"It's up to the Consumer to be Smart": Understanding the Security and Privacy Attitudes of Smart Home Users on Reddit

Jingjie Li[1], Kaiwen Sun[2], Brittany Skye Huff[1], Anna Marie Bierley[1],
Younghyun Kim[1], Florian Schaub[2], and Kassem Fawaz[1]
[1]University of Wisconsin–Madison, {*jingjie.li, bshuff, bierley, younghyun.kim, kfawaz*}@*wisc.edu*
[2]University of Michigan, {*kwsun, fschaub*}@*umich.edu*

Abstract—**Smart home technologies offer many benefits to users. Yet, they also carry complex security and privacy implications that users often struggle to assess and account for during adoption. To better understand users' considerations and attitudes regarding smart home security and privacy, in particular how users develop them progressively, we conducted a qualitative content analysis of 4,957 Reddit comments in 180 security- and privacy-related discussion threads from `/r/homeautomation`, a major Reddit smart home forum. Our analysis reveals that users' security and privacy attitudes, manifested in the levels of concern and degree to which they incorporate protective strategies, are shaped by multi-dimensional considerations. Users' attitudes evolve according to changing contextual factors, such as adoption phases, and how they become aware of these factors. Further, we describe how online discourse about security and privacy risks and protections contributes to individual and collective attitude development. Based on our findings, we provide recommendations to improve smart home designs, support users' attitude development, facilitate information exchange, and guide future research regarding smart home security and privacy.**

1. Introduction

With the wide adoption of smart home technologies such as smart speakers, thermostats, and door locks, users enjoy the conveniences of automated daily experiences and the reduction of repetitive menial tasks [90]. However, as these technologies impact users' lives in various aspects, they also present unprecedented security and privacy (S&P) threats to users and their environments [33], [85], [88]. Existing work has looked into the role of S&P in users' adoption of smart home technology, especially during the acquisition and use stages [26], [28], [29], [45], [88]. Users factor S&P qualities of smart home products into their purchases, despite the observation that they may not be fully aware of S&P risks [28], [45]. Users may also come to realize S&P issues and implement reactive mitigation strategies during actual usage [29], [88].

Throughout the adoption journey, users' experiences with a product represent a reflective process from pre-purchase to post-consumption [41]. Considering S&P as a critical part of the user experience [85], [86], users exhibit varying S&P attitudes and concerns [25], [44]. While existing studies on users' S&P perceptions of smart home have primarily focused on singular timepoints in the adoption journey and are often conducted in controlled contexts using methods such as interviews and surveys [28], [33], [85], [88]; these studies may miss the rich dynamics when users develop their S&P considerations and attitudes over time. Meanwhile, little research has investigated and holistically understood how users organically develop varying S&P considerations and attitudes throughout their adoption journey.

Recently, researchers have started leveraging online communities to study users' attitudes, including those on S&P-related topics, in vivo [48], [73], [74]. Online communities provide venues for many smart home users to seek product information and exchange S&P ideas. Members of such online communities collectively drive the topics and discussions based on their interests. As such, we choose a smart home-related online discussion forum to investigate *how smart home users develop S&P considerations, which shape their S&P attitudes during the adoption of smart home products.* We investigate our main research objective through three research questions:

- **RQ1:** [Consideration] What are users' S&P considerations in the adoption of smart home technologies?
- **RQ2:** [Attitude] What are users' attitudes toward S&P, and how do users' S&P considerations shape them?
- **RQ3:** [Discourse Influence] How does online discourse influence users' S&P considerations and attitudes?

We utilize Reddit (`www.reddit.com`), a major online platform of interest-based communities, as our research site. In particular, we analyze users' discussions in `/r/homeautomation`, [1] one of the largest forums for smart home users. This forum covers a broad range of specific and in-depth S&P topics, making it a suitable medium to study how smart home users develop S&P considerations and attitudes. We conducted a qualitative content analysis of 180 discussion threads, including 4,957 comments.[2]

Our analysis contributes rich insights into users' dynamic considerations and attitudes. First, users develop two types of evolving and multi-dimensional S&P considera-

[1] https://www.reddit.com/r/homeautomation/

[2] Reddit uses a tree-like structure called "comment thread" for online discussion. One user starts a thread with an initial post (root comment), and other users may leave comments under the post or other comments [18].

tions: (1) S&P concerns regarding smart home technologies and (2) protective strategies during adoption. We observe that a set of interplaying contextual factors shape these considerations, including adoption phases and product factors (**RQ1**). Second, users' S&P considerations map to five categories of attitudes, namely dismissiveness, exploration, resignation, positive pragmatism, and devotion; each attitude combines the user's degree of S&P concern and level of incorporating protective strategies. We show that users' S&P attitudes are context-dependent and evolve according to the progression of considerations as they seek and gain information. However, their preconceptions may override a more objective assessment (**RQ2**). Third, while users exchange opinions and resolve ambiguity to develop S&P considerations and attitudes, they also wrestle with occasional social pressures and inaccessibility of accurate information during online discussion (**RQ3**).

Based on our findings, we provide recommendations to better support smart home users' evolving and dynamic S&P considerations and attitudes with improved designs and practices, S&P nudging, and information exchange. Finally, we inform future research to study smart home users' longitudinal attitudes from multiple angles, the geopolitical and cultural influences, and the impact of information access on smart home users' attitudes.

2. Related Work

Security and privacy concerns and smart home adoption. Prior research highlighted users' unique S&P concerns toward smart home products. From the security perspective, users worry about vulnerabilities and threats in smart home products and networking, such as malicious devices, adversarial control, and cloud insecurity [85]. They also fear security compromises that lead to physical safety hazards [34]. Concerns of smart home privacy issues arise when users' private activities and information such as conversation and precise location data are collected [16], [17], [88]. While some users are aware of respective risks, others lack a full understanding of certain sensitive practices and risks, including how data is exploited for analytics [1], [71]. Often, users' limited technical knowledge results in bias and lack of S&P concerns [85], [88].

Users are also concerned about the stakeholders involved in the smart home ecosystem, including users with different roles, companies, and government entities. For instance, in multi-user smart homes, different users' varying S&P concerns can remain unresolved due to current role-based access control approaches [20], [32], [37], [86]. In particular, less tech-savvy users, such as children, are treated as passive smart home users who encounter privacy and safety issues [70]. Users further think companies and governments should be responsible for addressing smart home privacy concerns [33].

Users do not develop all S&P concerns at once. While some studies found that users lack S&P awareness or concerns before purchase, others identified users' realization of S&P issues through use [27], [29], [70]. Researchers have quantified the effect of S&P attributes on purchase willingness in relation to risk perception and other concerns such as usability [27]–[29]. In hypothetical scenarios where users are prompted with threats, users show higher demand for S&P protective strategies [71]. Whereas in actual use, users would repurpose a product to mitigate S&P risks [14] or ultimately abandon a certain smart home feature or S&P control [39].

Unlike many studies that have investigated users' S&P concerns at a single point in time or in hypothetical scenarios, our analysis of users' S&P discussion on `/r/homeautomation` enables us to study how S&P considerations progress during adoption over time without researchers' intervention.

Security and privacy attitudes. Researchers studied users' S&P attitudes and the associated behaviors. Westin segmented users' privacy attitudes into three groups, corresponding to high, medium, and low levels of concerns [44]. However, Watson et al. found that users' S&P attitudes tend to be more complex [79]. Dupree et al. clustered users' attitudes according to how they are motivated to protect their privacy and their knowledge about privacy [25]. Users also present paradoxical privacy choices as their self-reported privacy attitudes and concerns are inconsistent with their actual behaviors [10].

This disconnect can be attributed to the complex context of S&P, which is often missing in attitude predictors [83]. While many users are "very concerned" about privacy, a myriad of factors impacts users' privacy behaviors [4], [5], e.g., the reward in trading off privacy for convenience [2], [8], [82], the trust of entities that request information [40], self-efficacy [33], [46], [56], [81], and social influence [6], [30]. Moreover, triggers such as social influences, external events, and active priming can change users' attitudes and behaviors [23], [48], [53], [57], [60], [78]. Compared to prior work that categorizes users according to their static S&P attitudes [25], [44], our study focuses on how users' attitudes evolve through the interplay of considerations about S&P concerns and protective strategies when users interact with each other in an online social discussion setting.

Online discussion of security and privacy. Social interaction influences users' S&P preferences [27] and behaviors [23]. Online discussion offers people a platform to exchange opinions, learn from each other, and provide support. Users consider S&P in this collaborative environment [72], [78], but online discussions about S&P topics only recently started gaining attention [13], [48], [74], [76], [80]. This is possibly because users tend to focus more on functional requirements.

Despite the challenges in locating relevant discussions about S&P, researchers uncover insights of S&P from online discussion [48], [65], [73], [77]. Analysis of online discussions concerning intimate partner violence showed that such an approach is useful for studying issues of their safety and security [13], [76], [80]. Meanwhile, in the privacy realm, prior research using discussion forums has investigated software developers' questions about privacy [74], advice for privacy [73], and in-depth discussion about data practices [48]. However, how smart home users discuss S&P online remains elusive. To the best of our knowledge, our work is the first to leverage online discussion data (Reddit) to understand smart home users' S&P considerations and attitudes. Moreover, we study the interaction dynamics created by multiple users to show how attitudes and discussion patterns influence each other, other than the topics and intent of individual users' commenting [48], [74].

3. Method

We analyzed online discussions on Reddit to investigate how users' S&P considerations are discussed during their adoption of smart home products. This approach has the advantage of observing people's actual behaviors and information-seeking processes. A large body of research has studied the discussion on Reddit platform, with increasing interest by S&P researchers [13], [48], [76], [77]. Reddit uses a threaded structure in discussion – each initial post (root comment) is followed by a series of comments over time. This feature provides an opportunity to observe discourse and interaction dynamics among discussants [48].

Reddit consists of subreddits, which are forums for specific topics. We looked for smart home-related subreddits that cover diverse products and integration levels. We decided to focus on `/r/homeautomation`, compared to other smart home-relevant subreddits suggested by Reddit's engine [64], for multiple reasons. First, it includes broad topics, diverse brands, products, and smart home ecosystems to support users' varying needs in different adoption and use phases, from seeking purchase advice to recommending customized automation. Existing work has leveraged the same subreddit to study smart home users but did not focus on the S&P aspects [7], [31], [42]. Second, `/r/homeautomation` has a large user base. Established in 2010, `/r/homeautomation` has about 1.6M members as of March 2022, much larger than other relevant subreddits, e.g., the second largest `r/homenetworking` (223K members) and the third largest subreddits `r/smarthome` (133K members) suggested by Reddit.[3] Third, `/r/homeautomation` has over 20 new threads per day, providing rich data to study.

3.1. Dataset

Identifying discussion threads relevant to S&P from `/r/homeautomation` is non-trivial because of the massive amount of data and high diversity in the S&P terminology being used. Neither a manual nor a keyword-based approach is desirable due to the huge effort and lack of inclusiveness. Instead, we used a semi-automatic approach with a customized machine learning filter to increase the inclusiveness of data while easing human involvement. Our data collection and study received an 'exempt' determination from our Institutional Review Board. We downloaded data from `pushshift.io`, which maintains an up-to-date public archive for Reddit and complies with Reddit's terms of service in data collection and maintenance [12], [59]. `pushshift.io` ingests data through Reddit's official application programming interface (API) and handles removal requests, although some removal requests may not be timely [11], [58]. Following prior work that used `pushshift.io` [48], [67], we neither de-anonymized users nor included sensitive data.

3.1.1. Initial corpus collection & cleaning. Leveraging `pushshift.io`, we downloaded all available comments on the `/r/homeautomation` subreddit between December 2010 and June 2021. By excluding threads and comments deleted or removed by the administrator or the user, the resulting corpus contains 46,637 threads with an average number of 12.72 comments per thread (*std* = 19.98).

3.1.2. Automated selection of candidate threads. To identify threads with S&P topics, we leveraged machine learning to process natural language text through fine-tuning a binary classification model to report a sentence's relevance to S&P on a pre-trained DeBERTa model [36]. We adapted it for our corpus and task since there is no perfectly sufficient off-the-shelf trained model.

Annotating the training data. Two authors, both experts in information and computer security, independently labeled 1,000 samples by their relevance to S&P-related topics. In annotation, we considered criteria adopted in multiple prior studies on S&P, such as the CMU taxonomy of Internet of Things S&P [26], [28], [29]. These aspects included data privacy, platform security, vulnerability, etc.

Evaluating sentence classification. We achieved a Cohen's Kappa κ of 0.92 from our annotation, showing high intercoder agreement. We obtained 115 positive samples among the 1,000 coded samples. Then we randomly sampled 800 sentences for fine-tuning our machine learning filter and 200 samples for sentence testing. The model we trained attained a satisfactory F1 (micro-averaged) score of 0.965 on sentence classification.

Generating thread candidates. We considered a thread a candidate if the classifier labeled at least one sentence positive (i.e., related to security or privacy) within the thread. This strategy optimized for reducing the false-negative rate by capturing relevant discussions as much as possible. The same strategy will result in a higher false-positive rate as sentences might be taken out of context. However, we can still accommodate a non-low false positive rate as manual coding rules out false-positive threads. For validation, we sampled 50 threads from a pool, mixing an even number of positive and negative threads reported by our filter. The same annotators labeled these 50 threads (κ = 0.82) without prior knowledge about the prediction. As a result, we found 13 misclassifications among the 50 threads, with only one of them corresponding to a false negative, indicating that the classifier is unlikely to miss relevant threads. We opted to deal with false positives later on in the qualitative cod-

[3] We show a comparison of subreddits in Table 1 (Appendix).

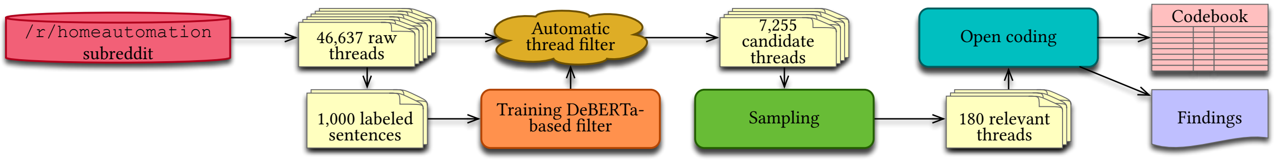

Figure 1. Our data analysis pipeline.

ing stage. In summary, the filter identified 7,255 candidate threads from the entire corpus.

3.1.3. Sampling. Following the guidelines in prior research, we randomly sampled and coded threads, from the period between 2010 and 2021, until we reached data saturation [68]. Threads not relating to smart home S&P were filtered out in the process. In total, we coded and reached saturation with 180 relevant threads (4,957 comments) among 303 random candidates sampled from all 7,255 threads.

3.2. Data Analysis

Our analysis considered all comments over time in each thread. First, two authors went through 28 threads to create the analytical memos that revealed initial codes. The research team discussed these codes, clarified definitions, resolved disagreements, and established an initial codebook. Then, these two authors independently coded a subset of 15–20 threads randomly sampled from the dataset each time, while comparing codes and revising the codebook iteratively until high inter-rater reliability at the comment level was reached ($\kappa = 0.74$) at the 82nd thread. Using the revised codebook, the two authors then split the samples and coded independently until hitting saturation at the 180th thread. Then, we revisited all threads multiple times and conducted thematic analysis. We make our codebook available online.[4] From the 180 threads, we observed 2,181 users. Noticeably, 477 of them actively participated in S&P-related discussions.

3.3. Limitations

Our analysis has several limitations. First, there is sample selection bias as we collected data from /r/homeautomation. Presumably, users on this forum are more passionate and knowledgeable about smart homes than the general population. This is reflected in our observation, where many users demonstrated extensive knowledge of device functions and the associated S&P issues. Second, we did not have access to our sample's demographic data such as age, gender identity, education level, or occupation. So it is difficult to ascertain whether the demographic distribution of the sample is reflective of the general population. Future work may want to study how smart home S&P is discussed on other forums with different focuses or within other populations. Third, in our findings, we discuss various actions such as abandoning product ownership. As is common with self-reported behavior, users' discussions may not necessarily correlate with their actual actions. Fourth, our focus in this work is not the temporal relation between different threads, which potentially captures more dynamics of how users develop considerations and attitudes in a longer period of time. Finally, our methodology to detect S&P-related discussion using text classification is generalizable across different domains, e.g., Twitter, and future work may leverage our content analysis and codebook. However, the quantitative results we report are less likely to generalize due to the Reddit population that is presumably more tech-savvy. Keeping these limitations in mind, our research still revealed significant trends in S&P discussions in a previously unstudied population, and it fills a gap in the literature about users' S&P considerations and attitudes.

3.4. Roadmap

In the following sections, we present the findings in correspondence with our research questions. Figure 2 shows our analysis framework. We first reveal users' S&P considerations in Section 4 – how they assess their S&P concerns and incorporate S&P protective strategies – given the contextual factors, such as adoption phases and product factors. Then, in Section 5 we map the considerations to five major categories of S&P attitudes during smart home product adoption, namely dismissiveness, exploration, resignation, positive pragmatism, and devotion. Lastly, we discuss how online discourse influences users' S&P considerations and attitudes in Section 6. In addition, we show the prevalence and co-occurrence of themes and subthemes regarding the three research questions from Figure 3 to 8 to support our qualitative findings.

4. RQ1: Security and Privacy Considerations

Our analysis of /r/homeautomation reveals two types of user considerations: (1) their S&P concerns regarding smart home technologies and (2) how they incorporate protective strategies during adoption. We observe that a set of interplaying contextual factors shape these considerations, including adoption phases and product factors. Next, we describe the contextual factors, explain how users consider S&P issues, and show how users incorporate S&P-protective strategies in smart home adoption. We note, however, that users do not necessarily fully develop their considerations during discussion or may only exhibit a subset of them in their comments.

[4] https://osf.io/2zs9n/?view_only=e40279edd16b459883b3680ece0546bc

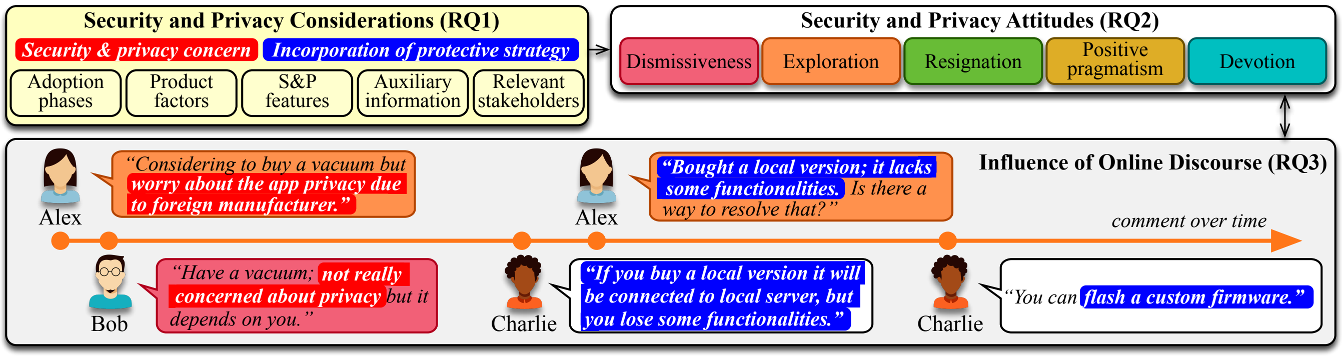
Security and Privacy Considerations (RQ1)
Security & privacy concern
Incorporation of protective strategy
Adoption phases
Product factors
S&P features
Auxiliary information
Relevant stakeholders
Security and Privacy Attitudes (RQ2)
Dismissiveness
Exploration
Resignation
Positive pragmatism
Devotion
Influence of Online Discourse (RQ3)
Alex
"Considering to buy a vacuum but worry about the app privacy due to foreign manufacturer."
Bob
"Have a vacuum; not really concerned about privacy but it depends on you."
Charlie
"If you buy a local version it will be connected to local server, but you lose some functionalities."
Alex
"Bought a local version; it lacks some functionalities. Is there a way to resolve that?"
Charlie
"You can flash a custom firmware."
comment over time

Figure 2. Our analytical framework with a paraphrased Reddit thread as an example. The texts that show either considerations of concern and protective strategies are color-coded by red and purple. The text box's color aligns with the user's S&P attitude in discourse, if exists. In this example, Alex started a thread to seek advice on buying a robot vacuum with potential privacy concerns due to its foreign manufacturer. Bob declared that they were aware but not concerned about privacy of the vacuum personally. Charlie offered an alternative to acquiring the local version that does not connect to the foreign server. Following Charlie, Alex confirmed their purchase of the local version and further sought advice to balance its privacy tradeoff with the functionality. During both pre- and post-purchase, Alex showed considerations of privacy concerns and protective strategies, demonstrating an exploration attitude; Bob dismissed their concern.

4.1. Contextual Factors

During the discussion, users reference a range of factors affecting their considerations. Our thematic analysis reveals five themes of contextual factors: adoption phases, product factors, S&P features, auxiliary information, and relevant stakeholders.

Adoption phases. Users' S&P considerations evolve during the discussion according to their adoption phase for a product. Consistent with prior work [19], [29], [54], we observe four major phases: *consideration of product acquisition*, e.g., purchase, inheriting, and sharing; *acquisition of the product but not in use*; *active use*, during which users may personalize the product; and *abandonment or transfer of product ownership*.

Product factors. Product-related factors during the discussion lead to users' awareness of S&P issues. We observe that users reference two kinds of product factors: *quality requirements* and *technology features*. Product quality requirements include compatibility, reliability, price, customization, and core functionality. Examples of the technology features of products include (open-source) software, cloud dependency, connectivity, user control, and data storage.

Security & privacy features. Users also reference specific S&P features of the product. These features fall into five categories: *account access* (e.g., resource authorization), *safety measures* (e.g., data backup), *system integration* (e.g., exposure to network), *privacy options* (e.g., rights to review, edit, and delete their data), and *security features* (e.g., encryption).

Auxiliary information. Users leverage auxiliary information about S&P aspects throughout their adoption journey. We identified two types of information sources: *public information channels* and *evidence from real-life interaction*. The former covers news and reports, social media, customer reviews, or privacy policies. The latter includes experiences of suspicious activities or communications with customer support.

Relevant stakeholders. In addition to external attackers, users recognize different stakeholders in the smart home ecosystem. These stakeholders include *companies* (manufacturers, vendors, and service providers), *governments*, *users*, and other *third parties*. Users associate stakeholders with different roles. For example, the government can serve as a regulator or a possible adversary. Similarly, third parties can provide compliance oversight or impose threats. Lastly, users discuss sharing devices in multi-user smart home scenarios, with attention to special populations, e.g., children and the elderly.

4.2. Developing Security and Privacy Concerns

The first component of S&P considerations is developing S&P concerns. As users develop S&P concerns, they perform threat modeling that consists of three themes as shown in Figure 3: *security and privacy awareness* – recognition of potential concern, *threat identification* – mapping of potential to actual threats based on smart home products and associated stakeholders, and *risk assessment* – assessment of the likelihood and severity of threat influences. Next, we elaborate on the three themes and the subsequent subthemes; Figure 3 depicts the frequency of each subtheme in the coded threads.

4.2.1. Security and privacy awareness.

The first theme describes how users' needs, the adoption phases, and information sources drive their S&P awareness. It includes two subthemes: how contextual factors contribute to awareness and how awareness evolves according to contextual factors. Figure 3 shows a noticeable contribution of contextual factors to S&P awareness, compared to other subthemes.

Contextual factors contribute to awareness. Users' S&P awareness arises from the smart home device features they

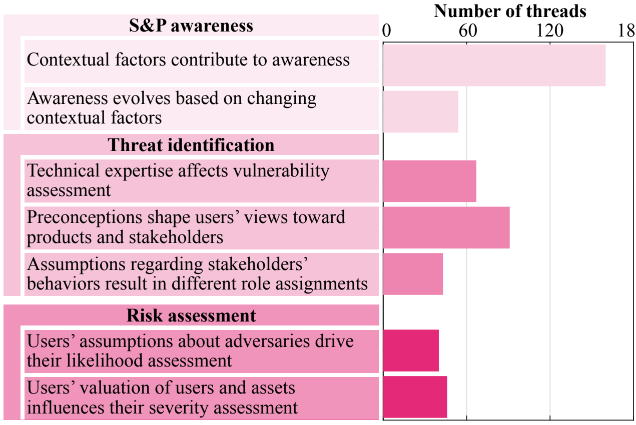

Figure 3. Three themes and the frequencies of seven subthemes of users' considerations in developing security and privacy concerns. Note that when we refer to "contextual factors" in a subtheme, it indicates a list of items, as we explain in Section 4.1, such as S&P features and auxiliary information.

deploy to address their needs. Users associate specific concerns (eavesdropping, spying, safety hazard, etc.) with distinctive product modalities, such as audio recording by voice assistants or room scanning by a robot vacuum. For example, one user expressed concern about their smart lock being tampered via *"the digital part than the actual deadbolt"* (U6-T33). Many concerns center around devices' dependency on the Internet or cloud to function, e.g., trigger-action services through MQTT, which may possibly *"expose something on your home network to the internet"* (U2-T9). Also, S&P information contributes to users' awareness. For example, one user was concerned about the *"(lack of) privacy policy"* prior to purchasing a product (U40-T29). Additionally, awareness arises from users' specific use cases, such as remotely allowing tenants to enter a rental home via smart entrance by giving them *"a one use access code to dial on pad"* (U1-T155).

Awareness evolves based on changing contextual factors. Users interact with stakeholders, products, and information sources across adoption phases, prompting an evolution of S&P awareness. We find that before acquiring a new product, users have abstract S&P awareness; they are more concerned about product features. The awareness becomes more concrete after the purchase, when users describe specific concerns about the product. In one case, even before receiving the purchased device, a user developed a concern about a phone call they received about the product due to *"the information [shipping location, credit card, etc.]"* the caller asked for (U1-T8).

After acquiring the product, user awareness becomes more specific to their experience with the device or stakeholders. The example below shows that the user returned a thermostat after they had noticed its lack of privacy options:

> *"Yeah i had gotten a discounted nest thermostat from my power company but after seeing their reluctance to let me access *my own data* i returned it."* (U5-T69)

During adoption, auxiliary S&P information, such as media reports, further contributes to a user's awareness, as evident in one user's complaint about a company's response to a threat:

> *"8 months ago Ring's VP said he'd come back here to tell us when their firmware stopped sending data to China. He hasn't commented since."* (U1-T139)

Awareness about S&P issues persists post abandonment. For example, when transferring their device to others, one user recommended to *"wipe everything from my [their] accounts, setup new accounts...and hand it over"* (U4-T23).

4.2.2. Threat identification.

The second theme of developing S&P concerns covers users identifying specific threats in their smart home, such as data misuse, unwanted data collection, and surveillance. This theme consists of three subthemes. First, users' technical expertise affects their vulnerability assessment. Second, their preconceptions and assumptions – preconceptions are subjective while assumptions are more situational – of stakeholders shape how they define the adversary. Third, users assess the vulnerability in smart homes and place stakeholders as adversaries, victims, or good Samaritans.

Technical expertise affects vulnerability assessment. Although some users name specific attacks, several exhibit uncertainty regarding how particular products or technologies are vulnerable. For example, when discussing buffer overflow attacks on device firmware, one commentator confused the device firmware with the wireless protocol it employs:

> *"I assume Z-Wave doesn't suffer from this problem due to the certification process? Or are there attack vectors that could be leveraged against that particular tech?"* (U4-T133)

Further, insufficient technical understanding manifests in over- or under-estimation of the threat. One user described any device requiring an Internet connection as insecure when comparing products that rely on WiFi connectivity versus those on Zigbee and Z-Wave. In the same thread, another user clarified the threat model, comparing WiFi versus Zigbee and Z-Wave devices, that the latter are *"not IP routable so they are much more difficult to use as attack vectors"* (U19-T79).

Preconceptions shape users' views toward products and stakeholders. Users carry preconceptions, e.g., perceived trust, reputation, or reliability, which they *"hearken from the bad old days"* and reflect in their views toward products or stakeholders (U3-T51). These preconceptions can arise from previous experience with a stakeholder. For example, when considering a replacement purchase, one user warned others *"DO NOT buy a Skybell [smart doorbell they want to replace]"* by referencing their concern about the security and reliability of a smart doorbell from their prior use and issues *"that are well documented across Reddit"* (U1-T11).

Further, users exhibit differing trust and reputation preconceptions for the same stakeholder; for example, one thought *"Apple's reputation for privacy far outweighs Amazon's"*, while another was more positive about Amazon because *"historically speaking, Amazon is much more protective of user data [compared to Nest]"* (U2-T81, U30-T29).

However, we observe a predominant distrust toward Chinese smart home companies, not just particular brands, on privacy and quality. For instance, one user argued:

> *"Not specifically for Xiaoyi, but it is quite common for low-priced Chinese brands to have embedded backdoors or privacy-invading snooping by the company."* (U15-T58)

This distrust possibly arises from the perceived tie between Chinese manufacturers and authorities, sometimes described as the *"Chinese state overlords"* (U17-T119).

Assumptions regarding stakeholders' behaviors result in different role assignments. Users have different assumptions about the behaviors of stakeholders or products (such as security practices). These assumptions result in different assignments of adversarial roles to stakeholders. Users' assumptions also do not necessarily align with their views toward the stakeholder, as shown in the three distinct outcomes below.

First, users associate the for-profit business model with more vulnerable products because their manufacturers *"have zero incentives to patch holes in their older products"* (U6-T3). Second, users consider these companies as an adversary because of the *"blatant disregard for the moral and ethical responsibility that companies should have when they have access to such sensitive data"* (U16-T58). Third, the same for-profit business model, interestingly, leads to users assuming companies to be good Samaritans because enforcing data privacy improves their competitiveness:

> *"Well Google records all your data, but they are highly incentivized to keep it safe and not sell it, because having exclusive access to it is their core business."* (U97-T115)

Similarly, for authorities, some users note their positive role in regulating companies. Below we show an example:

> *"There are laws that vary depending on region, such as Europe's GDPR privacy laws, hence why Facebook is acting like they would pull out of Europe."* (U15-T151)

Others are, however, skeptical about governments' role in regulating smart home companies. One user thought that, because governments are not doing *"what's right about trade," "it's up to the consumer to be smart."* Another user sarcastically responded: *"and... we [users]'re doomed"* (U7-T147, U5-T147).

4.2.3. Risk assessment.

After identifying S&P threats, the third theme involves evaluating the associated risks, i.e., how these threats might affect users' health, finances, and physical and digital assets. This assessment consists of two subthemes: the evaluation of the likelihood and severity of a threat.

Users' assumptions about adversaries drive their likelihood assessment. Users associate the likelihood of attacks with the required technical sophistication. For example, one user assumed that attackers can use a cheap radio to jam a wireless security system that does not employ frequency hopping:

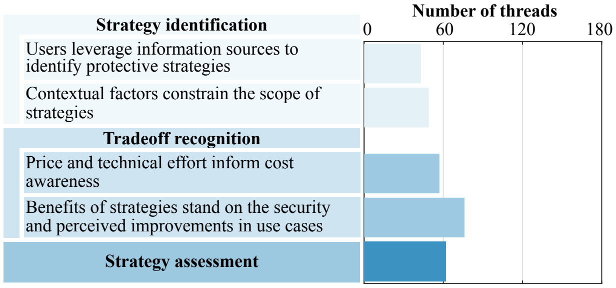

Figure 4. Three themes and the frequencies of five subthemes of users' considerations in examining protective strategies.

> *"I can disable the system with a walkie talkie after using an SDR [software defined radio] to find the exact frequency the system is on and just blast it the entire time I'm in your house . . . $20 baofeng [radio] will kill simplisafe since it uses 433[MHz]."* (U4-T45)

On the other hand, users doubt the likelihood of attacks that appear resource-consuming. For example, an attacker is unlikely *"sitting outside my [their] house for the next month trying to guess"* an 8-digit smart lock code from fingerprint dusting (U3-T100). Some users think certain attacks are unlikely since they bring low benefit to the attackers, e.g., attacking a smart vacuum to reveal *"how dirty your carpet is"* (U3-T125).

Users' valuation of users and assets influences their severity assessment. Even with an adequate threat model, users have different valuations of the associated risks. For instance, while all recognized the threat from a compromised voice assistant, some were concerned about sensitive conversations being recorded by the device when working from home:

> *"I need to deal with sensitive HR [Human Resources] issues from home, all of which should never be recorded without consent of a third party."* (U8-T68)

Similarly, other users elevated perceived risks when special populations interact with devices, due to severe consequences that *"[the elderly] can't escape 99 degree or higher heat"* (U1-T3).

However, others devalued the severity of recorded voice, e.g., chatting with family members, as they thought *"nothing I say in my home is important that I worry someone heard"* (U1-T68).

In contrast, users may assign possible attacks with lower severity based on the countermeasures in place. For example, one user felt their home would be safe as their security system *"is basically tamper proof"* (U46-T30). In that case, the device employed power backup and intrusion alarm against malicious power shutoff and wireless jamming.

4.3. Incorporating Protective Strategies

The second component of S&P considerations is users examining whether and how to incorporate S&P protective strategies into their smart home deployment. We observe two types of protective strategies. The first represents adoption decisions such as the purchase or abandonment of a specific product. The second includes product setup, customization, or configuration such as changing passwords, disabling the Internet, and DIY solutions. We identify three themes of how users arrive at protective strategies: *strategy identification*, *tradeoff recognition*, and *strategy assessment*. First, users identify potential strategies to alleviate S&P concerns (if any), given the adoption context. Second, users recognize the tradeoffs associated with the identified strategies. Last, users assess whether to incorporate the S&P protective strategies after assessing the identified tradeoffs. Figure 4 shows the five subthemes comprising the three themes; the distribution of the subthemes is relatively uniform in the coded threads.

4.3.1. Strategy identification.

4.3.1. Strategy identification. We identify two subthemes for strategy identification. First, users leverage available information sources to explore possible protective strategies. Second, facing the constraints from contextual factors, users narrow the scope of their strategies.

Users leverage information sources to identify protective strategies. Users leverage their knowledge and understanding to explore protective strategies. They build their knowledge or understanding from access to information sources, e.g., online discussions. For example, one user opened a poll for *"best practice advice"* as they sought to secure their smart home against external threats from the Internet (U1-T139). Additionally, users learn about possible strategies from auxiliary information. For instance, a user referenced an online open-source project about rooting a robot vacuum's firmware to alleviate a privacy concern (U3-T73). Stakeholders, including third-party organizations, represent another source of information about possible strategies. In one case, a user praised *"Consumer Reports"* for their *"good write up"* on alternatives for secure smart locks (U3-T100).

Contextual factors constrain the scope of strategies. First, stakeholders, such as companies or governments, might restrict the scope of possible strategies for marketing or legal reasons. For example, returning a product because of a security issue might be infeasible due to a restrictive return policy. In one case, a user asked if they should return a smart lock, within the return period, in response to a warning that indicates it has *"weaker security"* (U1-T122). Additionally, some products lack S&P configurations, forcing users to consider "all-or-nothing" strategies. In other cases, users were unaware of such configurations because they were inaccessible. One comment referred to an interface, which disables cloud access of a smart bulb, as *"[buried] in the app"* (U4-T72).

Second, being a secondary user limits available protective strategies, e.g., one user expressed a loss of control of using a voice assistant with *"3rd party always-on microphones"* in a hotel (U4-T20). Third, inadequate understanding or limited information contributes to constraining the scope of protective strategies. For example, one user mistakenly referenced the U.S. Federal Communications Commission (FCC)'s terms to question the legitimacy of deploying WiFi access control by deauthentication flood in enterprise settings (U8-T128).

4.3.2. Tradeoff recognition. We observe two subthemes in how users recognize tradeoffs associated with the identified strategies. First, the price and technical effort of incorporating a protective strategy inform their cost awareness. Second, users identify the benefits of strategies based on perceived improvements, e.g., enhanced security.

Price and technical effort inform cost awareness. First, users reference the monetary value of a strategy as part of its cost. For example, when a user was wary about buying a security camera from a foreign manufacturer, a user responded:

> *"What's your budget? If you want the best Axis cameras are the most reliable cameras..."* (U12-T75)

Second, users evaluate how the technical effort associated with the customization strategies contributes to the cost. One Reddit user mentioned the technical knowledge and effort needed for a DIY alternative to commercial voice assistants:

> *"Actually if you know python writing a voice assistant capable of controlling your house and doing other basic functions is a matter of a couple days."* (U21-T29)

Benefits of strategies stand on the security and perceived improvements in use cases. The benefits of incorporating a strategy depend on users' use cases, e.g., their smart home setup or feature requirements. Users prefer compatibility between S&P improvements, brought by the strategy, and other desired qualities in their use cases. For example, a potential buyer wanted a *"*very* secure lock"* that is compatible with other functions of HomeKit, Apple's smart home app (U9-T5).

However, users might not be fully aware of the S&P benefits of a strategy, e.g., due to its deployment. For example, one user sought confirmation about whether their exposed information can be limited to only *"details of the separate network, address, and room layout"* if they associate their smart vacuum with a dedicated phone on a separate network (U1-T90).

4.3.3. Strategy assessment. Finally, users assess the tradeoffs between cost and benefits to determine which strategies are viable. Users incorporate strategies when they think the benefits outweigh the cost, e.g., one thought a product that was a *"little pricey"* but *"worth it"* (U4-T18). The user's tradeoff assessment tilted toward the strategy when the use case is important to them. For example, one user preferred to purchase a more secure smart thermostat when the primary user is an older adult: *"[the elderly]'re unable to set their own thermostat, and their caretaker isn't close by to address the situation"* (U1-T3). Some users value the power of customization; even when they perceive a cost from the needed effort to incorporate, the added controls outweigh these costs:

> *"I agree that Homeseer's interface is not the prettiest one around, but so far it does far and away more, is stable, and exposes the "nerd knobs" needed to do darn near anything including secure z-wave."* (U9-T1)

Benefit valuation depends on the user's assumptions and understanding of the threat. Several users perceived an added security benefit when they cover their internal IP in a posted photo as they thought there was *"no reason to give our potentially vulnerable information,"* and *"if they compromise a router, internal IPs could be useful"* (U1-T120, U8-T120). But others considered covering *"non internet routable"* IPs as *"diminishing returns"* since if the router is compromised, these IPs can be easily revealed by port scanning (U7-T120, U10-T120).

When they perceive the cost as outweighing the benefits, users are less motivated to incorporate the strategy. Cost manifesting in a high technical effort can dissuade them from a protective strategy, e.g., when they consider themselves *"not [technically] qualified"* (U3-T73). An extreme case is fatalism [84], where every protective strategy is perceived as ineffective since *"everything can be broken"* (U10-T100).

Takeaway-RQ1. We observe that smart home users' S&P considerations consist of S&P concerns and protective strategies. First, users develop S&P concerns through in-depth and tech-involved threat modeling: becoming aware of the S&P issues, identifying and assessing the actual S&P risks and threats. Second, users identify and assess S&P protective strategies while recognizing cost-benefit tradeoffs. As such, these considerations are multi-dimensional and depend on an interplay of contextual factors in adoption, as shown in Figures 3 and 4. We also find that users' considerations progress according to changing contextual factors, e.g., adoption phases and access to information. These takeaways contrast with prior findings, where users' assessment of threats and protective strategies can be single-dimensional and static [33], [85], [88].

5. RQ2: Security and Privacy Attitudes

We now discuss users' S&P attitudes toward the adoption of smart home products. These attitudes are the result of users' (1) S&P concerns and (2) incorporation of protective strategies. As shown in Figure 5, we identify five categories of attitudes: *dismissiveness* of S&P concerns; *exploration* of possible concerns and protective strategies; *resignation* to incorporating S&P protective strategies; *positive pragmatism* in terms of incorporating protective strategies that balance cost and benefit tradeoffs; and *devotion* to incorporating protective strategies. We observe that one user may exhibit different S&P attitudes as the context varies; users' attitudes may evolve over time during exploration as they advance their considerations with the progressing context or better knowledge of it. As such, we do not segment users based on attitudes. Also, some boundaries between attitudes are blurry (e.g., some pragmatic traits shared in resignation), and users may not fully express their attitudes in online discussion. We complement qualitative insights with frequencies of attitudes to characterize their prevalence. The frequencies in Figure 5 characterize users on this subreddit: many are technically informed and devoted to incorporating protective strategies. Figure 6 shows the co-occurrence of users' attitudes and their considerations.

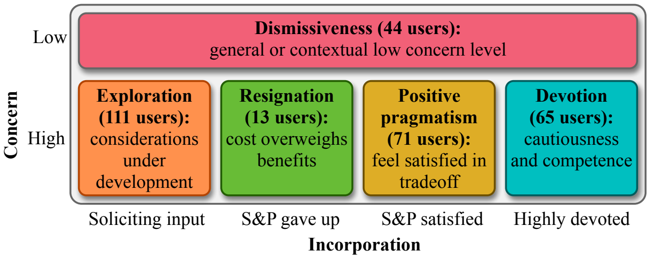
Low
Dismissiveness (44 users):
general or contextual low concern level
Concern
High
Exploration (111 users): considerations under development
Resignation (13 users): cost overweighs benefits
Positive pragmatism (71 users): feel satisfied in tradeoff
Devotion (65 users): cautiousness and competence
Soliciting input
S&P gave up
S&P satisfied
Highly devoted
Incorporation

Figure 5. Users' S&P attitudes in adoption aligned with considerations of concerns and incorporating protective strategies. Representative traits are summarized with each category, and we report the frequency of each attitude among the 255 out of 477 users who revealed their attitudes in S&P-related discussion. Note that one user may hold more than one attitude. We observe more users carrying exploration attitudes than others. Consistent with prior findings [25], [44], we see many pragmatism users. The users devoted to incorporating protective strategies are noticeable, too.

Dismissiveness as a contextual or general attitude. The dismissive attitude refers to users who exhibit low S&P concerns; this attitude leads to users' reluctance to further incorporate protective measures. First, some users exhibit low S&P concerns in general, sometimes regarded as *"wilfull [willful] ignorance"* by others (U12-T20). For example, some users were not concerned about privacy in the smart home because they felt *"privacy honestly isn't of utmost importance to all"* or they *"got nothing to hide"* (U18-T26, U28-T115). Interestingly, these users may rationalize their attitudes by making an analogy with physical privacy:

> *"Personally I'd go with something like, having a private conversation in public and notice the person a table over eavesdropping but don't really care."* (U9-T68)

Second, while some users have general S&P concerns, they might be less concerned about specific use cases. For example, one rationally dismissed their concern *"through some troubleshooting"* after they had determined that the suspicious device traffic was due to repeated attempts of a firmware update (U5-T110). When dismissing a concern, users may appear to be inconsistent, e.g., by saying *"privacy is a big concern, and so is use case,"* when they were not *"personally worried about the privacy implications"* of smart speakers (U4-T180).

Exploration as an attitude while developing considerations. The exploration attitude features users' proactive needs to develop their understanding of S&P threats and protective strategies. Users may exhibit the exploration attitude at different adoption phases, depending on their evolving awareness. Users solicit input from others to educate themselves about possible S&P threats. For instance, one user was open to learning more about integration vulnerability and threat:

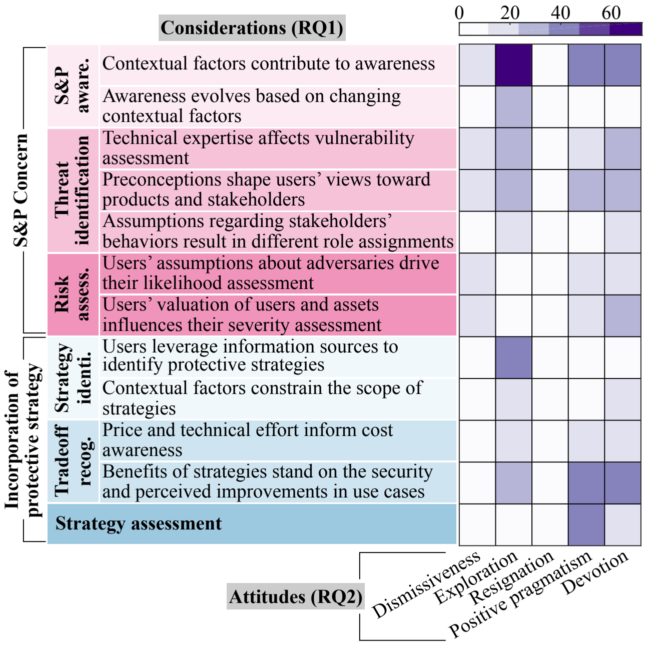

Figure 6. Co-occurrence of users' S&P attitudes with subthemes in considerations, which supports our attitude mapping. For example, users with dismissiveness attitudes rarely consider protective strategies; users demonstrate their devotion and pragmatism by the final assessment of concerns and protective strategies; users seldom reach the final assessment during exploration.

> *"Network security definitely isn't my strong suit, although it is a priority of mine ... I'd definitely like to hear what other people have to say."* (U2-T34)

Others explore additional protective strategies; one user asked for help on Reddit when they noticed a mismatch in the password length limits between their WiFi and a smart AC control:

> *"Have you just shorten your WiFi password, returned the devices and/or find any other solution? What password length do you find both secure enough and compatible with almost any connected device?"* (U1-T41)

After exploration, a user's attitude may change, such as dismissing S&P concerns after troubleshooting (U5-T110).

Resignation as a result of cost outweighing security or privacy benefits. The resignation attitude highlights users who worry about S&P issues but tend to give up on incorporating protective strategies. This resignation results from their perception that the cost of protective strategies outweighs any potential S&P benefits. For instance, one user regarded S&P practices as *"too much of a hassle,"* when they had to include network separation that impacts connectivity (U7-T35). Similarly, another thought price and device availability contributed to their resignation as *"there's not a better option [of a smart door bell]"* compared to other brands (U41-T17).

Another motivation behind resignation is users' fatalism, previously mentioned in Section 4.3.3. They consider S&P threats inevitable due to the loss of control [21]. Such beliefs appear to be a result of users' continuous exposure to tracking, e.g., due to people *"walking around with a cellphone 24/7"* (U6-T38).

Positive pragmatism results from satisfactory tradeoffs. Similar to resignation, this attitude features the tradeoffs users make when considering protective strategies. The difference is that users value S&P more than the other factors. They feel satisfied with protective strategies that strike a compromise between cost and benefits. For example, one voice assistant user *"values convenience over complete privacy"*; they thought opting out of data sharing suffices to protect privacy (U6-T68).

While pragmatic users can be technically competent, they may seek protective strategies with lower costs. One user, who *"program[s] by day,"* felt comfortable with setting up a smart home with network separation rather than setting up a secure smart home by DIY, as *"the last thing I [the user] want to do on the weekend is fiddle with Raspberry Pi"* (U4-T29).

Devotion as a result of caution and competence. Users with high S&P concerns tend to be devoted to S&P-protective strategies. While some users' devotion stems from their overreaction to an incomplete threat model, others are technically competent and enthusiastic about sharing their knowledge.

Devoted users thoroughly form their threat model, even by decompiling an app to examine its encryption standard:

> *"So far I've decompiled the app and found that it uses Ayla Networks IoT platform. Oh and the Cipher Suite for added security."* (U11-T121)

Others form their threat models from their prior experience; one user referenced their job when expressing security concerns about unpatched hubs:

> *"I once worked at a company with 8M customers. My mantra regarding problems was '1 in a million happens every 3 hours' "* (U1-T133)

Some devoted users are capable of incorporating sophisticated mitigation strategies, e.g., multi-layer security:

> *"I still have fallback if somethings fail so i'm never without some degree of protection. Personally I would and have layered the devices in 3 layers, A 'real' security panel for the vital parts where a burglar must pass..."* (U3-T45)

However, devotion does not mean blindly adopting a more technically involved strategy. For example, one user concerned about unpatched hubs showed fatigue in reacting to vulnerabilities, e.g., by patching. They would rather invest in other brands if they were *"going to guess at the next target"* (U1-T133).

Takeaway-RQ2. We map the S&P considerations to five categories of attitudes; each attitude combines the user's degree of S&P concern and level of incorporating protective strategies (Figures 5 and 6). We observe that users' S&P attitudes are context-dependent and evolve according to the progression of considerations. Users do not hold a fixed S&P attitude; their attitudes change depending on the context (e.g., product factors and adoption phase), as many of them proactively seek and gain more information. Also, prior experiences or preconceptions about a product might shape a user's attitude, overriding a more objective assessment. These findings enrich literature where the focus has been traditionally on users' static S&P attitudes [25], [44].

6. RQ3: Influence of Online Discourse

Discourse in an online forum fulfills users' information and social needs despite their varying attitudes. It also fosters users' development of considerations and attitudes. We identify three themes of active interactions in discussing smart home S&P-related topics. These themes are: users' *strategies to resolve ambiguity* in S&P-related discourse; *contributions of the discourse to users' attitude development*; and *the influence of users' varying attitudes on the discourse environment*. We identify seven subthemes, e.g., collaborative exploration through exploration. We show each subtheme's frequency and the co-occurrence of users' attitudes and these subthemes in Figures 7 and 8. These figures support our qualitative findings, e.g., the high occurrence of users with devotion attitudes informing others of alternative strategies, which contradicts prior findings that S&P fundamentalists are reluctant to help [25].

6.0.1. Strategies to resolve ambiguity.

We describe how users resolve problems and confusion collectively.

Collaborative exploration through elaboration. We find that users seek input to complete their understanding of S&P threats and better evaluate protective strategies. They try to resolve ambiguities through iterative elaboration together, which helps them better understand the sources of others' confusion. For example, a user was skeptical of others' concerns about a smart remote and asked for elaboration: *"What are they recording me with? It's an IR blaster"* (U42-T170). After observing concerns about *"someone could tunnel in and eavesdrop on cameras,"* U42-T170 elaborated that this issue may not represent a threat as the device uses a local API.

Transfer of personal experience to a new context. Users become aware of others' backgrounds and contexts when exploring a problem together. So, they transfer personal experiences and understandings to support other people in new smart home contexts. For example, one user suggested blocking internal IPs based on their experience with a router. However, they were aware that this suggestion might not apply to owners of a robot vacuum, as it can hinder the vacuum's functionality.

> *"In my TPLink router, I have an option to block internal IP addresses from accessing the internet. Would it still work at all if it had NO connection?"* (U4-T125)

Supplementary information as evidence. During collaborative exploration, users often use supplementary information to strengthen their arguments. In a thread in which multiple users discussed their concerns about a smart lock's vulnerability, one user cited news about a product update that had potentially patched the vulnerability: *"I believe this was resolved in 2016 with a new version of smart key. [url of the news]"* (U6-T10).

We see other patterns to supplement information, e.g., forum moderators pinning a *"good discussion"* (U4-T139) about S&P for more visibility. This effort, however, seems ad-hoc, and users still have difficulty navigating S&P information on Reddit. For example, one user reused advice across similar threads about networking protocols and security since it is *"a recurring topic and reddit churns so much that reuse makes sense"* (U3-T51).

6.0.2. Contribution to attitude development.

Above, we discussed users' strategies to collectively resolve ambiguity in the discourse related to S&P. Here, we present how users' attitudes change as a result.

The discourse affects S&P concerns. Users' discourse with others makes them more aware of S&P risks (Section 4.2.1), leading them to revisit their attitudes. For example, one user changed their attitude, from exploration to dismissiveness, about a presumed "credit card scam":

> *"Edit: You're right, I wasn't scammed, but if it is a scam, someone else could easily fall for this."* (U1-T8)

However, discourses do not always change opposing attitudes. In a previous example (Section 4.3.1), the intensive debate about the legitimacy of performing a deauthentication flood for access control did not change either of the parties' attitudes. One user described the others as *"knowing participant in a criminal conspiracy"* and rejected their interpretation of evidence from multiple news or legal documents (U5-T128).

The discourse informs alternative strategies. As discussed in Section 4.3, users inform others of S&P protective strategies. Rather than replicating the advice, users take inspiration from the collective wisdom and develop new strategies. For example, being inspired by others' advice on how to transfer smart device ownership securely, a user took a hybrid approach, moving from the exploration to the pragmatist attitude:

> *"UPDATE: I took a hybrid approach. I setup a gmail account for the house and moved all accounts to it. I removed one of my Wink Relays..."* (U1-T23)

A user, who had almost *"abandoned all hope"* in flashing custom vacuum firmware for privacy, benefited from discourse and posted their updates for *"those who might search the forum"* in need (U1-T89). This example shows a user changing their attitude from the resigned to the pragmatist category.

6.0.3. Influence on the discourse environment.

Facing the complex topics of smart home S&P in conjunction with other technical and personal issues, users hold various considerations and attitudes in the discourse. We observe that the sentiment created by users' consensus and disagreement in the discourse influences the discourse environment.

Opposing attitudes result in topic incoherence. When S&P discussions intertwine with other topics, users tend to go off-topic, especially when they have opposing attitudes. In one thread, two users discussed how security systems help thwart the adversary. One user questioned the security improvements of smart cameras compared to an alarm system because it is not temper proof, as *"simply disconnecting your cable will render your comms [communications] useless"* (U4-T16). The discourse then drifted to presumption about personal stances:

> *"We will just have to agree to disagree. I understand your profession as a security system employee is threatened by home automation, and rightfully so."* (U2-T16)

Empathy resonates across attitudes. Some users show empathy when bridging the gaps between different attitudes. Users who share similar considerations are more likely to create empathy and resonance. For example, many users shared similar complaints about voice assistants being activated by kids:

> *"... our son managed to get the Google Home Mini to recognize his 'HEY GOOGLE!!' this morning. People with small children and voice recognition.... Help?"* (U1-T78)

Resonance also spans different attitudes, such as sharing a negative view of companies. For example, one user, who fell into the devotion category, did not *"trust Google, Apple, or the NSA with my [their] naked pictures."* Similarly, another user, who exhibited resignation, thought *"everything is controlled by the megacorps of modern society"* (U11-T137, U3-T137).

Opposing attitudes create social pressure. There is a sense of social pressure created when users of different attitudes interact. Users with dismissive attitudes may view those who worry about WiFi thermostats as being *"paranoid"* (U15-T136). In another case, two users reinforced their stance on surveillance issues when discussing smart speaker deals.

> *"right?! anyone skeptical of government surveillance can GTFO my life!!"* (U8-T55)

On the opposite, when defending their view about spying activities from smart speakers, a user was passive-aggressive toward others who dismissed the concern by saying *"fill your house with internet-connected microphones"* (U12-T20).

Meanwhile, we observe self-censorship when some users stated their attitudes:

> *"Am I weird for thinking it's weird that someone would potentially have access to control many things in my home through that echo?"* (U1-T24)

Takeaway-RQ3. Compared to prior work that focused mainly on the topics and users' intent in online S&P discussions [48], [74], we show how attitudes and discussion patterns influence each other, supported by quantitative statistics in Figures 7 and 8. Facing complex smart home S&P topics, users with different attitudes spontaneously resolve the ambiguity of information, contributing to attitude development. However, this process remains challenging for users due to complex topics and social pressures from opposing attitudes in other circumstances. We also identify an information gap in online discussion. Users rarely refer to reputable and understandable information sources about S&P properties of smart home products during discussions. Also, while community moderators highlight informative comments about S&P, this effort seems ad-hoc, and they are unlikely to correct misinformation at scale.

7. Discussion

Based on our findings, we provide three sets of recommendations in addition to future work. First, smart home companies should consider transparency, flexibility, and accessibility in product designs and practices to account for users' multi-dimensional S&P considerations (Takeaway-RQ1). Second, stakeholders (companies, governments, and third parties) should provide S&P nudges to help users develop S&P attitudes by improving users' awareness of S&P risks and appropriate protective strategies (Takeaway-RQ2). Third, online communities should facilitate the access and exchange of smart home S&P-related information, possibly with automated information retrieval and moderation (Takeaway-RQ3).

7.0.1. Incorporating users' multi-dimensional S&P considerations into smart home designs. Our findings reveal that users face challenges, such as limited information and product support, when deciding on S&P protective strategies; the associated tradeoffs force users to pick either a less secure or a less usable deployment. To mediate the conflicts between users' S&P considerations and other functional needs, it is important for smart home designs to incorporate users' multi-dimensional considerations to help them assess S&P risks and the appropriate protective strategies. However, it can be challenging to incorporate users' multi-dimensional considerations due to the interplay of many contextual factors, users' lack of comprehensive understanding of S&P risks, and the diversity of use cases. Therefore, we recommend three product design and practice guidelines for smart home companies.

Companies should ***inform users about smart home operations and practices in a transparent and understandable manner***. Our findings indicate that users' incomplete views of stakeholders and products could result in bias and conflicts when they assess S&P concerns. When users are not sure *"how reputable [the companies] are,"* their privacy concerns may even conflict with a product's security settings; for example, one user hesitated to provide their WiFi password to a smart bulb app (U1-T74). Thus, we suggest that companies should first provide understandable information about their compliance with S&P standards and regulations. Then, companies should communicate with users transparently about S&P threats, e.g., how the company *"responds to zero days"* as well as how they enforce S&P protection institutionally (U3-T121) [33]. In addition, explaining the operation of smart home designs, e.g., how the device certification guarantees reliability or interoperability, could help users assess associated S&P concerns when developing tech-involved threat models.

Smart home companies should ***make S&P protective strategies available and flexible for products***. Our findings reveal that users may not adopt certain smart home products when S&P protective strategies are unavailable or inflexible to mitigate users' concerns. For example, the availability and flexibility could be achieved by making features that cause users' S&P concerns (e.g., becoming a part of a mesh network with neighbors) as opt-in rather than a default, as well as by allowing users to delete data after device abandonment (U7-T87). For more tech-savvy users, companies could provide customizable designs that include the exposure of *"nerd knobs"* or allow DIY and open-sourced software to support their more sophisticated needs to personalize protective strategies (U9-T1). Companies may also offer controls in smart homes that allow users to balance between their S&P needs and utility requirements [47], [61]. In addition, companies may reduce the perceived cost of protective strategies by improving usability, e.g., via an *"easy to use GUI"* (U5-T101).

Smart home designs should ***accommodate considerations of different users, e.g., tech-savvy vs. novice, for specific use cases***. Users' use cases vary, especially in device-sharing contexts, which may lead to different assessments of S&P risks and protective strategies even for the same smart home product. For instance, users demanded accessible S&P controls to *"only activate [smart speaker] for approved people"* or prevent sensitive conversations from being recorded when working from home (U6-T78, U1-T68). Furthermore, though many users in our dataset are tech-savvy, we recognize their awareness of the technical cost and desire to support less tech-savvy users. Thus, smart home designs could offer a collaborative framework to support the S&P need of less tech-savvy users. In response, companies could establish "tech caregiving," which provides a software interface for technically informed users to help others such as the elderly [43], [87].

7.0.2. Supporting smart home users' attitude development with S&P nudges. We find that users' S&P attitudes, manifested in the level of S&P concerns and incorporation of protective strategies, change depending on the context. Users demonstrate varying assessments of S&P risks, with prior experiences and preconceptions often overriding objective assessments. As such, they develop attitudes that do not always result in secure and privacy-preserving behaviors. Companies, governments, and third parties could provide S&P nudges – gentle interventions that direct users toward safer practices [3] – to help users' attitudes evolve toward preserving S&P.

Smart home products could ***nudge users' S&P attitudes with physical metaphors***. We observe that users leverage physical S&P metaphors, e.g., comparing an always-listening voice assistant to a person eavesdropping over a table, to rationalize their smart home S&P attitudes. This observation is logical given that users exhibit more developed S&P attitudes in the physical world [38], [51], [66]. As such, a physical metaphor can help inform users about S&P risks and better utilize protective strategies. For instance, the "privacy nutrition labels" take inspiration from food nutrition labels to provide understandable S&P information [26], [28], [29]. Another example by Teyssier et al. explored anthropomorphic smart home product designs that prompt privacy awareness through mimicking bystanders via a human-eye-liked camera [75]. Protective strategies that draw analogies from the physical world might also be more intuitive to users, such as physical webcam covers or voice assistant jammers [15].

Stakeholders, such as regulators and non-profits (e.g., Consumer Reports and Mozilla), could ***help deploy S&P nudges at scale through automated assessment of smart home products***. Deploying nudges at scale solely by companies could be challenging as we observe that users are disappointed by their lack of responsibility. Other entities that are potentially motivated to deploy respective nudges for users include the workplaces, as the prevalence of working-from-home may motivate them to inform their employees about smart home S&P concerns. Furthermore, third-party non-profits may leverage automated S&P assessment via natural language processing to audit smart home products based on their privacy policies and apps [35]. S&P nudges could include the assessment results and inform users about the S&P properties of diverse products, e.g., compliance with regulations.

7.0.3. Supporting smart home users in accessing and exchanging online S&P information. While users actively seek information and voluntarily provide advice in the online discussion, we find that they face several challenges in accessing and exchanging online information about smart home S&P. The various information types, e.g., news, reviews, and anecdotes, are complex in nature. Reputable and understandable information sources are not easily accessible to online users. Moreover, we identify that users' opposing attitudes add pressure and may amplify the difficulties in knowledge exchange. To address these challenges, we suggest that online communities improve information access potentially with the help of automation.

Discussion forums could ***highlight the access to credible S&P information and sources***. We find that forum moderators' efforts in highlighting S&P information seem adhoc, as some users had to repeat the same advice to others. There is also little S&P information at the time being on the `/r/homeautomation` wiki page [62], where smart home resources are more organized. Thus, we suggest moderators maintain an up-to-date section about S&P on the wiki page with other volunteers. Moreover, we observe only occasional references to credible third parties that provide accessible S&P assessments, such as Consumer Reports or Mozilla. As such, we suggest online forums, smart home companies, and credible third parties collaboratively maintain communication channels to bridge S&P information and users online. For example, companies may leverage these channels to share S&P information in time, such as patching notices. Companies and third parties may also leverage automated agents to share S&P information via online communities' APIs [50], [65].

Online communities and credible third parties could ***help mediate S&P discussion by detecting misinformation and moderation***. Our findings show that users sometimes perceive others' views of S&P information as conspiratorial. Online communities may moderate discussions to facilitate more peaceful conversations. Moderation may ease tension resulting from opposing attitudes and detect inappropriate content, e.g., hate speech. Further, automated agents that process natural language may help mediate S&P discussion and ease the burden on moderators and third parties [52].

7.0.4. Directions for future work. Our findings, along with our methodology and limitations, e.g., the demographic bias on Reddit, motivate our suggestions for future research on smart home users' dynamic attitudes and considerations. Our method to detect S&P-relevant discussions and codebook may contribute to future research.

We suggest that research should ***consider users' dynamic and context-dependent S&P attitudes from multiple domains***. Future studies should consider a richer representation of S&P attitudes beyond associating individuals with a static S&P attitude. Such studies may capture users' adoption journeys and contexts from multiple domains, such as other social media platforms (Twitter, etc.) [49], [55], customer reviews [89], and even non-S&P related comments. Moreover, researchers could look into the alignment of users' attitudes between smart homes with other digital and physical S&P domains.

Researchers should ***study users' attitudes longitudinally at a community level***. Our findings on users' evolving attitudes motivate future longitudinal research to investigate attitude development between discussion threads over time in online communities. From `/r/homeautomation`, we observe such evidence of attitude shifts in the S&P discussions over the past decade. For example, in a 7-year-old thread, one comment suspected the smart home market might not take off due to interoperability problems, and there were few S&P concerns *"if we can't even build the system"* (U3-T136). However, we now observe discussions of S&P concerns about specific brands and products. Longitudinal research could track users' attitudes at the community level, including the community's responses to certain major S&P "events." For example, the widespread publicity of the *"Mirai"* attack affected user attitudes toward smart cameras (U1-T104) [9].

Future work may ***investigate the underlying geopolitical and cultural influences on smart home users' S&P attitudes***. We notice other factors influencing users' S&P considerations and attitudes. For example, the common distrust in Chinese products possibly arises from national security and political perspectives. Prior research showed the influence of geopolitical and cultural factors on the adoption of digital products [22], [24], [45], e.g., Chinese consumers' transition to using mobile payment instead of physical "Red Packets" for transferring ceremonial money [69]. However, these influences are not fully revealed by users on `/r/homeautomation`, since some content, including racism, violates Reddit's content policy [63]. Therefore, researchers can potentially study these influences in conjunction with other platforms, e.g., social media in different countries. Furthermore, researchers could cross-compare different countries' attitudes toward each other, e.g., how Chinese users consider U.S. products and vice versa.

Another venue is to ***study the impact of different designs of online S&P discussion platforms or reviews on users' information access***. As users value information sources when considering smart home S&P, the question of how the sources' information presentation, interaction structures, and credibility may influence users' S&P considerations and discussions remains open. In addition, future work may couple smart home users' demographics and roles to online S&P information, including children and victims of intimate partner violence who have different intentions to access such information [76].

8. Conclusion

We analyze smart home users' S&P considerations and attitudes from a major Reddit forum, `/r/homeautomation`. Through our analysis of 180 threads, we discover that smart home users develop multi-dimensional considerations regarding the interplay of contextual factors. Users' S&P attitudes are shaped and further evolve with these considerations. We also study the influence of online discourse–users exchange knowledge and develop attitudes collectively. Accordingly, we propose recommendations to support users' S&P considerations, attitude development, information exchange, and future research to study users' S&P attitudes from multiple angles.

Acknowledgment

We thank our reviewers for their valuable comments. This work is supported in part by NSF under grants 1845469, 1942014, 2003129, and 2112562.

References

[1] N. Abdi, K. M Ramokapane, and J. M. Such. More than smart speakers: Security and privacy perceptions of smart home personal assistants. In *SOUPS*, 2019.

[2] A. Acquisti. Privacy in electronic commerce and the economics of immediate gratification. In *ACM EC*, 2004.

[3] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, et al. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM CSUR*, 50(3):1–41, 2017.

[4] A. Acquisti, L. Brandimarte, and G. Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015.

[5] A. Acquisti, L. Brandimarte, and G. Loewenstein. Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, 30(4):736–758, 2020.

[6] A. Acquisti and R. Gross. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *PETS*, 2006.

[7] T. Ammari, J. Kaye, J. Y. Tsai, and F. Bentley. Music, search, and IoT: How people (really) use voice assistants. *ACM TOCHI*, 26(3):17–1, 2019.

[8] J. Angulo, E. Wästlund, and J. Högberg. What would it take for you to tell your secrets to a cloud? In *NordSec*, 2014.

[9] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, et al. Understanding the Mirai botnet. In *USENIX Security*, 2017.

[10] S. Barth and M. D. T. De Jong. The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online behavior–a systematic literature review. *Telematics and Informatics*, 34(7):1038–1058, 2017.

[11] J. Baumgartner. Pushshift's update on removal requests. https://twitter.com/jasonbaumgartne/status/1431845831984943104?s=21, 2021.

[12] J. Baumgartner, S. Zannettou, B. Keegan, M. Squire, and J. Blackburn. The Pushshift Reddit dataset. In *ICWSM*, 2020.

[13] R. Bellini, E. Tseng, N. McDonald, R. Greenstadt, D. McCoy, T. Ristenpart, and N. Dell. "So-called privacy breeds evil" narrative justifications for intimate partner surveillance in online forums. *PACM HCI*, 4(CSCW3):1–27, 2021.

[14] G. Chalhoub, M. J. Kraemer, N. Nthala, and I. Flechais. "It did not give me an option to decline": A longitudinal analysis of the user experience of security and privacy in smart home products. In *ACM CHI*, 2021.

[15] V. Chandrasekaran, S. Banerjee, B. Mutlu, and K. Fawaz. PowerCut and obfuscator: An exploration of the design space for privacy-preserving interventions for smart speakers. In *SOUPS*, 2021.

[16] E. K. Choe, S. Consolvo, J. Jung, B. Harrison, and J. A. Kientz. Living in a glass house: A survey of private moments in the home. In *ACM UbiComp*, 2011.

[17] E. K. Choe, S. Consolvo, J. Jung, B. Harrison, S. N. Patel, and J. A. Kientz. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *ACM UbiComp*, 2012.

[18] D. Choi, J. Han, T. Chung, Y. Y. Ahn, B. G. Chun, and T. T. Kwon. Characterizing conversation patterns in Reddit: From the perspectives of content properties and user participation behaviors. In *ACM COSN*, 2015.

[19] J. Clawson, J. A. Pater, A. D. Miller, E. D. Mynatt, and L. Mamykina. No longer wearing: Investigating the abandonment of personal health-tracking technologies on Craigslist. In *ACM UbiComp*, 2015.

[20] C. Cobb, S. Bhagavatula, K. A. Garrett, A. Hoffman, V. Rao, and L. Bauer. "I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. In *PETS*, 2021.

[21] Nora A. D. and Joseph T. The corporate cultivation of digital resignation. *New Media & Society*, 21(8):1824–1839, 2019.

[22] A. Daffalla, L. Simko, T. Kohno, and A. G. Bardas. Defensive technology use by political activists during the Sudanese revolution. In *IEEE S&P*, 2021.

[23] S. Das, L. A. Dabbish, and J. I. Hong. A typology of perceived triggers for end-user security and privacy behaviors. In *SOUPS*, 2019.

[24] P. Dourish and K. Anderson. Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-Computer Interaction*, 21(3):319–342, 2006.

[25] J. L. Dupree, R. Devries, D. M. Berry, and E. Lank. Privacy personas: Clustering users via attitudes and behaviors toward security practices. In *ACM CHI*, 2016.

[26] P. Emami-Naeini, Y. Agarwal, L. F. Cranor, and H. Hibshi. Ask the experts: What should be on an IoT privacy and security label? In *IEEE S&P*, 2020.

[27] P. Emami-Naeini, M. Degeling, L. Bauer, R. Chow, L. F. Cranor, M. R. Haghighat, and H. Patterson. The influence of friends and experts on privacy decision making in IoT scenarios. *PACM HCI*, 2(CSCW):1–26, 2018.

[28] P. Emami-Naeini, J. Dheenadhayalan, Y. Agarwal, and L. Faith. Cranor. Which privacy and security attributes most impact consumers' risk perception and willingness to purchase IoT devices? In *IEEE S&P*, 2021.

[29] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor. Exploring how privacy and security factor into IoT device purchase behavior. In *ACM CHI*, 2019.

[30] C. Flender and G. Müller. Type indeterminacy in privacy decisions: The privacy paradox revisited. In *QI*, 2012.

[31] R. Garg and S. Sengupta. He is just like me: A study of the long-term use of smart speakers by parents and children. *ACM IMWUT*, 4(1):1–24, 2020.

[32] C. Geeng and F. Roesner. Who's in control? Interactions in multi-user smart homes. In *ACM CHI*, 2019.

[33] J. M. Haney, Y. Acar, and S. M. Furman. "It's the company, the government, you and I": User perceptions of responsibility for smart home privacy and security. In *USENIX Security*, 2021.

[34] J. M. Haney, S. M. Furman, and Y. Acar. User perceptions of smart home privacy and security. *NIST Interagency/Internal Report*, 2020.

[35] H. Harkous, K. Fawaz, R. Lebret, F. Schaub, K. G. Shin, and K. Aberer. Polisis: Automated analysis and presentation of privacy policies using deep learning. In *USENIX Security*, 2018.

[36] P. He, X. Liu, J. Gao, and W. Chen. DeBERTa: Decoding-enhanced BERT with disentangled attention. In *ICLR*, 2020.

[37] W. He, M. Golla, R. Padhi, J. Ofek, M. Dürmuth, E. Fernandes, and B. Ur. Rethinking access control and authentication for the home Internet of Things (IoT). In *USENIX Security*, 2018.

[38] J. Holvast. History of privacy. *The History of Information Security*, pages 737–769, 2007.

[39] Y. Huang, B. Obada-Obieh, and K. Beznosov. Amazon vs. my brother: How users of shared smart speakers perceive and cope with privacy risks. In *ACM CHI*, 2020.

[40] A. N. Joinson, U. D. Reips, T. Buchanan, and C. B. P. Schofield. Privacy, trust, and self-disclosure online. *Human-Computer Interaction*, 25(1):1–24, 2010.

[41] E. Karapanos, J. Zimmerman, J. Forlizzi, and J. B. Martens. User experience over time: An initial framework. In *ACM CHI*, 2009.

[42] V. Koshy, J. S. Park, T. C. Cheng, and K. Karahalios. "We just use what they give us": Understanding passenger user perspectives in smart homes. In *ACM CHI*, 2021.

[43] J. Kropczynski, R. Ghaiumy Anaraky, M. Akter, A. J. Godfrey, H. Lipford, and P. J. Wisniewski. Examining collaborative support for privacy and security in the broader context of tech caregiving. *PACM HCI*, 5(CSCW2):1–23, 2021.

[44] P. Kumaraguru and L. F. Cranor. *Privacy indexes: A survey of Westin's studies*. 2005.

[45] E. Lafontaine, A. Sabir, and A. Das. Understanding people's attitude and concerns towards adopting IoT devices. In *ACM CHI EA*, 2021.

[46] D. Lee, R. Larose, and N. Rifon. Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology*, 27(5):445–454, 2008.

[47] J. Li, A. R. Chowdhury, K. Fawaz, and Y. Kim. Kalεido: Real-time privacy control for eye-tracking systems. In *USENIX Security*, 2021.

[48] T. Li, E. Louie, L. Dabbish, and J. I. Hong. How developers talk about personal data and what it means for user privacy: A case study of a developer forum on Reddit. *PACM HCI*, 4(CSCW3):1–28, 2021.

[49] K. Logan. Why isn't everyone doing it? A comparison of antecedents to following brands on Twitter and Facebook. *Journal of Interactive Advertising*, 14(2):60–72, 2014.

[50] T. Lokot and N. Diakopoulos. News bots: Automating news and information dissemination on Twitter. *Digital Journalism*, 4(6):682–699, 2016.

[51] N. Malazizi, H. Alipour, and H. Olya. Risk perceptions of Airbnb hosts: Evidence from a Mediterranean island. *Sustainability*, 10(5):1349, 2018.

[52] S. Malmasi and M. Zampieri. Detecting hate speech in social media. In *RANLP*, 2017.

[53] P. Mayer, Y. Zou, F. Schaub, and A. J. Aviv. "Now I'm a bit angry:" Individuals' awareness, perception, and responses to data breaches that affected them. In *USENIX Security*, 2021.

[54] N. Meng, D. Keküllüoğlu, and K. Vaniea. Owning and sharing: Privacy perceptions of smart speaker users. *PACM HCI*, 5(CSCW1):1–29, 2021.

[55] S. Mukherjee and P. K. Bala. Detecting sarcasm in customer tweets: an NLP based approach. *Industrial Management & Data Systems*, 2017.

[56] P. Norman, H. Boer, E. R. Seydel, and B. Mullan. Protection motivation theory. *Predicting and Changing Health Behavior*, pages 70–106, 2015.

[57] S. Parkin, E. M. Redmiles, L. Coventry, and M. A. Sasse. Security when it is welcome: Exploring device purchase as an opportune moment for security behavior change. In *USEC*, 2019.

[58] N. Proferes, N. Jones, S. Gilbert, C. Fiesler, and M. Zimmer. Studying Reddit: A systematic overview of disciplines, approaches, methods, and ethics. *Social Media+ Society*, 7(2):20563051211019004, 2021.

[59] pushshift.io. https://pushshift.io/, 2022.

[60] P. Rajivan and J. Camp. Influence of privacy attitude and privacy cue framing on android app choices. In *SOUPS*, 2016.

[61] N. Raval, A. Machanavajjhala, and J. Pan. Olympus: Sensor privacy through utility aware obfuscation. In *PETS*, 2019.

[62] Reddit. /r/homeautomation wiki. https://www.reddit.com/r/HomeAutomation/wiki/index, 2021.

[63] Reddit. Reddit Content Policy. https://www.redditinc.com/policies/content-policy, 2022.

[64] Reddit. Subreddit Search. https://www.reddit.com/subreddits/search?q=smart+home, 2022.

[65] E. M. Redmiles, N. Warford, A. Jayanti, A. Koneru, S. Kross, M. Morales, R. Stevens, and M. L. Mazurek. A comprehensive quality evaluation of security and privacy advice on the web. In *USENIX Security*, 2020.

[66] P. M. Regan. Privacy as a common good in the digital world. *Information, Communication & Society*, 5(3):382–405, 2002.

[67] M. Saeed, S. Ali, J. Blackburn, E. De Cristofaro, S. Zannettou, and G. Stringhini. Trollmagnifier: Detecting state-sponsored troll accounts on Reddit. In *IEEE S&P*, 2022.

[68] B. Saunders, J. Sim, T. Kingstone, S. Baker, J. Waterfield, B. Bartlam, H. Burroughs, and C. Jinks. Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, 52(4):1893–1907, 2018.

[69] H. Shen, C. Faklaris, H. Jin, L. Dabbish, and J. I. Hong. 'I can't even buy apples if i don't use mobile pay?' When mobile payments become infrastructural in China. *PACM HCI*, 4(CSCW2):1–26, 2020.

[70] K. Sun, Y. Zou, J. Radesky, C. Brooks, and F. Schaub. Child safety in the smart home: Parents' perceptions, needs, and mitigation strategies. *PACM HCI*, 5(CSCW2):1–41, 2021.

[71] M. Tabassum, T. Kosinski, and H. R. Lipford. "I don't own the data": End user perceptions of smart home device data practices and risks. In *SOUPS*, 2019.

[72] M. Tahaei, A. Frik, and K. Vaniea. Privacy champions in software teams: Understanding their motivations, strategies, and challenges. In *ACM CHI*, 2021.

[73] M. Tahaei, T. Li, and K. Vaniea. Understanding privacy-related advice on Stack Overflow. *PETS*, 2022.

[74] M. Tahaei, K. Vaniea, and N. Saphra. Understanding privacy-related questions on Stack Overflow. In *ACM CHI*, 2020.

[75] M. Teyssier, M. Koelle, P. Strohmeier, B. Fruchard, and J. Steimle. Eyecam: Revealing relations between humans and sensing devices through an anthropomorphic webcam. In *ACM CHI*, 2021.

[76] E. Tseng, R. Bellini, N. McDonald, M. Danos, R. Greenstadt, D. McCoy, N. Dell, and T. Ristenpart. The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums. In *USENIX Security*, 2020.

[77] D. Votipka, M. N. Punzalan, S. M. Rabin, Y. Tausczik, and M. L. Mazurek. An investigation of online reverse engineering community discussions in the context of ghidra. In *IEEE EuroS&P*, 2021.

[78] H. Watson, E. Moju-Igbene, A. Kumari, and S. Das. "We hold each other accountable": Unpacking how social groups approach cybersecurity and privacy together. In *ACM CHI*, 2020.

[79] J. Watson, H. R. Lipford, and A. Besmer. Mapping user preference to privacy default settings. *ACM TOCHI*, 22(6):1–20, 2015.

[80] J. B. Whiting, R. D. Olufuwote, J. D. Cravens-Pickens, and A. Banford Witting. Online blaming and intimate partner violence: A content analysis of social media comments. *The Qualitative Report*, 2019.

[81] A. Whitten and J. D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *USENIX Security*, 1999.

[82] F. Wolf, R. Kuber, and A. J. Aviv. "Pretty close to a must-have:" Balancing usability desire and security concern in biometric adoption. In *ACM CHI*, 2019.

[83] A. Woodruff, V. Pihur, S. Consolvo, L. Brandimarte, and A. Acquisti. Would a privacy fundamentalist sell their DNA for $1000... if nothing bad happened as a result? the Westin categories, behavioral intentions, and consequences. In *SOUPS*, 2014.

[84] W. Xie, A. Fowler-Dawson, and A. Tvauri. Revealing the relationship between rational fatalism and the online privacy paradox. *Behaviour & Information Technology*, 38(7):742–759, 2019.

[85] E. Zeng, S. Mare, and F. Roesner. End user security and privacy concerns with smart homes. In *SOUPS*, 2017.

[86] E. Zeng and F. Roesner. Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. In *USENIX Security*, 2019.

[87] J. C. Zhao, R. C. Davis, P. S. Foong, and S. Zhao. Cofaçade: A customizable assistive approach for elders and their helpers. In *ACM CHI*, 2015.

[88] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster. User perceptions of smart home IoT privacy. *PACM HCI*, 2(CSCW):1–20, 2018.

[89] J. J. Zhu, Y. C. Chang, C. H. Ku, S. Y. Li, and C. J. Chen. Online critical review classification in response strategy and service provider rating: Algorithms from heuristic processing, sentiment analysis to deep learning. *Journal of Business Research*, 129:860–877, 2021.

[90] V. Zimmermann, M. Bennighof, M. Edel, O. Hofmann, J. Jung, and M. von Wick. 'Home, smart home'–Exploring end users' mental models of smart homes. In *Mensch und Computer*, 2018.

A. Appendix

TABLE 1. Comparison of smart home-related subreddits suggested by Reddit's engine. We show the top 10 subreddits ranked by their subscribers as of March 2022. /r/homeautomation is the most appropriate, because it has the largest user base and covers diverse products and integration levels. Note that while smart home S&P may also be discussed on other subreddits, we were interested in how S&P topics emerge organically from smart home-focused discussions. And we decided to focus on subreddits that center around smart home topics (e.g., product information and adoption considerations).

Subreddit	Subscribers	Appropriate?	Explanation
r/homeautomation	**1,622,028**	Yes	
r/googlehome	587,788	No	Brand-specific
r/hue	227,287	No	Brand-specific
r/homenetworking	223,605	Yes	
r/homeassistant	166,711	No	Brand-specific
r/iota	146,161	No	Brand-specific
r/smarthome	133,135	Yes	
r/ubiquiti	124,902	No	Brand-specific
r/amazonecho	124,089	No	Brand-specific
r/homekit	119,568	No	Brand-specific

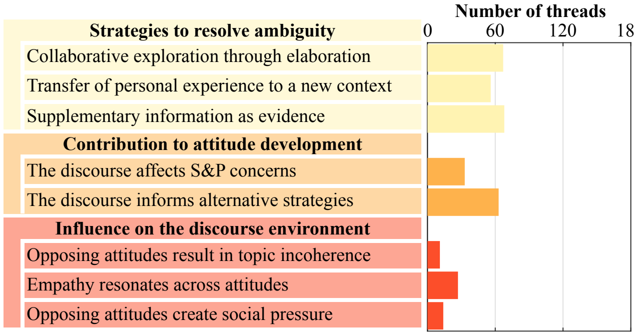

Figure 7. Three themes and the frequencies of eight subthemes of the online discourse's influences.

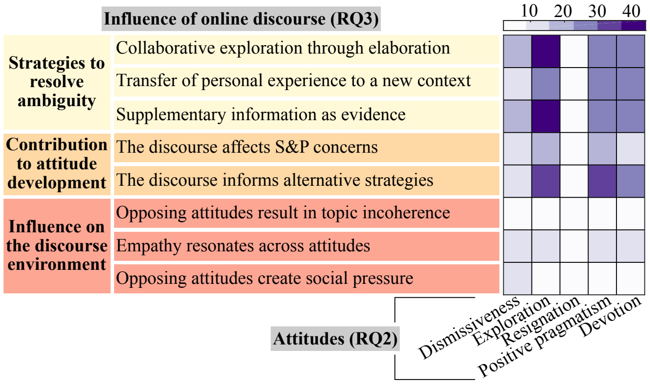

Figure 8. Co-occurrence of users' S&P attitudes with the subthemes in discourse influences per thread. The statistics highlight the participation of users carrying exploration, positive pragmatism, and devotion in resolving ambiguities for S&P-related discussion and their active contribution to attitude development, e.g., informing alternative strategies. In contrast to prior findings that S&P fundamentalists are reluctant to help [25], we observe users of high technical competence (devotion) proactively support others.