https://policyadvice.net/insurance/insights/smart-home-statistics/, 2021.

[40] Statista. Smart home penetration rate forecast for selected countries 2020. https://www.statista.com/forecasts/483757/penetration-rate-of-smart-homes-for-selected-countries, 2020.

[41] Statista. Smart home device household penetration in the United States in 2019 and 2021. https://www.statista.com/statistics/1247351/smart-home-device-us-household-penetration/, 2021.

[42] Richard Swedberg. Exploratory research. In Colin Elman, John Gerring, and James Mahoney, editors, *The production of knowledge: Enhancing progress in social science*, pages 17–41. Cambridge University Press, 2020.

[43] Madiha Tabassum, Tomasz Kosiński, Alisa Frik, Nathan Malkin, Primal Wijesekera, Serge Egelman, and Heather Richter Lipford. Investigating users' preferences and expectations for always-listening voice assistants. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(4):1–23, 2019.

[44] Madiha Tabassum, Tomasz Kosiński, and Heather Richter Lipford. "I don't own the data": end user perceptions of smart home device data practices and risks. In *15th Symposium on Usable Privacy and Security*, 2019.

[45] Mary Theofanos, Brian Stanton, Susanne Furman, Sandra Spickard Prettyman, and Simson Garfinkel. Be prepared: how US Government experts think about cybersecurity. In *Workshop on Usable Security (USEC)*, 2017.

[46] United States Census Bureau. Historical household tables. https://www.census.gov/data/tables/time-series/demo/families/households.html, 2022.

[47] U.S. Census Bureau. Current population survey basic monthly October 2020. https://www.census.gov/data/datasets/time-series/demo/cps/cps-basic.html, 2020.

[48] Kami Vaniea, Emilee Rader, and Rick Wash. Betrayed by updates: How negative experiences affect future security. In *2014 SIGCHI Conference on Human Factors in Computing Systems (CHI 14)*, pages 2671–2674, Toronto, Canada, April 2014. ACM.

[49] Kami Vaniea and Yasmeen Rashidi. Tales of software updates: the process of updating software. In *2016 SIGCHI Conference on Human Factors in Computing Systems (CHI 16)*, pages 3215–3226, San Jose, CA, USA, May 2016. ACM.

[50] Rick Wash, Emilee Rader, Kami Vaniea, and Michelle Rizor. Out of the loop: how automated software updates cause unintended security consequences. In *10th Symposium On Usable Privacy and Security*, pages 89–104, 2014.

[51] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *13th Symposium on Usable Privacy and Security*, 2017.

[52] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home IoT privacy. *ACM on Human-Computer Interaction*, 2(CSCW), 2018.

Appendix A: Regression Tables for Cumulative Link Mixed Models

Statistically significant p-values < 0.05 are bolded.

TABLE 6. REGRESSION RESULTS OF CLMM FOR UPDATE IMPORTANCE.

Independent Variable	Coefficient	Odds Ratio	Std Error	z	p
Gender (baseline = Female)					
Male	-0.081	0.922	0.28	-0.29	0.773
Age (baseline = 65+)					
18 - 24	0.203	1.226	0.538	0.38	0.705
25 - 34	0.529	1.697	0.463	1.14	0.253
35 - 44	0.967	2.631	0.391	2.47	**0.013**
45 - 54	0.14	1.15	0.525	0.27	0.79
55 - 64	1.113	3.104	0.429	2.64	**0.008**
Education Level (baseline = Graduate degree)					
Less than high school	1.06	2.886	0.9	1.18	0.237
High school degree	-0.117	0.889	0.522	-0.22	0.822
Some college	0.56	1.75	0.5	1.12	0.262
Associate's degree	0.632	1.881	0.549	1.15	0.25
Bachelor's degree	0.318	1.375	0.426	0.75	0.455
IT Experience (baseline = No)					
Yes	0.791	2.206	0.383	2.07	**0.039**
Smart Home Experience (baseline = 6+ years)					
Less than 1 year	-1.79	0.167	0.769	-2.33	**0.02**
1 - 2 years	-0.685	0.504	0.406	-1.69	0.092
3 – 5 years	0.248	1.281	0.37	0.67	0.502
Device Category (baseline = voice assistants)					
Lighting	-1.19	0.306	0.214	-5.55	**0.0**
Security	0.555	1.741	0.198	2.8	**0.005**
Sensors	0.25	1.284	0.214	1.17	0.243
Thermostats	0.07	1.072	0.228	0.31	0.76

TABLE 7. REGRESSION RESULTS OF CLMM FOR UPDATE URGENCY.

Independent Variable	Coefficient	Odds Ratio	Std Error	z	p
Gender (baseline = Female)					
Male	0.111	1.118	0.32	0.35	0.728
Age (baseline = 65+)					
18 - 24	0.355	1.426	0.618	0.57	0.566
25 - 34	0.786	2.194	0.532	1.48	0.14
35 - 44	0.857	2.356	0.442	1.94	0.053
45 - 54	0.978	2.66	0.605	1.62	0.106
55 - 64	1.25	3.488	0.487	2.56	**0.01**
Education Level (baseline = Graduate degree)					
Less than high school	1.573	4.821	1.029	1.53	0.126
High school degree	0.459	1.582	0.599	0.77	0.443
Some college	0.997	2.71	0.571	1.74	0.081
Associate's degree	0.867	2.285	0.624	1.39	0.163
Bachelor's degree	0.459	1.582	0.485	0.95	0.344
IT Experience (baseline = No)					
Yes	0.681	1.975	0.433	1.57	0.116
Smart Home Experience (baseline = 6+ years)					
Less than 1 year	-1.238	0.29	0.881	-1.4	0.16
1 - 2 years	-0.157	0.855	0.462	-0.34	0.735
3 – 5 years	0.648	1.91	0.421	1.54	0.124
Device Category (baseline = voice assistants)					
Lighting	-0.367	0.692	0.213	-1.72	0.085
Security	1.007	2.737	0.204	4.93	**0.0**
Sensors	0.531	1.701	0.218	2.44	**0.015**
Thermostats	0.413	1.511	0.229	1.8	0.071

TABLE 8. REGRESSION RESULTS OF CLMM FOR SECURITY CONCERN.

Independent Variable	Coefficient	Odds Ratio	Std Error	z	p
Gender (baseline = Female)					
Male	0.017	1.017	0.4	0.04	0.966
Age (baseline = 65+)					
18 - 24	1.745	5.723	0.782	2.23	**0.026**
25 – 34	1.192	3.293	0.665	1.79	0.073
35 - 44	1.509	4.522	0.556	2.71	**0.007**
45 - 54	0.893	2.441	0.755	1.18	0.237
55 - 64	1.155	3.173	0.603	1.91	0.056
Education Level (baseline = Graduate degree)					
Less than high school	0.54	1.717	1.271	0.43	0.671
High school degree	-0.996	0.369	0.751	-1.33	0.185
Some college	-1.217	0.296	0.714	-1.7	0.088
Associate's degree	-0.933	0.394	0.783	-1.19	0.234
Bachelor's degree	-1.474	0.229	0.61	-2.42	**0.016**
IT Experience (baseline = No)					
Yes	0.67	1.953	0.538	1.25	0.213
Smart Home Experience (baseline = 6+ years)					
Less than 1 year	1.33	3.783	1.122	1.19	0.236
1 - 2 years	0.223	1.249	0.582	0.38	0.702
3 – 5 years	0.042	1.042	0.527	0.08	0.937
Device Category (baseline = voice assistants)					
Lighting	-1.552	0.212	0.206	-7.52	**0.0**
Security	-0.097	0.908	0.177	-0.55	0.584
Sensors	-0.697	0.498	0.198	-3.53	**0.0**
Thermostats	-1.072	0.342	0.215	-4.99	**0.0**

TABLE 9. REGRESSION RESULTS OF CLMM FOR DEVICE SECURITY.

Independent Variable	Coefficient	Odds Ratio	Std Error	z	p
Gender (baseline = Female)					
Male	0.476	1.61	0.317	1.5	0.133
Age (baseline = 65+)					
18 - 24	-0.695	0.5	0.616	-1.13	0.259
25 – 34	0.412	1.51	0.524	0.79	0.431
35 - 44	0.988	2.687	0.442	2.24	**0.025**
45 - 54	-0.065	0.937	0.595	-0.11	0.913
55 - 64	0.33	1.391	0.476	0.69	0.488
Education Level (baseline = Graduate degree					
Less than high school	-0.877	0.416	0.998	-0.88	0.38
High school degree	0.688	1.99	0.591	1.16	0.244
Some college	0.265	1.303	0.561	0.47	0.637
Associate's degree	0.153	1.166	0.614	0.25	0.803
Bachelor's degree	0.629	1.876	0.481	1.31	0.192
IT Experience (baseline = No)					
Yes	0.768	2.155	0.429	1.79	0.073
Smart Home Experience (baseline = 6+ years)					
Less than 1 year	-3.039	0.048	0.91	-3.34	**0.001**
1 - 2 years	-0.684	0.505	0.459	-1.49	0.136
3 – 5 years	-0.294	0.745	0.416	-0.71	0.479
Device Category (baseline = voice assistants)					
Lighting	1.37	3.928	0.221	6.18	**0.0**
Security	0.537	1.711	0.193	2.77	**0.006**
Sensors	0.858	2.357	0.218	3.94	**0.0**
Thermostats	1.21	3.354	0.233	5.2	**0.0**

TABLE 10. REGRESSION RESULTS OF CLMM FOR PRIVACY CONCERN.

Independent Variable	Coefficient	Odds Ratio	Std Error	z	p
Gender (baseline = Female)					
Male	0.205	1.227	0.353	0.58	0.561
Age (baseline = 65+)					
18 - 24	1.829	6.231	0.685	2.67	**0.008**
25 – 34	1.371	3.938	0.588	2.33	**0.02**
35 - 44	1.635	5.128	0.493	3.32	**0.001**
45 - 54	1.188	3.281	0.668	1.78	0.076
55 - 64	1.289	3.628	0.531	2.43	**0.015**
Education Level (baseline = Graduate degree)					
Less than high school	0.13	1.139	1.18	0.11	0.912
High school degree	-0.951	0.386	0.66	-1.44	0.15
Some college	-1.247	0.287	0.628	-1.99	**0.047**
Associate's degree	-0.27	0.764	0.688	-0.39	0.695
Bachelor's degree	-0.947	0.388	0.538	-1.76	0.078
IT Experience (baseline = No)					
Yes	0.243	1.275	0.476	0.51	0.61
Smart Home Experience (baseline = 6+ years)					
Less than 1 year	1.934	6.92	1.004	1.93	0.054
1 - 2 years	0.416	1.516	0.51	0.82	0.415
3 – 5 years	0.175	1.191	0.463	0.38	0.705
Device Category (baseline = voice assistants)					
Lighting	-1.715	0.18	0.204	-8.41	**0.0**
Security	-0.223	0.8	0.172	-1.3	0.195
Sensors	-1.402	0.246	0.2	-7.0	**0.0**
Thermostats	-1.453	0.234	0.211	-6.87	**0.0**

TABLE 11. REGRESSION RESULTS OF CLMM FOR DEVICES PROTECT PRIVACY.

Independent Variable	Coefficient	Odds Ratio	Std Error	z	p
Gender (baseline = Female)					
Male	0.365	1.441	0.342	1.07	0.286
Age (baseline = 65+)					
18 - 24	-0.321	0.725	0.666	-0.48	0.63
25 – 34	1.248	3.483	0.572	2.18	**0.029**
35 - 44	1.465	4.327	0.479	3.06	**0.002**
45 - 54	0.632	1.881	0.646	0.98	0.328
55 - 64	0.211	1.234	0.514	0.41	0.682
Education Level (baseline = Graduate degree)					
Less than high school	-0.197	0.821	1.1	-0.18	0.858
High school degree	1.286	3.62	0.641	2.01	**0.045**
Some college	0.411	1.509	0.606	0.68	0.497
Associate's degree	0.312	1.366	0.666	0.47	0.639
Bachelor's degree	0.486	1.626	0.519	0.94	0.349
IT Experience (baseline = No)					
Yes	0.332	1.393	0.462	0.72	0.473
Smart Home Experience (baseline = 6+ years)					
Less than 1 year	-2.956	0.052	0.953	-3.1	**0.002**
1 - 2 years	-1.32	0.267	0.499	-2.64	**0.008**
3 – 5 years	0.574	0.563	0.45	-1.28	0.202
Device Category (baseline = voice assistants)					
Lighting	1.002	2.722	0.218	4.59	**0.0**
Security	1.1	2.992	0.202	5.42	**0.0**
Sensors	1.2	3.305	0.223	5.35	**0.0**
Thermostats	1.002	2.724	0.235	4.26	**0.0**