Mahsa Saeidi*, McKenzie Calvert, Audrey W. Au, Anita Sarma, and Rakesh B. Bobba

If This *Context* Then That *Concern*: Exploring users' concerns with IFTTT applets

Abstract: End users are increasingly using trigger-action platforms like *If-This-Then-That* (IFTTT) to create applets to connect smart-home devices and services. However, there are inherent implicit risks in using such applets—even non-malicious ones—as sensitive information may leak through their use in certain contexts (*e.g.,* where the device is located, who can observe the resultant action). This work aims to understand to what extent end users can assess this implicit risk. More importantly we explore whether usage context makes a difference in end-users' perception of such risks. Our work complements prior work that has identified the impact of usage context on expert evaluation of risks in IFTTT by focusing the impact of usage context on end-users' risk perception. Through a Mechanical Turk survey of 386 participants on 49 smart-home IFTTT applets, we found that participants have a nuanced view of contextual factors and that different values for contextual factors impact end-users' risk perception differently. Further, our findings show that nudging the participants to think about different usage contexts led them to think deeper about the associated risks and raise their concern scores.

Keywords: Privacy, IoT, Smart home, IFTTT applets, Contextual factors

DOI 10.2478/popets-2022-0009
Received 2021-05-31; revised 2021-09-15; accepted 2021-09-16.

1 Introduction

Many homes are being out-fitted with Internet connected sensors and devices to create interactive and adaptive smart living spaces with a promise of convenience, safety, security, and energy efficiency. Programming platforms and frameworks such as IFTTT [1], OpenHAB [19], and Microsoft Flow [4] enable end users to compose different smart devices and services to make it easy for them to monitor and control their smart-home environments. Frameworks like IFTTT use very simple trigger-action formats–*"if trigger then action"*–to enable new and rich functionality. For example, consider a simple applet that allows end users to control their smart camera via voice assistants such as Alexa; users can then voice activate their (hidden) nanny camera before going to work. "Regular end users" can now buy inexpensive off-the-shelf devices from different vendors and then connect them using frameworks like IFTTT. Because of this ease of creating "applets" that can connect devices from different vendors, and the proliferation of connected devices, *millions use these services*; some simply reusing already created applets, others creating their own. For IFTTT alone, there are *18 million registered users, running over 1 billion IFTTT applets (originally called recipes) each month in* 2020 [20].

While these platforms are easy to use and allow new functionalities, composing different services or connecting devices to services can lead to unexpected or undesirable behavior [8], especially if not deployed thoughtfully. For instance, in our example, a babysitter may simply turn off the nanny camera with a voice command to Alexa (since Alexa doesn't use any kind of filtering through voice recognition) without the user's knowledge (unauthorized modification). In this case, the voice assistant was in an accessible location and had no authentication capability undermining safety for the baby.

As another example, consider an applet that connects a smart camera to an online photo-storage service by taking and logging a picture when the camera detects motion. While this is a useful applet that can be used for home monitoring while one is away, deploying this applet can have severe privacy consequences depending on where the camera is located (*e.g.,* living room vs. bedroom), when it is active (*e.g.,* during working hours vs. all day), and who else has access to the online photo storage (*e.g.,* private folder vs. shared folder).

***Corresponding Author: Mahsa Saeidi:** Affil, E-mail: saeidim@oregonstate.edu
McKenzie Calvert: Affil, E-mail: calvertm@oregonstate.edu
Audrey W. Au: Affil, E-mail: auau@oregonstate.edu
Anita Sarma: Affil, E-mail: sarmaa@oregonstate.edu
Rakesh B. Bobba: Affil, E-mail: rakesh.bobba@oregonstate.edu

Given the popularity of IFTTT applets and the potential risks associated with deploying them, we wanted to see if and to what extent people think about these risks when considering an applet. This brings us to: *RQ1: How concerned are users about using IFTTT applets?* Especially, when given a simple description of the applet that explicitly identifies the applet *trigger* and *action*.

Further, the risks associated with an applet can be context dependent. For instance, in the home monitoring example above, logging smart camera pictures into a shared folder poses privacy risks, but the risk can be significantly different depending on the camera's location. If the camera is on the front porch, a more-or-less public location it is less of a concern as opposed to it being in the living room or other more private areas in the home. Time of the day matters too, pictures taken during the daytime may be less sensitive than those of individuals in their night attire (in the privacy of their home). This highlights the fact that the context of use can impact the risk of using such applets, and thus, a more nuanced view of context may help to identify these risks better. While Cobb *et al.* [11] have shown that security experts recognize the importance of context when assessing risks, it was not clear whether usage context mattered to end users for risk assessment. Therefore, we wanted to see if and how contextual factors influence users' concerns bringing us to: *RQ2: To what extent do contextual factors impact end-users' concerns?*

Given that millions of end users are downloading and using IFTTT applets, a deeper understanding of end-users' concerns, especially to what extent the usage context impacts these concerns, is necessary for the success of approaches to help users understand or mitigate the risks associated with IFTTT applets. For instance, without considering the context of use, current efforts that automatically identify potential risks with applets by tracking the flow of information from (public or private) sources to sinks (*e.g.,* [3, 36]) may be inadequate. While more finer grained security labels for automated information flow analysis have been adopted by Cobb *et al.* [11], they recognized that more contextual information is necessary.

While previous research in traditional mobile applications (*e.g.,* [27, 34]) or in sharing of online content (*e.g.,* [17]) has investigated the impact of context, their findings are not directly applicable to smart-home applets. This is because the interaction between physical environment and (multiple) sensors and devices in a smart-home environment leads to a unique, more nuanced, and richer context than previously considered.

To close this gap in our understanding of users' concerns with IFTTT applets and how those concerns are impacted by context we conducted an online Mechanical Turk based survey with 386 participants, who in total answered questions about 49 popular IFTTT applets. The survey first asked participants whether they had any concerns about using an applet by presenting them with a simple description (RQ1). It then prompts participants to think about specific contextual factors relevant to that applet (RQ2) through a subsequent set of questions.

Our findings indicate that nudging users to think about different usage contexts can help them better appreciate risks with applets and that contextual factors have a significant impact on users' concerns with using these applets. Further, in a majority of cases, participants were concerned because of security and privacy risks associated with the context of use of these applets.

2 Methodology

We conducted an online survey, approved by our Institutional Review Board (IRB), to explore users' concerns with IFTTT applets. In the survey, we first asked participants about their concerns with using an applet after reading a simple trigger-action description (without any potential contextual information in the original description). Next, the survey presented participants with a set of contextual factors and asked them about their concerns with using the applet for each context. We also collected demographic data including age, gender, education, and IoT/IFTTT related background.

2.1 Recruitment and participants

We recruited 386 participants through Amazon Mechanical Turk (MTurk). Participants had to be at least 18 years old, live in the United States, have an approval rate of 95% or greater, and have at least 100 HITs approved. We compensated participants $3.50, as our pilot study with 4 participants showed the survey took between 20 to 30 minutes. The MTurk participants took an average of 24 minutes to complete the survey. Of the 386 participants, 60% identified as men, 39% identified as women, and less than 1% from other categories. Majority of participants owned one to two IoT devices (65%) and used one to two IFTTT applets (61%). Majority of participants had some college education or higher

Table 1. Demographic of participants.

Gender		Age		Education		IFTTT applets		IoT devices	
Women	39%	18 – 24	10.4%	Less than high school	0.25%	0	22%	0	10.1%
Men	60%	25 – 34	60.1%	High school	11.9%	1-2	61%	1-2	65%
Non-binary	< 1%	35 – 44	21.5%	Some College	13%	3-4	11.14%	3-4	18.4%
Trans	< 1%	45 – 54	4.15%	2 year degree	10.4%	5+	6.74%	5+	6.48%
		55 – 65	3.37%	4 year degree	51.8%				
		65+	0.51%	Professional degree	11.9%				
				Doctorate	0.77%				

(88%). Table 1 captures demographics of the participants.

2.2 Study design

Applet selection. The focus of our paper is to investigate users' concerns with the applets that have context of use within the home environment. So, we selected popular applets where at least one of the action or trigger services occurred in the home or served house members. Therefore, we picked the 50 most frequently used applets from smart-home relevant categories from the IFTTT dataset published by Ur *et al.* [40]. The categories we used were "appliances", "lighting", "environment control & monitoring", "security & monitoring systems", "location", "smart hubs & systems", and "voice assistants". This gave us a total of 350 applets.

We reviewed all applets' descriptions and removed the following types of applets: (1) duplicates, (2) those that did not have clear descriptions, (3) those that involved services that are now uncommon (*e.g.,* Ubi), (4) those that were not related to smart homes (*e.g.,* News applets), and (5) those that were IFTTT specific services, such as sending notification to IFTTT e-mail. After this filtering stage we had 90 applets. Next, two researchers discussed each applet to identify if there were potential security and privacy risks for each applet. As our goal was to understand end-users' concerns in using potentially risky applets we filtered out those applets for which the researchers could not come up with potential risks. This resulted in a final dataset of 49 applets that are smart-home related applets and at the time of study deployment, the majority of them (47 out of 49) were still highly popular within their categories[1]. Table 2 shows the distribution of selected applets with each of seven applet categories.

Finally, we converted all applet descriptions to a standardized format that explicitly stated the triggers and actions. We did this because in some cases the descriptions in the dataset were confusing or had very little description of the trigger or action. For instance, for the applet that blinks the Hue light when the user receives a new SMS (Applet#20), the IFTTT description was: *"Never miss an important text on your Android phone with this Applet."* The standardized format helped us direct participants to think about the trigger-action rules and collect their concerns about the applets rather than about the IoT devices.

Table 2. Distribution of selected applets across selected IFTTT categories. The sum is more than 49 since the categories were not mutually exclusive.

Applet category	#Applets
Appliances	10
Lighting	10
Environment control & monitoring	5
Security & monitoring systems	11
Location	10
Smart hubs & systems	2
Voice assistants	13

Context description. We selected those contextual factors that are related to home environments. We included "location" as a factor as it has been found to be relevant in prior work (*e.g.,* [18, 25, 26, 29]). We considered both the location of the *triggering* IoT device and the location of the resultant *action*. Since IFTTT applets that connect IoT devices to online services are an important class, we explicitly considered their action location, *i.e.,* action in online services as a separate contextual factor. Further, we analyzed the situations in which integrity and confidentiality violations might occur [36]. This led us to consider *who is involved* in triggering and *who is observing* applets as contextual factors. Finally, we considered the "time of the day" as it can lead to different security and privacy implica-

1 The list of applets' descriptions are provided in the Appendix.

tions. We now discuss briefly the list of values for each contextual factor in our study:

- **Trigger Location** considers the area in the home where the IoT device is located (trigger events occur). We considered public areas as places that are accessible to outsiders (*e.g.,* front entrance areas), semi-private areas as those that are accessible to visitors and homeowners (*e.g.,* living room and kitchen), and private areas as those where access to them is largely limited to homeowners (*e.g.,* bedroom and bathroom).
- **Action Location** considers the area in the home where the IoT device or service that acts as an action service is located. It included public areas such as, front entrance areas, semi-private areas such as, living room and kitchen, and private areas such as, bedroom and bathroom.
- **Action in Online Services** includes situations where the applet's action is reported/logged in online services (*e.g.,* a Facebook post when the user arrives home). It captures concerns where the information through online services is accessible to (or shared with) others. For example, if the Facebook post is on a public page there might be privacy concerns.
- **Who Can Use** considers who is able to use or trigger the applet. It primarily considers the different groups of people based on their relationship to the homeowner, and included: spouse, kids, visitors, and outsiders (anyone outside of the house).
- **Who is Around (can observe)** considers who is nearby and can observe the applet action. This factor included people based on their relationship to the homeowner: spouse, kids, visitors, and outsiders.
- **Time** of the day that an end user uses the applet included factor values: morning, afternoon, and night.

Survey design. We designed seven surveys (7 MTurk HITS), with two sections each. The first section, common across all the surveys, covered demographic questions. We collected demographic information of participants including age, gender, education, number of IoT devices they own (or had owned), and the number of IFTTT applets they use (or had used). The second section covered applet-specific questions with each survey (HIT) covering seven unique applets out of the 49 (7 surveys x 7 applets). We used stratified random selection to populate seven different surveys with applets from different applet categories (Table 2). The demographic questions and the questions for one applet are shown in the Appendix. Each survey was released in MTurk sequentially and each participant could have responded to only one survey (HIT).

Users' concerns with applets from applet descriptions (RQ1). For each applet, we asked participants to rate their concerns through a direct question: "Would you be concerned about using this applet?" The answer choices were on a Likert scale ranging from *Not at all concerned* (1) to *Extremely concerned* (5). We used the more generic word "concern" to avoid priming participants. Preibusch [31] recommends treating privacy concern as a latent variable and not explicitly asking users about it. Of course, users are still prompted to think critically about the applets' use. Our results (See Section 3) show that despite having this critical eye, users failed to notice potential risks from reading the applet descriptions.

Impact of contextual factors on users' concerns (RQ2). Then we presented participants with the context questions to find which contextual factors might influence users' concerns with using the applets. Specifically, we asked participants to rate their concerns with using each applet under the six previously discussed contextual factors. Similar to the previous question, participants had to choose from among the five options on a Likert scale ranging from *Not at all concerned* (1) to *Extremely concerned* (5). If participants' responses were at level 3 (*Somewhat concerned*) or above, then we asked participants to provide an explanation of their choice via open-ended questions. We used participants' responses to these open-ended questions to understand if and how their concerns changed after considering contextual factors, and how their concerns differed across different contextual factors for each applet. These responses also gave us confidence that participants were reacting to the applets rather than individual IoT devices connected by the applets. In the rest of the paper, we refer to these responses as "open-ended responses."

2.3 Study limitations

First, accurately capturing participants' concerns with the IFTTT applets in a study setting is not easy. One limitation can be caused by "privacy paradox" where participants differ in their self reports of privacy preferences and their privacy behavior [30]. Since in our survey participants self reported their concerns, their responses may not match their behavior if they were to use the applets. Further, we asked participants to imagine using a particular applet in a particular usage context (*e.g.,* using Alexa to turn on the light when Alexa is placed

in the kitchen). While we have selected real IFTTT applets that are popular in their categories, participants may have been asked about applets or usage contexts that they do not experience, impacting their responses.

Second, our dataset included 49 applets across 7 categories relevant to smart homes. This is but a small set in the universe of IFTTT applets and our findings might not generalize to all IFTTT applets. Additionally, our assumptions about the usage context of specific smart-home devices may have caused us to miss some usage situations. For instance, we did not consider the front door area as a location for Alexa, and only considered kitchen as a location for an oven. These assumptions may not always be valid. For example, an oven maybe in the living room in a studio apartment. In this regard, our findings may not generalize to all usage contexts.

Finally, a majority of our participants were educated (4 year degree 51.8%) and young ($25-34, 60.1\%$), a common demographic of MTurk workers. While a past study [23] had found that MTurk workers were not representative of US population, a more recent (2019) study [33] has shown that MTurk workers are more representative of the U.S. population to study privacy attitudes when compared to Telephone-based or Web-based samples.

2.4 Data analysis

We report our findings based on both quantitative and qualitative analysis. To verify the quality of collected data, we considered i) survey time and ii) the quality of the responses to open-ended questions. In our sandboxing (pre-pilot study), the minimum time to complete the survey by security experts was about 10 minutes. The minimum time spent by participants on the survey (8 min) was not much lower than the minimum time in sand-boxing (10 min), so instead of filtering participants simply based on time, we also reviewed their qualitative responses to open-ended questions. Overall, we excluded responses from 33 participants whose open-ended responses were suspect. For example, we excluded participants who simply copied and pasted the applet definition from the Internet in response to such questions. We did so since this signaled that these participants may not have filled out the survey correctly. This left us with 353 participant responses which we considered further for our quantitative and qualitative analyses.

For quantitative analysis, we converted all categorical Likert scale variables to numerical variables. We used descriptive statistics (*e.g.,* frequencies, means) and statistical analysis for comparisons. For statistical comparisons, since the measured concern level is ordinal in nature, we used a cumulative link mixed model (CLMM) with the random intercepts per participant and per applet to account for within-user data dependencies [39]. To investigate if a contextual factor (independent variable) was a significant factor in participants' concerns, we created two regression models for each contextual factor: (i) the *null model* without any contextual factor as a fixed effect and (ii) the model with a contextual factor as a fixed effect (called *[contextual factor]-model*). Then, we used the Likelihood Ratio Test (LRT) to test the difference between the likelihood of these two models. If the result was significant, then we can conclude that the contextual factor was significant in participants' concerns. If found significant, we next investigated how the different values of the contextual factor (*e.g.,* public, semi-private, private values in Trigger Location) played a role. We ran pair-wise comparisons across these values through post-hoc tests using *lsmeans* function, which uses Tukey to account for multiple comparisons. Similarly, we employed regression analysis with the random intercepts per participant and per applet to investigate the impact of demographics and IFTTT/IoT background on participants' concerns. We used a significance level of $\alpha = 0.05$. All analyses were implemented using the statistical software package R [32]. We used ordinal package to perform CLMM.

Since each survey (MTurk HIT) was static encompassing 7 pre-selected applets per HIT, we re-ran all regression analysis by using "Survey #" as a factor in these tests to investigate if framing effect had an impact on our findings. We found that the survey# did not have a significant impact (See Section 4.1.1). Similarly, to check if there was a potential learning effect based on the order in which participants saw the applets, we analyzed whether the applet order had an impact. We used LRT to compare an ordinal regression model with 'order' as an independent variable with a null model (without 'order' as a variable) and found that the order did not have a significant impact (See Section 3).

For qualitative analysis of the reasons behind participants' concerns, we performed inductive coding of the open-ended responses. We coded 4009 valid responses. For each contextual factor, the lead author performed open coding on a small subset of the responses (5% of responses chosen in random order) to create an initial codebook. Two researchers then used the codebook to independently code the responses, and discussed and updated the codebook as needed. Once the codebook was stabilized and the researchers attained a high inter-

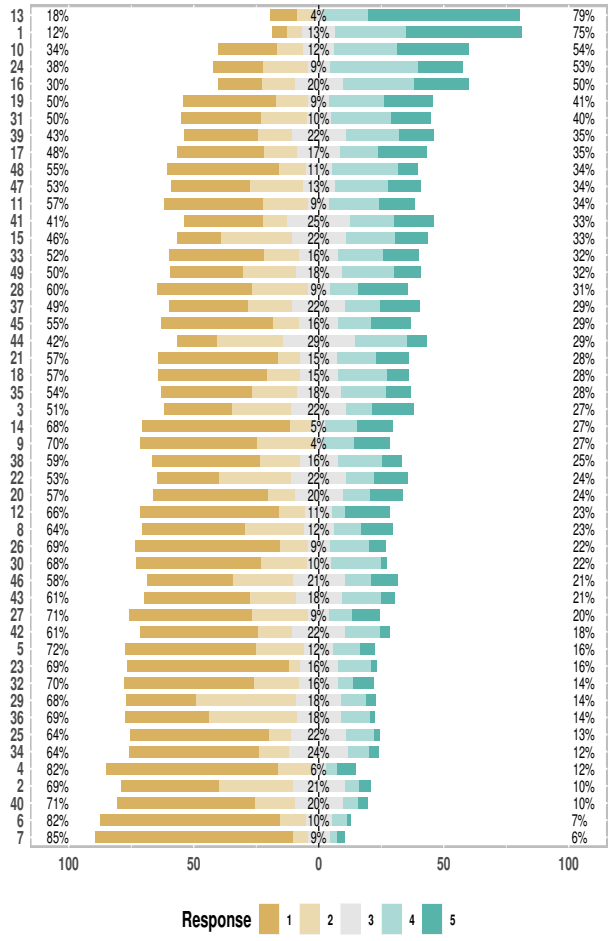

Fig. 1. Participants' concern scores after reading each applet description, sorted by percent of participants expressing Extreme or Moderate concern (1: Not at all concerned, 2: Slightly concerned, 3: Somewhat concerned, 4: Moderately concerned, 5: Extremely concerned).

rater reliability (Cohen's κ [16]) in 20% of the responses (Trigger Location: Cohen's $\kappa = 0.85$, Action Location: Cohen's $\kappa = 0.93$, Action in Online Service: Cohen's $\kappa = 0.9$, Time: Cohen's $\kappa = 0.9$, Who Can Use: Cohen's $\kappa = 0.86$, Who is Around: Cohen's $\kappa = 1$), the second researcher independently coded the rest of the responses.

3 Users' concerns with applets (RQ1)

The goal of our first research question is to create a baseline understanding of whether users have any concerns in using applets after reading their descriptions.

Table 3. Distribution of participants' concern score, after reading applet descriptions across all applets (1:Not at all concerned, 2:Slightly concerned, 3:Somewhat concerned, 4:Moderately concerned, 5:Extremely concerned.) Not at all concerned was the most frequently selected (40.8%) and Extremely concerned was the least selected (12.9%).

Concern level	1	2	3	4	5
Percentage of responses	40.8%	16.5%	14.9%	14.7%	12.9%

This baseline allows us to gauge to what extent participants understand the consequences of using the applet when provided with a simple applet description that explicitly stated the trigger and action.

In general, participants were not overly concerned about using the applets after reading their description. *Not at all concerned* was the most frequently selected (40.8%) and *Extremely concerned* was the least selected choice (12.9%), with the rest of the options more or less evenly split (around 15.5%) (See Table 3). The mean concern score was 2.42 out of 5 ($STDEV = 1.46$), which falls between *Slightly concerned* and *Somewhat concerned*. These concerns scores are despite the fact that all applets selected for the study had a potential privacy or security risk (See Section 2.2).

Figure 1 shows the distribution of participants' concerns for each applet in the study; arranged in a descending order of the percent of participants expressing *Moderate* or *Extreme* concern. There are a few applets (#13, #1, #10, #24, #16) for which the majority of responses fall between *Somewhat concerned* or *Extremely concerned*. It turns out that all these five applets connected a location service to an online service. For example, Applet #13 connected a user's location with Facebook by posting a status update whenever the user entered a specified area. Similarly, Applet #1 connected a user's location with Twitter by posting a tweet whenever the user entered a specified location.

Further, 7 of the 8 applets in our dataset that explicitly connect a user's location to an online service (#1, #10, #13, #16, #19, #24, #41) show up in the top 15 in Figure 1. The mean of concern scores for these 8 applets (mean = 3.26, STDEV = 1.51) is higher when compared to the rest of the applets (mean = 2.24, STDEV = 1.38) indicating that participants were concerned about their location privacy.

Although participants were concerned about leaking their location data to online services, they were less concerned when such a leak could occur indirectly. For example, participants did not seem overly concerned about using applets that connected thermostats (#30, #46) or

light switches (#2, #12) to online services, which might indirectly leak participants' location or their presence at home. A case in point is Applet #30, which sends an email whenever the thermostat is set to "away". If someone gains access to the email logs they can infer when the participants were at home (or away). The majority of responses (68%) for Applet #30 show that participants were only *Slightly* or *Not at all concerned*. This lack of concern for indirect leakages is reflected by low concern scores for Applet #6, which logs motions detected by a camera in an online service; and Applets that connects Alexa to a device in a home (#7); or to an online service (#40) (bottom of Figure 1). We posit that this might be because the applet descriptions were insufficient in allowing participants to adequately assess the consequences of using such trigger-action applets.

To understand if and how much demographic factors (gender, age and education level), prior IoT device and prior IFTTT applet experience influenced users' concern scores, we used regression analysis with the random intercepts per participants and per applet and found that concern scores were statistically significantly related to: *age* ($\chi^2(df = 5) = 26.29, p = 7.28e - 05$), *education level* ($\chi^2(df = 3) = 13.56, p = 0.003$), and *IFTTT experience* ($\chi^2(df = 3) = 17.8, p = 0.0004$). Gender and IoT background were not found to be significant factors.

When considering *age* and *education*, pair-wise comparisons did not give us any clear significant result about trends in concern score. When considering *IFTTT experience*, we could only observe significant differences between participants with no IFTTT applet with those who had used 1-2 or 3-4 applets before. Participants with prior IFTTT experience were likely to be less concerned about using IFTTT applets compared to those with no experience ($p-value < 0.05$). This might reflect that participants who had low concerns about IFTTT applets were the ones who were using them.

To check if the order of the applets had an impact on our results, we ran a regression model with 'order' as an independent variable. The likelihood ratio test with two models, one with the order variable and one without, as inputs showed that the order did not have a significant impact ($\chi^2(df = 1) = 3.2923, p = 0.06$).

4 Impact of contextual factors on users' concerns (RQ2)

To understand the role of contextual factors, we directed participants' attention to the six contextual factors relevant to each of the 49 applets in our study. Our findings show that each and every participant—on thinking about specific context of use—*increased* their concern for at least one of the contextual factors. Figure 2 shows the average change in participants' level of concerns for each contextual factor and for each applet. To measure the change in level of concern, we considered the highest concern score across different values for each contextual factor. Then, we calculated the difference with baseline concern score after just reading the description. Finally we computed the average of the differences across all participants' responses for each applet.

As Figure 2 shows, on average, concerns increased with few exceptions. Further, Figure 2 shows that the increase in concerns was higher for some applets and contextual factors than others. To understand the details of how context impacted participants' concerns with using these applets, we conducted both qualitative and quantitative analysis.

4.1 How significant is impact of each contextual factor

We used regression analysis to investigate the impact of each contextual factor on participants' concerns with using the IFTTT applets. However, before running the regression models, for each contextual factor we removed the applets for which that contextual factor was not applicable. For instance, the contextual factor Trigger Location is not applicable for applets that activate based on the time of the day (Applet#32 turning Phillips Hue Light on or off at specific times).

Next, we report the findings from our statistical analysis for each contextual factor categorized into three broad classes—*location* of the trigger & action, the *time* of the day, and *access* to the trigger & action.

4.1.1 Location

The location of where the applet is triggered (Trigger Location), as well as where the action is recorded —in the home (Action Location) or online (Action in Online Services)—can have associated risks.

Trigger Location. To analyze the impact of different Trigger Locations on participants' concerns with using an applet, we categorized those applets were Trigger Location was relevant (33 out of 49 applets) into two groups: 1) applets whose locations can only be inside the house; for example, in an applet that connects Alexa

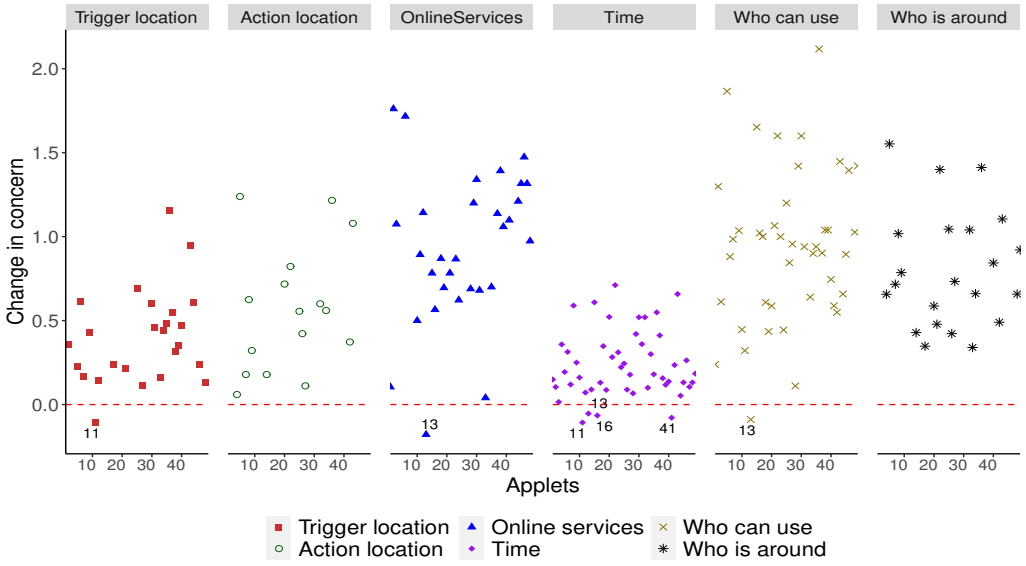

Fig. 2. Average of change in participants' concern when considering contextual factors. Change in level of concern score was calculated by taking the highest concern score across different values of each contextual factor (for each response). On average, concerns increased with few exceptions including, Applet #11, Applet #13, Applet #16, and Applet #41 for a few contextual factors.

to other IoT devices, Alexa is unlikely to be located at the front door, and 2) applets that can be located both inside and outside; for example, for an applet that connects a camera to online services, the camera can be located inside or outside the house. Then for applets in each category, we tested the effect of Trigger Location on participants' concerns by fitting two regression models: null model and TriggerLocation-model and using LRT to assess the differences between these two models (recall from Section 2.4). The Trigger Location impacted participants' concerns for applets in both categories (Significant differences for Category1: $\chi^2(df = 1) = 35.606, p < 0.001$ and for Category2: $\chi^2(df = 2) = 27.474, p < 0.05$).

In the first category, participants differentiated between private (bedroom, bathroom) and semi-private (kitchen, living room) locations ($p < 0.001$, See TriggerLocation-model-1 in Table 4). As expected, participants were less concerned about the semi-private locations as compared to private locations (negative coefficient in Table 4). In the second category, which included three types of locations (private, semi-private, public), we ran pair-wise comparisons using the *lsmeans* function to see if participants differentiated between these types of locations. Table 5 shows significant differences between all pairs of locations ($p < 0.05$)[2]. Recall that (See Section 2.4) we re-ran the regression analysis using "Survey #" as a factor to investigate the impact of framing effect on our results. The likelihood ratio test with these two models as inputs shows no significant differences between the two models ($\chi^2(df = 1) = 9.9e-09, p = 0.9$) indicating that survey # did not have an impact. We got similar results for the rest of the tests.

Action Location. As our goal was to compare differences in concerns across different locations that an action could be seen, we refined the subset of applets to those where the devices could be placed at different locations. This, therefore, excluded applets such as those that connect Alexa to the oven (Applet#17) or to the printer (Applet#7), since the oven can only be in the kitchen and the printer is unlikely to be at the front door. This resulted in a set of 9 applets that we investigate further.

The regression models and LRT results show that Action Location had a significant effect on participants' concerns ($\chi^2(df = 2) = 87.272, p < 0.001$). According to the regression result (ActionLocation-model in Table 4), participants were less concerned with the semi-private locations compared to private locations. Pair-wise comparisons also confirm this distinction and also show that there was a statistical difference in participants' concerns for semi-private locations (kitchen, living room), and front door area ($p < 0.05$, See Table 8 in the Appendix).

Action in Online Services. In applets where the action (outcome) of an applet is transmitted to an online service (*e.g.,* an email, a tweet, a Google calendar

2 The details of the pair-wise comparisons for the remaining contextual factors are in the Appendix.

Table 4. Summary statistics & regression results for contextual factor influence on participants' concerns. We used a separate regression model for each contextual factor. First factor in each model was considered a base (intercept) by CLMM.

TriggerLocation-Model-1(inside only) [1]					**Time-Model**				
	Coeff.	**Std.Err.**	**z-value**	**P-value**		**Coeff.**	**Std.Err.**	**z-value**	**P-value**
Private locations	-	-	-	-	Morning	-	-	-	-
Semi-private locations	-0.289	0.048	-5.956	$2.58e-09$	Afternoon	0.041	0.062	0.672	0.502
					Night	0.371	0.062	5.977	$2.28e-09$
TriggerLocation-Model-2(inside/outside) [2]					**WhoCanUse-Model**				
	Coeff.	**Std.Err.**	**z-value**	**P-value**		**Coeff.**	**Std.Err.**	**z-value**	**P-value**
Private locations	-	-	-	-	Spouse	-	-	-	-
Semi-private locations	-0.182	0.065	-2.781	0.005	Kids	0.262	0.062	4.218	$2.46e-05$
Public locations	0.229	0.078	2.915	0.003	Visitors	0.894	0.061	14.489	$< 2e-16$
					Outsider	1.419	0.063	22.385	$< 2e-16$
ActionLocation-Model					**Whoi sAround-Model**				
	Coeff.	**Std.Err.**	**z-value**	**P-value**		**Coeff.**	**Std.Err.**	**z-value**	**P-value**
Private locations	-	-	-	-	Spouse	-	-	-	-
Semi-private locations	-0.526	0.064	-8.109	$5.11e-16$	Kids	0.224	0.095	2.355	0.018
Public locations	0.070	0.076	0.912	0.362	Visitors	0.612	0.094	6.484	$8.95e-11$
					Outsiders	1.173	0.096	12.172	$< 2e-16$

[1] Applets whose triggers can only be located inside the house.
[2] Applets whose triggers can be located both outside and inside.

Table 5. Pairwise comparisons of different values for Trigger location related to regression model TriggerLocation-model 2.

	Estimate	Std.Err.	z value	Pr($>\|z\|$)
Private - Semi-private	0.182	0.065	2.781	**0.015**
Private - Public	-0.230	0.078	-2.915	**0.01**
Semi-private - Public	-0.412	0.079	-5.192	**<.0001**

event), participants rated their concerns with using the applets if these services were shared with others or allowed access to other people (*e.g.,* a public Facebook page). In fact, this was one of the few contextual factors for which participants were concerned (*Extremely* (38%), Moderately (20%)) in the majority of applets.

4.1.2 Time.

Testing the differences between two regression models (null model and Time-model) shows that participants' concerns varied significantly for *time* ($\chi^2(df = 2) = 42.84, p < 0.001$). The regression result (Time-model in Table 4) shows that participants were more concerned about the night time compared to morning. Pairwise comparisons highlight that participants were more concerned about night time when compared to afternoons ($p < 0.05$, See Table 9 in the Appendix).

4.1.3 Access.

Security and privacy implications can arise because of *who can use* the device (access the trigger) or *who is around* to observe (access) the action.

Who Can Use. The regression analysis shows that "who can use" was a significant factor in participants' concerns ($\chi^2(df = 3) = 636.96, p < 0.001$). Table 4 (WhoCanUse-model) shows that participants were less concerned if their spouse would use these applets compared to other users. Overall, participants were less concerned about their family members using the applet—spouse ($Mean = 2.16, SD = 1.45$) and kids ($Mean = 2.29, SD = 1.45$)—as compared to those who do not reside in the home—visitors ($Mean = 2.67, SD = 1.53$) and outsiders ($Mean = 3.02, SD = 1.61$). To find if these differences were significant, we ran pairwise comparisons and found that significant differences exist between all pairs of user types ($p < 0.05$ for all pairs, See Table 10 in the Appendix).

Who is Around. The regression analysis shows that "who is around" to observe the action event was a significant factor ($\chi^2(df = 3) = 175.83, p < 0.001$). Table 4 (WhoisAround model) shows that participants were more concerned about visitors and outsider as compared to their spouse. Pairwise comparisons found significant differences between all pairs of user types except for spouse and kids ($p < 0.05$, See Table 11 in the Appendix). This suggests participants did not differentiate

much between family members when considering this contextual factor.

4.2 Reasons to be concerned with using the applets in different usage contexts

The quantitative analyses showed that participants' concerns increased almost universally when they considered the contextual factors. Here we explore the reasons for participants' concerns through qualitative analyses of the 4009 valid open-ended responses. We excluded the responses in which participants did not explicitly explain reasons (*e.g.,* when the response was a reiteration of the Likert option or of the related contextual factor) from final results. Table 6 shows the top reasons across the six contextual factors.

4.2.1 Leakage of sensitive data.

As shown in Table 6 (last column), about 51.8% of all open responses included concerns about users' sensitive data being collected and used in different contexts. Participants were particularly concerned with applets connecting to *online services* that could record their private information. For example, participant P265 was concerned about a smart thermostat: "*... [others] will be able to tell when the thermostat is set to away mode, meaning no one is home*". A majority of concerns (97.4% of responses for *Action in Online Services*, Table 6) were about online logs of such sensitive information about users' presence at home, their daily activities, or their schedules. Participants were also concerned about the sensitive nature of the data that could be recorded in private locations (45.9% of valid responses for *Trigger Location*). As P319 reported: *"certain rooms are sensitive and supposed to be private. I would not want it to collect info about people in the bathroom or bedroom, for instance."* They were also concerned about the visibility of the actions (28.1% valid responses for *Action Location*), especially when in semi-private or public places. For example, consider (Applet#7) that enables printing a personal shopping list through Alexa. If the printer is *located* in a semi-private space (*e.g.,* living room), there is a chance that visitors (*e.g.,* maid or babysitter) can also see the shopping list (and any sensitive items on the list). Participants reported concerns with who could view the actions (10.9% of responses for *Who is Around*), as visitors or outsiders could then infer participants' schedules by noticing the actions. For example, P46 was concerned about (Applet#4) that turns on the coffee maker when the user wakes up: *"Because then ill intentioned people will learn my schedule and learn when I'm sleeping or awake."* Participants thought that the *Time* of the day could impact the severity of the leakage (61.6%). For instance, P14 when talking about (Applet#1) that posts an update status of users' location to Twitter said: *"...I don't want where I am to be tweeted regardless of the time of day. But night time presents its own unique risks..."*

In addition to the data leakage because of the IFTTT applets, participants were also concerned about voice assistants recording private conversations without consent. As participant P332 reported: *"I don't want my children or unsuspecting guests recorded without their permission."* Finally, some participants were concerned with leakage of details about how their home automation worked; participant P25 mentioned: *"If someone overhears me turn off the camera, then it could be used without me knowing."*

4.2.2 Unauthorized/unintended access

The second largest category of participants' concerns with applets involved unauthorized or unintended access to the applets and the resulting implications (Table 6, last column). Like with leakage of sensitive data, *location* of the IoT device raised concerns about unauthorized or unintended access. For example, with (Applet#5) that allows user to turn off the camera with a voice assistant like Alexa, P34 reported their concern about Alexa being in semi-private locations such as the living room: *"Because if its close to a visitor or outsider they can disable the cameras by saying the words to turn the cameras off."* Similarly, participants reported their concern with the risk of an applet controlled IoT device being in more sensitive areas. For instance, P289 responded: *"... I don't want the bathroom light to be controllable from outside the bathroom."* For the applet that connected cameras, participants were concerned when the camera was located in private areas (bedrooms, bathrooms) as well as at the front door. As participant P2 reported: *"I think the front[door] camera is likely the most important, so I don't want that turned off without my knowledge."*

While unauthorized/unintended accesses were of significant concern when considering location of devices (15.1% of valid responses for *Trigger Location*, 27.5% of valid responses for *Action Location*; See Table 6), they were the single largest concern (52%) when consider-

Table 6. Top coded reasons for being concerned to use applet in each usage context[2].

Reasons	Location			Time	Access		%of all responses
	Trigger location	Action location	Online services[1]	Time	Who can use	Who is around	
Leakage of sensitive data	45.9%	28.1%	97.4%	61.6%	10.9%	56.7%	51.8%
Unauthorized/unintended access	15.1%	27.5%	-	6%	52%	18.2%	22.2%
Privacy/security misconception	17.8%	3.1%	1.7%	0.6%	33.3%	4.4%	13.7%
Inconvenience	10.6%	29.3%	-	12.6%	0.1%	6.3%	5.8%
Safety	2.4%	6.2%	-	6.4%	0.6%	8.9%	2.7

[1] Action in online services

[2] The reported percentages in the table are calculated based on the responses that explicitly mention a reasoning for participant's concern

ing *who can use* the applets. In particular, participants highlighted their concern with having kids access to the applets, especially when those applets involved a voice assistant (*e.g.,* Alexa) controlling IoT devices or online services. Participants reported that this was a concern because a child could play with Alexa and end up changing the settings for applets that control the lights (Applet#36), thermostats (Applet#34), or security cameras (Applet#5). Such incorrect changes could in turn lead to incorrect configurations that could increase costs or put the house at risk. As participant P258 mentioned *"kids can't touch it as they don't know how to properly use it. It needs to be set at a certain temp as I am on a savings plan. Would cost me money if others touched it."* Other examples included situations where a child could inadvertently say things that could be posted as tweets (Applet#33), included in shopping lists (Applet#7), or added as events to Google Calendar (Applet#48). For example, participant P359 wrote about how Alexa could be misused: *"My kids could ask Alexa something [unsuitable] or order things without permission."* Another participant P267 was wary of an applet that allows Alexa to post tweets "*Kids can say some stupid stuff sometimes, ..."*

Apart from children, participants were also concerned about visitors and outsiders gaining access to their applets, particularly those related to security features such as security camera in the case of visitors. For outsiders, their concerns encompassed almost all applets. Participant P14 quoted: *"I am not concerned with who can turn the switch on, unless they are an outsider. Outsider implies [someone] I have not invited into my home."*

4.2.3 Privacy/security misconception.

Several participants' responses (13.7% of all responses) also highlighted misconceptions about privacy and security risks. Most of these are related to applets that connect IoT devices (*e.g.,* security cameras and smart locks), or location to online services. In particular, participants could not distinguish between unauthorized/unintended modification (write access) to their online accounts and leakage of information from those accounts (read access). For instance, in an applet that sends an email to the user when the security system is turned off (Applet#15), participant P145 reported: *" Because I worry about people getting access to my email and turning off the system."*

4.2.4 Inconvenience.

About 6% (Table 6, last column) of responses included concerns about the inconvenience of using the applets in different contexts. A majority of these were about the *Action Location* (29.3%), especially for devices that notified users through blinking or turning on lights as they could disturb others during the night (*Time*: 12.6%, *Who is Around*: 6.3%). For instance, participant P181 said: *"If it blinks the lights in my bedroom it could wake me up."* In 10.6% cases, participants were concerned about the accessibility of the (Trigger) location, especially the placement of voice assistants in the house, as participant P163 reported: *"if my voice does not reach the Alexa it does not work."*

4.2.5 Safety.

A small portion of concerns (2.7%, Table 6) were about the safety of using smart appliances, such as smart coffee makers, ovens, and vacuums, in an automated or unsupervised fashion. For example, participant P41 was worried if (Applet#4) would start the coffee maker when they wake up but still in bed and if their child was unsupervised in the kitchen: *"My child, because I do not want the coffee to start brewing and she touches it."* Similarly, participant P137 was concerned about (Applet#17) that enables user to turn off the oven through Alexa: *"If it were in the kitchen, I could keep an eye on the oven while it turns off. The further away I am, the more dangerous."*

5 Discussion

5.1 Applets introduce additional risks

The potential information flows that might happen as a result of connecting two IoT devices or online services is beyond the risks associated with each individual IoT device and online service. For instance, in an applet that connects Alexa to a security camera, the risks associated with Alexa and camera in terms of information collecting, storing, and sharing with third parties [2, 29], still exist and were addressed by prior work. But the applets connecting them introduce new risks even if the involved devices and services are safe (*e.g.,* data leakage from trigger source to action sink, unauthorized access to the action as a result of access to the trigger entity, *etc.*) as observed in prior work (*e.g.,* [11, 36]). These are implicit risks that might arise even with safe devices and benign applets in the home environment. Responses to open ended questions showed that the participants were able to focus on these new risks. For instance, responses from P41 and P137 (See Section 4.2.5) show that while appliances like coffee maker and oven have their own risks, participants were concerned about applets starting the appliance without the users being able to supervise their operation. Further, in the threat model of these applets, adversaries are not necessarily the external entities such as the device manufacturers, third-party frameworks, or the over-privileged apps. Our findings indicate that participants considered threats from other end-users of applets inside the home including, spouse, kids, and visitors.

Our findings from the qualitative analysis show that risks participants reported regarding a specific context are different from those of data collection scenarios and IoT devices. For instance, "Location" is a common usage context studied by most of the prior work (*e.g.,* [18, 25, 26, 29]) for its impact on users' privacy preferences. Prior work all agreed that location influences participants' comfort with data sharing. However, our qualitative analysis shows participants' concern with the location is because of different reasons. They were concerned not only because of sharing their location data resulting from implicit data flow caused by applets, but also about the accessibility of the devices and resulting in unauthorized access. For instance, with (Applet#5) that allows user to turn off the camera with a voice assistant like Alexa, P34 reported their concern about Alexa being in semi-private locations such as the living room: *"Because if its close to a visitor or outsider they can disable the cameras by saying the words to turn the cameras off."*

5.2 Applet descriptions alone are not sufficient to assess their risk

While deployments of applets brings implicit risks, it was not clear whether such risks were apparent to end users. Previous works have studied end-users' concerns with applets or their ability to assess risk by giving explicit data flow scenarios [2, 11, 29]. In contrast, in this work we explore users' concerns after giving a simple applet description, similar to what is typically available when downloading such applets, and then after providing different usage context prompts.

Our findings indicate that the descriptions of trigger-action applets were insufficient for participants to assess the risks of using IFTTT applets. Even after reading explicit trigger-action description, participants on average had low concerns with using these applets except for when the location data is reported to online services (See Section 3). This despite all the fact that all chosen applets had potential security and privacy risks. Of course, one can argue that this low concern score could be an artifact of the study setup itself, where participants "simply" answered the survey question, whereas in real life they might have given a deeper consideration to the descriptions and deployment. However, our results are in line with past work [44] that has also shown that end users have difficulty in understanding security and privacy implications of IoT devices.

Another artifact of the study setup is the time that participants took to think about each applet. Recall that participants spent an average of 3-4 minutes per applet. While this is short, it is probably how long end users will take (if that) when they review the applet descriptions during installation. For example, studies have shown that when installing applications users just want to get the application running and rarely change default settings or read privacy disclosures [5, 35].

Further, in many cases participants had difficulty understanding the security & privacy risk implications. For example, while participants readily understood the risks of leaking their location data to online services (See the applets on the top of Figure 1), they were far less concerned about applets that indirectly leaked user's presence or location by sharing house's thermostat configurations (applets at the bottom of Figure 1). Moreover, the analysis of the open-ended responses revealed there were security & privacy misconceptions (13.7%) across all the contextual factors, which were primarily related to applets connecting to online services (See Section 4.2.3). This is likely because of mismatches in participants' mental models of what and where the applet records, and the reality of how the applet operates. Past work [22, 23] has shown that end users, especially those without technical background, have simplistic mental models about information flows and about who has access to their personal data or communication.

5.3 Impact of context on end-users' risk perception

While end users reported low concern scores about deploying IFTTT applets after reading just the applet description, when prompted to think about specific usage contexts their concern ratings almost universally increased (See Figure 2) indicating that context matters to end-users' risk perception. In these cases, their main concerns (74%) were largely about leaking sensitive data and unauthorized or unintended access.

Prior work [11, 36] have observed that privacy and security risks in IFTTT applet deployment are context dependent. However, this observation was from the perspective of a security expert. Here our focus was to understand if and how contextual factors may influence end-users' risk perception. Our study is the first validation survey that empirically shows the impact of context on end-users' risk perception when determining security and privacy risks with IFTTT applets for smart homes.

Further, our findings also show that end users have a more nuanced view of the context in smart-home settings. For instance, our findings show that end users differentiate between locations within the home—private (*e.g.,* bedroom) vs. semi-private (*e.g.,* living room) as well as among house members (spouse vs. kids vs. visitors) when using applets (See Section 4.1). Thus, approaches looking to automatically detect undesirable information flows must take into account this nuanced view of contexts by end users.

Furthermore, our findings indicate that contextual factors may not influence all users in the same way and that implications of a privacy violation depend both on the context of use and the users' privacy perception. As we saw in Section 4.1.3 participants were overall less concerned about their family members getting access to their applets. For instance, P327 was concerned if her calendar was shared with anyone other than her husband *"My calendar is personal to me and should not be shared with anyone outside of my husband. It could be used to track my behaviors and not everyone uses that information for good intentions."* However, there were still participants that expressed concerns with their spouse or kids using some of the applets in certain specific contexts. For instance P359 reported her concern about her kids: *"My kids could ask Alexa something [unsuitable] or order things without permission."*

Therefore, to what extent someone is going to be concerned about the loss of privacy or security depends both on the usage context (*e.g.,* location, time, *etc.*) and user context (*e.g.,* individual's family, lifestyle, and trust relations). There is no "one size fits all" solution. This suggests that automated information flow violation detection may need to be tailored to individual user preferences in addition to considering contextual factors.

Our work opens the door for further research on the interactions between the contextual factors as well. In this work, we have only looked at a handful of contextual factors—those that were applicable to the 49 applets we studied. There may be other contextual factors that are relevant for other types of applets. Further, the different contextual factors interact. For example, a camera that can be switched off is much more problematic, if it is a security camera, if it is switched off at night time, and there are (young) kids in the house. Such interaction of different contextual factors and the implications of those interactions on privacy concerns needs further study.

5.4 Using contextual factor considerations as a "nudge"

Prior work has proposed "nudging" users towards making better decisions about sharing information in online social networks [28, 42], for example, by showing what others in their peer groups have done. Our finding that user concern scores increased almost universally when they were prompted to think about specific usage contexts opens a research opportunity around facilitating better security & privacy risk assessments by end users to help them make informed choices by using contextual factor considerations as a "nudge". In particular, there are opportunities for researching intuitive designs that smart-home management systems and frameworks (*e.g.,* SmartThings, HomeKit) can create to enable end users to easily and efficiently reflect on the different contextual factors that are applicable to a particular applet.

Previous work [11] has found that users desire to keep using their applets changed only a little even after providing a specific violation scenario. We might have seen bigger changes in participants' concerns because contextual information can direct users' attention to different possible violation scenarios instead of a specific scenario. Future research could investigate mechanisms to automatically create such security & privacy nudges based on the contextual factors applicable to a given applet and tailored to a users' profile or past data usage.

Another lighter-weight option could be a method to identify a set of standardized contextual factors for each class of applets and some metrics for portraying confidentiality (leakage of sensitive data) and integrity (unauthorized use) violations, akin to the concept of standardized labels proposed by Kelley *et al.* [24] for comparing privacy policies of websites.

6 Related work

Our work aims to understand how well end users are able to assess potential risks with using *trigger-action* applets in a smart-home environment. Further, we investigate how contextual factors might influence their assessment. Hence we focus on related work on the impact of context on users' concerns in mobile and Internet-of-Things (IoT) environments. We also survey work that looks at the risk from the perspective of unintended information flows and unauthorized accesses in IoT frameworks for smart homes.

6.1 Impact of context on users' concerns

Smart home and IoT: Much work has been done to understand users' privacy preferences broadly in IoT applications and frameworks. Importantly, *(i)* Emami-Naeini *et al.* [29] investigated users' comfort level with data collection scenarios and the impact of different contextual factors such as the type of data, retention time, purpose of data collection, and location of data collection; *(ii)* Lee *et al.* [25, 26] explored the impact of factors including location, what data is collected, who is collecting, the reason for data collection, and the frequency of data collection, on users' privacy preference in IoT. Other studies investigated the reasons users accept home sensing systems [10] or give external entities access to home IoT devices [44]; investigated factors that influence users' preferences about giving others access permissions to use the IoT apps [18], and privacy norms in which information transmission is un/acceptable [2].

In contrast to prior work, this work focuses on users' concerns with real world trigger-action applets that connect two or more IoT devices/services rather than on individual IoT devices [2, 18, 25, 26] or IoT data collection scenarios [29]. Further, this work considers contextual factors that are relevant to the usage of the applets in the home environment and are different from those related to data collection [29].

Furthermore, unlike many previous works in this work we do not provide explicit details about privacy and security risks. For instance, instead of discovering user privacy norms with explicit information flow scenarios [2] or pointing to risks explicitly [11] we investigate whether users can even notice if certain undesirable information flows may exist when deploying an applet and how their perceived concerns evolve after being given just the applet description, and after being presented with different contextual factors. This also helps us to uncover other areas of concerns (*e.g.,* safety) depending on the context that might be considered when creating tools to help end users better understand impacts of using IoT devices.

Mobile applications: Much work on evaluating factors influencing users' concerns with mobile apps also exists. For example, Sadeh *et al.* [34] found that increasing users' awareness would help them make better choices regarding sharing their location information. Lin *et al.* [27] found that giving information about why a resource is being used by a mobile app can impact users' privacy concerns related to mobile apps. Tsai *et al.* [38] found that users became more comfortable with sharing their location data with friends and strangers after see-

ing feedback about who has viewed their location data, and when the location data was shared. In contrast, we investigate users' concerns with using applets that connect *multiple* home IoT devices or online services in a *richer context.*

6.2 Security and privacy concerns in IoT

IoT programming frameworks: The coarse-grained permission models that are being used by current programming frameworks (*e.g.,* Samsung SmartThings [13], Apple's HomeKit [6], OpenHAB) are ineffective in controlling sensitive information flows and unauthorized access of sensitive data. Fernandes *et al.* [14] evaluated SmartThings and discussed design flaws that lead to over-privileged apps. Several solutions to mitigate sensitive information flows and unauthorized accesses within IoT apps have also emerged. For example, ContextIoT [21], is a context-based permission system that identifies the usage context of sensitive actions using control and data flow information. Similarly, SAINT [7] uses static analysis of application code to identify sensitive information flows between taint sources and taint sinks. SmartAuth [37] system uses device information and app descriptions to identify over-privileged apps. Those approaches aim to fix sensitive information flows and improve access control models within a single app. However, explicit and implicit interactions between multiple IoT apps could also lead cause confidentiality and integrity violations.

Approaches to address cross application violations have also been proposed. For example, FlowFence [15] approach enforces information flow controls by restricting usage of sensitive data inside sandboxes. ProvThings [41] framework uses provenance data to identify malicious information flows across security sensitive IoT apps and device APIs. SOTERIA [8] uses the state model of individual or set of apps to check safety, security, and functional properties and find property violations. IoTGuard [9] proposes a dynamic policy-based enforcement system to protect users against integrity and confidentiality violations using predefined safety and security policies on individual or set of interacting apps.

In the preceding approaches, low level system contextual information including source code and/or security labels for data and entities defined by security experts were used to identify information flow-based and other security violations. However, such approaches cannot capture security and privacy violations that are dependent on high level semantic contextual factors such as usage context, and user privacy perceptions and preferences. Our findings in this work show that high level (as opposed to low level system context) contextual factors play an important role in users' perceived risks and hence in defining what constitutes a risk.

Trigger-action programming frameworks: Emerging trigger-action programming frameworks (*e.g.,* IFTTT, Microsoft Flow, Zapier [12]) that help end users to connect IoT devices with online services, also suffer from weak access control and other security and privacy issues similar to IoT programming frameworks. Lack of fine-grained access controls can lead to privacy and integrity violations [43]. Surbatovich *et al.* [36] proposed a security lattice model that uses labeled triggers and actions to identify sensitive information flows in IFTTT. A similar approach was used by Bastys *et al.* [3] to label triggers, actions, and to automatically prevent identified violations (*e.g.,* integrity, confidentiality, availability) by breaking the information flows from private sources to public sinks. The labels that are used in these previous two approaches are coarse grained and are based on *who can use* and *who can observe* the data and do not consider other usage contexts. For instance, those approaches do not differentiate between people inside a home environment.

Cobb *et al.* [11], improved on the security labels of Surbatovich *et al.* [36] and manually investigated the efficacy of the improved labelling scheme. Their work recognized and acknowledged that the granularity of secrecy and integrity labels can be improved through a better understanding of contextual factors. Our work empirically investigates to what extent contextual factors matter to participants, and the importance of these factors and their interplay.

The frameworks and systems discussed here can benefit from our work as they can be improved to create more fine-grained information flow policies based on our findings.

7 Conclusion

In this paper we reported on an online Mechanical Turk survey (n=386) on users' concerns related to *trigger-action* applets for smart homes that are available through the IFTTT platform.

Our results enhance the findings of previous works by showing how different contextual factors affect end-users' concerns. Our analysis shows that even when de-

scriptions explicitly mention the trigger-action components in applets, participants fail to perform adequate risk assessments, expressing low concerns with using applets with underlying security and privacy threats.

Our study shows that contextual factors are nuanced and their interplay affects users' concerns. We have only scratched the surface—evaluating 6 contextual factors— and shown that research opportunities exist to better understand *(i)* the role that context plays in end-users' concerns and *(ii)* how to devise mechanisms to help end users evaluate the context of use better. The extreme popularity and ubiquity of trigger-action applets necessitates further investigations into how we can help end users better perform risk assessments of trigger-action applets.

8 Acknowledgments

This work has been partially funded by NSF:2008089.

References

[1] If This, Then That (IFTTT). https://www.ifttt.com/. Accessed: 2019-09-9.

[2] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. Discovering smart home internet of things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(2):1–23, 2018.

[3] Iulia Bastys, Musard Balliu, and Andrei Sabelfeld. If this then what?: Controlling flows in iot apps. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1102–1119. ACM, 2018.

[4] Microsoft Flow: Automate processes and tasks. https://flow.microsoft.com/. Accessed: 2019-09-9.

[5] Rainer Böhme and Stefan Köpsell. Trained to accept?: A field experiment on consent dialogs. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 2403–2406, New York, NY, USA, 2010. ACM.

[6] Apple's HomeKit. http://www.apple.com/ios/home/. Accessed: 2019-09-9.

[7] Z Berkay Celik, Leonardo Babun, Amit Kumar Sikder, Hidayet Aksu, Gang Tan, Patrick McDaniel, and A Selcuk Uluagac. Sensitive information tracking in commodity iot. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 1687–1704, 2018.

[8] Z Berkay Celik, Patrick McDaniel, and Gang Tan. Soteria: Automated iot safety and security analysis. In *2018 USENIX Annual Technical Conference (USENIX ATC 18)*, pages 147–158, 2018.

[9] Z Berkay Celik, Gang Tan, and Patrick D McDaniel. Iotguard: Dynamic enforcement of security and safety policy in commodity iot. In *NDSS*, 2019.

[10] Eun Kyoung Choe, Sunny Consolvo, Jaeyeon Jung, Beverly Harrison, Shwetak N Patel, and Julie A Kientz. Investigating receptiveness to sensing and inference in the home using sensor proxies. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, pages 61–70. ACM, 2012.

[11] Camille Cobb, Milijana Surbatovich, Anna Kawakami, Mahmood Sharif, Lujo Bauer, Anupam Das, and Limin Jia. How risky are real users' ifttt applets? In *Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020)*, pages 505–529, 2020.

[12] Zapier: Automate Workflows. https://zapier.com/. Accessed: 2019-09-9.

[13] Samsung Smartthings. https://www.smartthings.com/. Accessed: 2019-09-9.

[14] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. Security analysis of emerging smart home applications. In *2016 IEEE symposium on security and privacy (SP)*, pages 636–654. IEEE, 2016.

[15] Earlence Fernandes, Justin Paupore, Amir Rahmati, Daniel Simionato, Mauro Conti, and Atul Prakash. Flowfence: Practical data protection for emerging iot application frameworks. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 531–548, 2016.

[16] Joseph L Fleiss, Bruce Levin, and Myunghee Cho Paik. *Statistical methods for rates and proportions*. john wiley & sons, 2013.

[17] Hana Habib, Neil Shah, and Rajan Vaish. Impact of contextual factors on snapchat public sharing. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2019.

[18] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. Rethinking access control and authentication for the home internet of things (iot). In *27th USENIX Security Symposium (USENIX Security 18)*, pages 255–272, 2018.

[19] OPENHAB: Open Source Automation Software for Home. https://www.openhab.org/. Accessed: 2019-09-9.

[20] What is IFTTT? How to use If This, Then That services . https://www.computerworld.com/article/3239304/what-is-ifttt-how-to-use-if-this-then-that-services.html. Accessed: 2020-12-12.

[21] Yunhan Jack Jia, Qi Alfred Chen, Shiqi Wang, Amir Rahmati, Earlence Fernandes, Zhuoqing Morley Mao, and Atul Prakash. Contexlot: Towards providing contextual integrity to appified iot platforms. In *NDSS*, 2017.

[22] Kim J Kaaz, Alex Hoffer, Mahsa Saeidi, Anita Sarma, and Rakesh B Bobba. Understanding user perceptions of privacy, and configuration challenges in home automation. In *2017 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*, pages 297–301. IEEE, 2017.

[23] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. Privacy attitudes of mechanical turk workers and the us public. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, pages 37–49, 2014.

[24] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. Standardizing privacy notices: An online study of the nutrition label approach. In *Proceedings of*

the SIGCHI Conference on Human Factors in Computing Systems, CHI '10, pages 1573–1582, New York, NY, USA, 2010. ACM.

[25] Hosub Lee and Alfred Kobsa. Understanding user privacy in internet of things environments. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pages 407–412. IEEE, 2016.

[26] Hosub Lee and Alfred Kobsa. Privacy preference modeling and prediction in a simulated campuswide iot environment. In *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 276–285. IEEE, 2017.

[27] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM conference on ubiquitous computing*, pages 501–510. ACM, 2012.

[28] Hiroaki Masaki, Kengo Shibata, Shui Hoshino, Takahiro Ishihama, Nagayuki Saito, and Koji Yatani. Exploring nudge designs to help adolescent sns users avoid privacy and safety threats. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2020.

[29] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an iot world. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 399–412, 2017.

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

[31] Sören Preibusch. Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies*, 71(12):1133–1143, 2013.

[32] R Core Team. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, Vienna, Austria, 2013.

[33] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 2019 IEEE Symposium on Security and Privacy (SP), Vol. 00. IEEE*, pages 227–244, 2019.

[34] Norman Sadeh, Jason Hong, Lorrie Cranor, Ian Fette, Patrick Kelley, Madhu Prabaker, and Jinghai Rao. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing*, 13(6):401–412, 2009.

[35] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. A design space for effective privacy notices. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*, SOUPS '15, pages 1–17, Berkeley, CA, USA, 2015. USENIX Association.

[36] Milijana Surbatovich, Jassim Aljuraidan, Lujo Bauer, Anupam Das, and Limin Jia. Some recipes can do more than spoil your appetite: Analyzing the security and privacy risks of ifttt recipes. In *Proceedings of the 26th International Conference on World Wide Web*, pages 1501–1510. International World Wide Web Conferences Steering Committee, 2017.

[37] Yuan Tian, Nan Zhang, Yueh-Hsun Lin, XiaoFeng Wang, Blase Ur, Xianzheng Guo, and Patrick Tague. Smartauth: User-centered authorization for the internet of things. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 361–378, 2017.

[38] Janice Y Tsai, Patrick Kelley, Paul Drielsma, Lorrie Faith Cranor, Jason Hong, and Norman Sadeh. Who's viewed you?: the impact of feedback in a mobile location-sharing application. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2003–2012. ACM, 2009.

[39] Gerhard Tutz and Wolfgang Hennevogl. Random effects in ordinal regression models. *Computational Statistics & Data Analysis*, 22(5):537–557, 1996.

[40] Blase Ur, Elyse McManus, Melwyn Pak Yong Ho, and Michael L Littman. Practical trigger-action programming in the smart home. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 803–812. ACM, 2014.

[41] Qi Wang, Wajih Ul Hassan, Adam Bates, and Carl Gunter. Fear and logging in the internet of things. In *Network and Distributed Systems Symposium*, 2018.

[42] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. A field trial of privacy nudges for facebook. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 2367–2376, 2014.

[43] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. Dolphinattack: Inaudible voice commands. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 103–117. ACM, 2017.

[44] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home iot privacy. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):1–20, 2018.

A Applet descriptions

Table 7. Applet descriptions.

App#	Description
App1	This applet connects your location and Twitter. This specific applet will post a tweet to twitter when you enter a location.
App2	This applet connects your WeMo Insight Switch and email. This specific applet sends an email every time your switch is turned on.
App3	This applet connects your EverNote and location. This applet specifically will add a new note when you enter an area.
App4	This applet connects your Fitbit and WeMo coffee maker. This specific applet turns your coffee maker on when your Fitbit logs that you have woken up for the day.
App5	This applet connects your Alexa and Nest security camera. This specific applet will turn your camera off when you say "Alexa, turn off camera".
App6	This applet connects your Nest security camera and Google spreadsheet. This specific applet will add a new row to your spreadsheet when your camera detects motion.
App7	This applet connects your printer and your Alexa. This specific applet will print your grocery list when you say "Alexa what's on my shopping list".
App8	This applet connects your Samsung Robot vacuum and time. This specific applet has your vacuum start cleaning everyday at a specific time.
App9	This applet connects your Alexa and your appliance. This specific applet will turn your TV on when you ask Alexa to "turn on your TV".
App10	This applet connects your location and EverNote. This applet specifically will add a new note when you exit an area.
App11	This applet connects your WeMo plug and google calendar. This specific applet adds an event to your calendar every time your switch is turned on.
App12	This applet connects your email and WeMo light switch. This specific applet sends you an email daily giving you the details of how much it costs to operate your light switch.
App13	This applet connects your location and Facebook. This specific applet will post a Facebook status when you enter an area.
App14	This applet connects your Nest thermostat and time. This specific applet turns your thermostat on once a day at a specific time for the length of time you decide.
App15	This applet connects your Arlo security system and email. This specific applet will send you an email when your security system is turned off.
App16	This applet connects your Google spreadsheet and location. This specific applet will add a row to your spreadsheet when you exit an area.
App17	This applet connects your appliance and Alexa. This specific applet will turn off your oven when you ask Alexa to "turn off your oven".
App18	This applet connects your Ring doorbell and EverNote. This specific applet adds a note when your doorbell detects motion as a visitor log.
App19	This applet connects your location and email. This specific applet will email you when you leave an area.
App20	This applet connects your Phillips Hue lights and Android SMS. This specific applet will blink your lights when you receive an SMS.
App21	This applet connects your Alexa and EverNote.This specific applet will add items to your list when you say "Alexa add milk to my grocery list".
App22	This applet connects your location and Phillips Hue lights. This specific applet will turn off all the lights when you leave a specific area.
App23	This applet connects your Samsung washer and EverNote app. This specific applet adds a note when you start a new washer cycle.
App24	This applet connects your location and Google spreadsheet. This specific applet will add a row to your spreadsheet every time you enter an area.

Table 7. Applet descriptions.

App#	Description
App25	This applet connects your Alexa and Phillips Hue lights. This specific applet will turn your lights turn off when you ask Alexa to "turn lights off".
App26	This applet connects your Samsung washer and Phillips Hue lights. This specific applet will blink your lights when your washer has started a load.
App27	This applet connects your Alexa and Nest thermostat. This specific applet will adjust your temperature when you say "Alexa, set thermostat to 62 degrees".
App28	This applet connects your Ring doorbell and Google calendar. This specific applet will add an event to your calendar when your doorbell detects motion.
App29	This applet connects your Samsung washer and google calendar. This specific applet adds an event to your calendar when the washer has finished a wash cycle.
App30	This applet connects your Nest thermostat and email. This specific applet will send you an email when your thermostat set away.
App31	This applet connects your email and Kevo lock. This specific applet will send you an email when your lock is locked.
App32	This applet connects your Phillips Hue lights and time. This specific applet will turn your lights off at a specific time everyday.
App33	This applet connects your Alexa and Twitter. This specific applet will post a tweet to your twitter when you say "Alexa, post a tweet".
App34	This applet connects your Alexa and Nest thermostat. This specific applet will turn your fan on for 15 minutes when you say "Alexa, turn fan on".
App35	This applet connects your Nest security camera and email. This specific applet sends you an email when your camera detects motion.
App36	This applet connects your Alexa and Phillips Hue lights. This specific applet will turn your lights on when you ask Alexa to "turn on lights".
App37	This applet connects your email and SmartThings hub. This specific applet will send you an email when it detects motion.
App38	This applet connects your Wemo plug and email. This specific applet sends an email when your plug is turned on.
App39	This applet connects your email and Kevolock. This specific applet will send you an email when your lock is unlocked.
App40	This applet connects your Alexa and Spotify. This specific applet will play your Spotify when you say "Alexa, play my Spotify top hit playlist".
App41	This applet connects your location and email. This specific applet will send you an email when you enter an area.
App42	This applet connects your Ring doorbell and Phillips Hue lights. This specific applet will blink your lights when your doorbell detects motion.
App43	This applet connects your Phillip Hue lights and Alexa. This specific applet will blink Philips Hue lights when you say "blink the lights".
App44	This applet connects your Google spreadsheet and SmartThings hub. This specific applet will add a row to your spreadsheet when your hub detects your motion.
App45	This applet connects your Samsung washer and email. This specific applets sends you an email when your washer has completed a cycle.
App46	This applet connects your email and Nest thermostat. This specific applet will send you an email when your thermostat set home.
App47	This applet connects your Arlo security system and email. This specific applet will send you an email when your security system has a problem.
App48	This applet connects your Alexa and Google calendar. This specific applet will add the next game to your calendar when you say "Alexa when do the Golden state warriors play next".
App49	This applet connects your location service on your smart phone and Arlo security system. This specific applet will turn your security system on when you leave your home.

B Sample survey questions

B.1 Demographics questions

1. What is your gender?
   - Male
   - Female
   - Trans
   - Non-binary
   - Prefer not to say
2. What is your age?
   - 18-24
   - 25-34
   - 35-44
   - 45-54
   - 55-64
   - 65+
3. What is the highest level of education you have completed?
   - Less than high school
   - High school graduate
   - Some college
   - 2 year degree
   - 4 year degree
   - Professional degree
   - Doctorate,
   - Prefer not to answer
4. How many IFTTT applets have you used?
   - 0
   - 1-2
   - 3-4
   - More than 5
5. How many smart home devices do you own?
   - 0
   - 1-2
   - 3-4
   - More than 5

B.2 Applet questions

Applet description: Suppose there is an applet that connects your **Alexa** and your **Nest security camera**. This specific applet will turn your camera off when you say "Alexa, turn off camera".

1. Would you be concerned about using this applet? (Answered on a five point Likert scale from “Not at all concerned” to “Extremely concerned”)
2. To what extent do the following factors affect your concern in using this applet? (Answered on a five point Likert scale from “Not at all concerned” to “Extremely concerned”(See Figure 3)
   - The time when you ask Alexa (Morning, Afternoon, Night)
   - The location of Alexa (Living room, Kitchen , Bedroom, Bathroom)
   - Who can talk to Alexa (Spouse, Kids, Visitor, Outsider)
   - The location of camera (Living room, Kitchen , Bedroom, Bathroom, Frontdoor)
   - Who is around (Spouse, Kids, Visitor, Outsider)
3. Why are you concerned with **what time** you talk to Alexa?
4. Why are you concerned with the **location of your Alexa**?
5. Why are you concerned with **who can talk** to your Alexa?
6. Why are you concerned with **who is around**?
7. Why are you concerned with the **location of your camera**?

	Not at all Concerned	Slightly Concerned	Somewhat concerned	Moderately Concerned	Extremely Concerned
The time when you ask Alexa					
Morning	○	○	○	○	○
Afternoon	○	○	○	○	○
Night	○	○	○	○	○
Location of Alexa					
Kitchen	○	○	○	○	○
Living Room	○	○	○	○	○
Bathroom	○	○	○	○	○
Bedroom	○	○	○	○	○
Who can talk to Alexa					
Spouse	○	○	○	○	○
Kids	○	○	○	○	○
Visitor	○	○	○	○	○
Outsider	○	○	○	○	○
Location of camera					
Kitchen	○	○	○	○	○
Living Room	○	○	○	○	○
Bathroom	○	○	○	○	○
Bedroom	○	○	○	○	○
Front door	○	○	○	○	○
Who is around					
Spouse	○	○	○	○	○
Kids	○	○	○	○	○
Visitor	○	○	○	○	○
Outsider	○	○	○	○	○

Fig. 3. The actual format of questions asking about contextual factors in the survey.

C Pairwise comparisons

Table 8. Pairwise comparisons of different values for Action location (See Section 4.1.1).

	Estimate	Std.Err.	z value	Pr($>\|z\|$)
Private - Semi-private	0.527	0.065	8.109	**<.0001**
Private - Public	−0.070	0.076	−0.912	0.632
Semi-private - Public	−0.597	0.078	−7.594	**< .0001**

Table 9. Pairwise comparisons of different values for Time (See Section 4.1.2).

	Estimate	Std.Err.	z value	Pr(>|z|)
Morning - Afternoon	−0.0417	0.062	−0.672	0.779
Morning - Night	−0.371	0.062	−5.977	**<.0001**
Afternoon - Night	−0.3300	0.062	−5.311	**<.0001**

Table 10. Pair wise comparisons of different values for Who can use (See Section 4.1.3).

	Estimate	Std.Err.	z value	Pr(>|z|)
Spouses - Kids	−0.26	0.062	−4.21	**0.0001**
Spouses - Visitors	−0.89	0.061	−14.48	**<.0001**
Spouses - Outsiders	−1.42	0.063	−22.38	**<.0001**
Kids - Visitors	−0.63	0.060	−10.50	**<.0001**
Kids - Outsiders	−1.15	0.061	−18.75	**<.0001**
Visitors - Outsiders	−0.52	0.059	−8.78	**<.0001**

Table 11. Pairwise comparisons of different values for Who is around (See Section 4.1.3).

	Estimate	Std. Err.	z value	Pr(>|z|)
Spouses - Kids	−0.224	0.095	−2.355	0.086
Spouses - Visitors	−0.613	0.094	−6.484	**<.0001**
Spouses - Outsiders	−1.173	0.096	−12.172	**<.0001**
Kids - Visitors	−0.388	0.092	−4.188	**0.0002**
Kids - Outsiders	−0.949	0.094	10.051	**<.0001**
Visitors - Outsiders	−0.561	0.092	−6.072	**<.0001**